

FINANCING ARTIFICIAL INTELLIGENCE READY DATA CENTERS IN
MODERNIZING CRITICAL INFRASTRUCTURE SECTORS

by

PRASHANT AGARWAL (Student ID 71209)

DISSERTATION

Presented to the Swiss School of Business and Management Geneva

in Partial Fulfillment

of the Requirements

for the Degree

DOCTOR OF BUSINESS ADMINISTRATION

SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

April 2026

FINANCING ARTIFICIAL INTELLIGENCE READY DATA CENTERS IN
MODERNIZING CRITICAL INFRASTRUCTURE SECTORS

by

PRASHANT AGARWAL

APPROVED BY

Iva Buljubasic

< Prof. Dr. Iva Buljubasic, Ph.D.> Dissertation Chair

RECEIVED/APPROVED BY:

Rense Goldstein Osmic

Admissions Director

Dedication

This thesis is lovingly dedicated to my family. To my wife, whose unwavering support, patience, and encouragement have been my constant source of strength. To my daughter, whose joy and curiosity inspire me to strive for excellence. And to my parents and sisters, who instilled in me the values of perseverance, integrity, and lifelong learning. And to my extended family, whose collective encouragement and well-wishes have supported me throughout this journey.

Acknowledgements

I would like to mention that I would not have achieved my DBA without my mentor, whose advice and support played a very significant role in my journey towards completing my doctoral degree. Your support and advice have been my constant push to keep going and reach this milestone.

I would also like to say a word of gratitude to SSBM Geneva, which has offered me a greater level of knowledge and academic excellence, and has enhanced my research and expanded my vision.

I also owe a debt of gratitude to the organizations that I am affiliated with for the assistance and opportunities that helped me to carry out this work. The knowledge and support I gained from them has been invaluable.

Lastly, I offer my love to my family—my wife, daughter, and parents—who have loved me, been patient, and made sacrifices. I would not have been able to do this without your support and faith in me.

ABSTRACT

FINANCING ARTIFICIAL INTELLIGENCE READY DATA CENTERS IN MODERNIZING CRITICAL INFRASTRUCTURE SECTORS

Prashant Agarwal

April 2026

This thesis explores the important role of AI-ready data centers in improving critical infrastructure sectors (CIS) such as energy, healthcare, transportation, and telecommunications. These data centers are specially designed to handle heavy computational tasks with real-time processing, ensuring systems are faster, smarter, and more reliable. However, as useful as they are, these data centers face big challenges related to high energy use, environmental impact, and the huge costs of building and maintaining them. The research develops a framework, based on Multi-Criteria Decision Analysis (MCDA), which evaluates different ways to finance AI-ready data centers sustainably. This framework considers factors like regulatory compatibility, scalability, and the unique needs of sectors across regions like the European Union (EU), United States, and Australia. The study shows that AI-ready data centers are essential for tasks like managing smart energy grids, improving healthcare diagnostics, monitoring transportation, and securing sensitive data. However, they consume enormous amounts of energy, often exceeding 15 MW annually, and require advanced cooling technologies like liquid cooling, which increases both their environmental impact and cost.

Key findings reveal that tools like green bonds, public-private partnerships (P3s), and sustainability-linked loans play a vital role in funding these centers. For example, the

EU relies on programs like the Green Deal and Horizon Europe to meet climate goals, while the U.S. benefits from federal grants and innovation funding. Australia's approach is driven by environmental, social, and governance (ESG) investments, which match its focus on sustainability. Case studies, such as those on disaster-resilient systems and energy-efficient cooling technologies, demonstrate that adopting tailored financing options can reduce costs by 30–50% and significantly improve energy efficiency. By linking financing with sustainability goals, such as using renewable energy or cutting carbon emissions, governments and businesses can make these advanced data centers more affordable and environmentally friendly. The thesis concludes that to fully unlock the potential of AI-ready data centers, there is a need for innovative financing methods like carbon credits, modular data systems, and decentralized setups. It also suggests standardized sustainability metrics, collaborative efforts between governments and businesses, and targeted regional policies to overcome challenges like climate change and funding limitations—especially in less developed countries. These changes will ensure digital transformation while protecting the environment and keeping essential services running smoothly.

Key words: Data centers, financing artificial intelligence, AI ready data center, critical infrastructure sector

TABLE OF CONTENTS

Dedication	iii
Acknowledgements	iv
Abstract	v
List of Tables	ix
List of Figures	x
List of Abbreviations	xii
CHAPTER I: INTRODUCTION.....	1-25
1.1 Artificial Intelligence (AI), Data Centers, and Critical Infrastructure Sectors (CIS)	1
1.2 Need for Modernizing CIS.....	7
1.3 Role of AI and Other Digital Tools in CIS Modernization	11
1.4 Research Gaps in AI-and Blockchain based Security for CIS.....	15
1.5 Research Problem	20
1.6 Research Questions and Objectives	21
1.7 Thesis Structure and Overview	24
CHAPTER II: RESEARCH DESIGN AND APPROACH	26-31
2.1 Theoretical Framework.....	26
2.2 Research Design and Methodology	26
2.3 Multi-Criteria Decision Analysis (MCDA) Framework.....	29
CHAPTER III: FINDINGS AND ANALYSIS	32-106
3.1 AI Ready Data Center	33
3.2 For RQ-1: Impact of AI Demand on Data Center Operations	37
3.3 For RQ-2: Sustainability Challenges and Mitigation Strategies in AI-Driven Data Centers	49
3.4 For RQ-3: Future Demands of AI on Data Center Infrastructure and Financing Implications	59
3.5 For RQ-4: Sustainable Finance Instruments for AI-Ready Data Centers	69
3.6 For RQ-5: Modifications and Innovations to Sustainable Finance Instruments for Data Center Modernization.....	78
3.7 For RQ-6: Risks and Rewards of Sustainable Finance for AI- Ready Data Centers.....	85

3.8 For RQ-7: Lessons Learned from Data Center Financing and Modernization Case Studies	91
3.9 For RQ-8: Regional Variations in Sustainable Financing Models for Data Center Modernization	99
3.10 For RQ-9: Research Propositions for Guiding Industry Adoption of Sustainable Financing Strategies for AI-Ready Data Centers	103
CHAPTER IV: DISCUSSION IN THE CONTEXT OF CIS AND RECOMMENDATIONS	107-150
4.1 AI-Ready Data Centers for Safeguarding CIS	107
4.2 Insights on Resilience and Safeguarding Mechanisms for Critical Infrastructure Sectors Through Sustainable AI-Ready Financing.....	110
4.3 The integration of AI-ready data centers and Financing Routes for each USA Critical Infrastructure.....	115
4.4 The integration of AI-ready data centers and Financing Routes for each Critical Infrastructure in Australia	128
4.5 The Integration of AI-Ready Data Centers and Financing Routes for Each EU Framework Critical Infrastructure	139
CHAPTER V: CONCLUSIONS AND BUSINESS IMPLICATIONS	151-157
5.1 Conclusion	151
5.2 Business Implications	153
5.3 Limitations and Future Research	154
REFERENCES	158-170
APPENDIX A. CRITERIA DEFINITIONS AND SELECTION PROCESS.....	171

LIST OF TABLES

Table: 2.1 Criteria applied for secondary data collection	28
Table: 2.2 The relative importance of each criterion represented as criteria weightage in %.....	29
Table: 3.1 Difference in power usage effectiveness between the AI-ready and traditional data centers along with a rationale.	43
Table: 3.2 Operational challenges between the AI-ready and traditional data centers along with a rationale.	45
Table: 3.3 Various financial instrument and their pros and cons	71
Table: 3.4 Evaluation of financial instrument suitability for different data centers based on the size	73
Table: 3.5 Evaluation of financial instrument suitability for traditional and AI-ready data centers.....	76
Table: 3.6 Proposed modifications and innovations for sustainable financial instruments tailored for data centers	82
Table: 3.7 Risk type in data centers and its assessment	86
Table: 3.8 Risk mitigation strategies and identification of potential rewards	88
Table: 3.9 Summary of interventions and results in Google's POP Facility Retrofitting.....	92
Table: 3.10 Quantitative outcomes summary for Google's POP Facility retrofitting.....	95
Table: 3.11 Scalability across multiple POPs in Google.	95
Table: 3.12 Summary of the impacts and benefits of retrofitting the data center.....	96
Table: 4.1 Financial routes with feasibility score for AI ready data center in 16 critical infrastructure sectors in USA.....	127
Table: 4.2 Financial routes with feasibility score for AI ready data center in 11 critical infrastructure sectors in Australia	135
Table: 4.3 Financial routes with feasibility score for AI ready data center in 10 critical infrastructure sectors in European Union	145

LIST OF FIGURES

Figure 3.1 Architectural shift between the traditional data center and AI-ready data center...	32
Figure 3.2 Architectural layout of the AI-ready data center.	33
Figure 3.3 Share of power usage effectiveness in traditional data centers..	38
Figure 3.4 Difference in power usage effectiveness in traditional and AI-ready data centers.....	39
Figure 3.5 Power density per rack in traditional, AI-ready and future AI data centers.	40
Figure 3.6 Power usage effectiveness for different cooling methods employed in AI-ready and traditional data centers.....	41
Figure 3.7 Share of power usage effectiveness in AI-ready data centers in comparison with traditional data centers..	43
Figure 3.8 Carbon emission of data centers due to electricity consumption and its comparison with other sectors	50
Figure 3.9 Carbon emission for data centers..	52
Figure 3.10 Water usage in data centers..	53
Figure 3.11 e-Waste from AI servers.....	54
Figure 3.12: e-Waste from AI data centers based on the literature data.....	56
Figure 3.13: Market size of data centers for future.....	59
Figure 3.14: Market share of data centers across various sectors.....	61
Figure 3.15: Projection of power demands based on the market size.....	62
Figure 3.16: Share of critical IT load for data center types under different operating modes.	62
Figure 3.17: Project of water withdrawals and water consumption for data centers.	63
Figure 3.18: CapEx of the data center.	64
Figure 3.19: AI training cost in the data centers.	65
Figure 3.20: Cash flows and unit economics of data centers.....	66
Figure 3.21: CapEx per different quarter and operational capacity added for hyperscale data center operator.	69

Figure 4.1: 16 critical infrastructure sectors essential for national security,
economic stability, and public health in USA. 116

Figure 4.2: 11 critical infrastructure sectors in Australia 129

Figure 4.3: 10 critical infrastructure sectors in European Union..... 140

LIST OF ABBREVIATIONS

ABS : Asset-Backed Securities

ADF : Australian Defence Force

AI : Artificial Intelligence

ASHRAE : American Society of Heating, Refrigerating and Air-Conditioning Engineers

CAP : Common Agricultural Policy

CEF : Connecting Europe Facility

CER : Critical Entities Resilience

CIS : Critical Infrastructure Sectors

CFATS : Chemical Facility Anti-Terrorism Standards

CRAC : Computer Room Air Conditioning

CRAH : Computer Room Air Handler

DC : Direct Current

DFARS : Defense Federal Acquisition Regulation Supplement

DNS : Domain Name Systems

DoS : Denial of Service

DDoS : Distributed Denial of Service

EaaS : Energy-as-a-Service

ECI : European Critical Infrastructure

EHR : Electronic Health Records

EIB : European Investment Bank

ESG : Environmental, Social, and Governance

ETLOP : ExaFLOP (exa floating-point operation)

FCC : Federal Communications Commission

FedRAMP : Federal Risk and Authorization Management Program

FEMA : Federal Emergency Management Agency

FISMA : Federal Information Security Management Act

GANs : Generative Adversarial Networks

GDPR : General Data Protection Regulation

GNNs : Graph Neural Networks

GPU : Graphics Processing Unit

HIPAA : Health Insurance Portability and Accountability Act

HITECH : Health Information Technology for Economic and Clinical Health

HMI : Human-Machine Interface

HVAC : Heating, Ventilation, and Air Conditioning

IEC : International Electrotechnical Commission

IoT : Internet of Things

IRR : Internal Rate of Return

ISO : International Organization for Standardization

IT : Information Technology

LMA : Loan Market Association

LLM : Large Language Model

MW : Megawatt

NBN : National Broadband Network

NCRIS : National Collaborative Research Infrastructure Strategy

NERC-CIP : North American Electric Reliability Corporation Critical Infrastructure Protection

NIS2 : Network and Information Systems Directive 2

NVLink : NVIDIA Link Interconnect

NVMe : Non-Volatile Memory Express

OT : Operational Technology
OPEX : Operational Expenditure
P3s : Public-Private Partnerships
PPA : Power Purchase Agreement
PUE : Power Usage Effectiveness
R&D : Research and Development
ROI : Return on Investment
SCADA : Supervisory Control and Data Acquisition
SDGs : Sustainable Development Goals
SGIP : Self-Generation Incentive Program
SLL : Sustainability-Linked Loan
TPU : Tensor Processing Unit
UPS : Uninterrupted Power Supply
VAEs : Variational Autoencoders

CHAPTER I

INTRODUCTION

Critical infrastructure refers to the physical and virtual systems, services, and assets that are essential for the functioning of a society, economy, or organization. Given this foundational role, we can consider that that CI is very essential for human life. Here after, I call critical infrastructure referring in the context of sectors. But if we look at the present situation, human life is transitioning to modernization. Reflecting on to this journey of human life, a question arises, what truly underpins modern life, the very fabric of our survival in an increasingly digital world? it's not just the algorithms and data of artificial intelligence (AI), but the often-unseen infrastructure (the data center) that makes it all possible. But are these data centers, the silent engines of our critical infrastructure sectors, truly ready for the AI revolution? Consider this: our energy grids, communication networks, water systems, and financial institutions – all essential for human survival – are now inextricably linked to these data hubs. As the Stanford Emerging Technology Review reminds us, AI is poised to transform our world, but this transformation hinges on data centers capable of handling unprecedented computational loads. So, the question becomes: how do we ensure these vital components of our critical infrastructure are not only powerful enough to support AI, but also resilient against threats, sustainable for the planet, and accessible to all? The challenge, then, is not just technological, but financial. This DBA thesis confronts this challenge head-on, exploring innovative financing strategies for modernizing data centers within these critical infrastructure sectors. By delving into this crucial intersection, I aim to safeguard the very foundations of our interconnected world, ensuring that the promise of AI enhances, rather than endangers, the essential services upon which we all depend.

1.1 Artificial Intelligence, Data Centers, and Critical Infrastructure Sectors

The rapid proliferation of artificial intelligence (AI) is driving an unprecedented surge in demand for data processing and storage, placing immense pressure on existing data center infrastructure. As these data centers become increasingly critical components of modern infrastructure sectors, ensuring their efficient, scalable, and sustainable operation is paramount. This thesis addresses the critical challenge of financing the modernization of these data centers to meet the demands of the AI era making the need for AI-ready data centers in the critical infrastructure sectors.

1.1.1 Artificial Intelligence

The evolution of Artificial Intelligence (AI) can be traced back to advancements in several enabling technologies, including computing power, machine learning, big data, cloud computing, open-source software, algorithms, and virtualization. What sets AI apart from these related technologies is its unique ability to learn, adapt, reason, and make decisions autonomously (Liu et al., 2022). Furthermore, AI exhibits capabilities such as managing uncertainty and noise, enabling interaction and collaboration, and performing representation and abstraction. While there is currently no universally accepted definition of AI, significant efforts are being made by researchers, governmental institutions, and industries to establish a standardized definition of its components. The challenge in achieving this standardization arises from the broad interpretation of AI, which encompasses not only intelligent technologies like smartphones and smart homes but also autonomous systems, such as self-driving cars and drones (Ćelić et al., 2024). Due to this lack of a uniform definition, existing literature often calls for studies and reviews that seek to expand the scope of frameworks, themes, and future research directions. However, an

attempt to define AI is offered by, who describes it as “an unnatural object or entity that possesses the ability and capacity to meet or exceed the requirements of the task it is assigned when considering cultural and demographic circumstances”

In recent years, cutting-edge AI research has brought notable advancements to critical information infrastructure protection (CIIP).

Generative AI

Generative AI models, particularly Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs), have shown the potential to transform CIIP by producing synthetic data to balance underrepresented cybersecurity scenarios (Pinto et al., 2023). Additionally, these models can simulate unexplored scenarios in predictive maintenance, aiding risk preparedness (Ćelić et al., 2024). Furthermore, GANs are being explored for generating attack samples to train robust models capable of defending against intrusions (Liu et al., 2022).

Representation Learning

Representation learning techniques simplify high-dimensional data into lower-dimensional latent spaces, allowing AI models to identify patterns and detect deviations effectively. For instance, VAEs have been used to establish baseline behavioural patterns in networks or software systems, with reconstruction errors providing insight into anomalous activities (Pinto et al., 2023).

Self-Supervised Learning

Self-supervised learning has gained prominence, especially in CIIs that generate large data volumes. By utilizing data-driven labelling methods, this approach eliminates costly

manual labeling processes. For example, researchers have utilized self-supervised learning to design privacy-preserving intrusion detection systems in 5G networks (Hossain et al., 2025) and for time-series analysis in detecting cyberattacks on water infrastructure systems (Mahmoud et al., 2022).

1.1.2 Data Centers

The significance of data centers is steadily increasing due to the development of 5G technology and the relentless expansion of the mobile phone market, with an estimated annual consumption growth rate of 5%. According to the International Energy Agency (IEA), global data center energy consumption reached approximately 460 TWh in 2022, accounting for about 2% of the world's total electricity usage. In the United States, data center energy consumption in 2014 comprised 1.8% of the country's total electricity use, amounting to nearly 70 billion kWh. The expanding use of artificial intelligence technologies and the cryptocurrency industry is projected to push data center energy consumption to 1,000 TWh by 2026. Efforts have been made by information and communication technology (ICT) companies to align with the 2015 Paris climate agreement, setting emissions reduction targets of 45% between 2020 and 2050. These reductions are primarily being pursued through energy efficiency improvements. Significant advances have been made in server power efficiency, with newer hard drive storage technologies reducing the number of physical drives required. Companies like Apple and Google have implemented energy-efficient infrastructure in their U.S. data centers, mitigating the increase in overall energy consumption despite the growing operational demand. Additionally, data centers are adopting green electricity, advanced heat management systems, and functional optimization to support global climate goals while enabling future growth in the ICT sector.

As the backbone of modern digital infrastructure, data centers are crucial for managing and processing the ever-increasing volume of digital data. These facilities power a vast array of applications, such as social media, e-commerce, scientific research, and cloud computing, thereby playing a vital role in contemporary digital economies. To meet their energy needs, some data centers generate electricity on-site, utilize co-location with nearby power plants, or secure renewable energy through agreements with third-party suppliers. However, data center energy consumption has continued to rise due to the demand for high reliability and increased digital transformation, particularly in the post-Covid-19 era. This has raised significant concerns regarding environmental sustainability and economic efficiency.

In response to these challenges, the industry is seeing a shift from smaller, localized data centers to larger, more energy-efficient, cloud-service-based facilities. Modern data centers have exhibited lower power usage effectiveness (PUE) values due to improved cooling technologies and more efficient power supply mechanisms. Success in addressing the growing energy consumption of data centers will depend on operators and engineers prioritizing innovations in energy efficiency, reducing carbon emissions, and maintaining high standards for performance and reliability. These strategies are critical not only for mitigating the environmental impact of data centers but also for ensuring the sustainability of the digital transformation and ICT ecosystem.

1.1.3 Critical Infrastructure Sectors

Critical infrastructure refers to the physical and virtual systems, services, and assets that are essential for the functioning of a society, economy, or organization. The most industrialized countries are equipped with increasingly extensive and sophisticated infrastructure systems, so-called critical infrastructures (CIs) such as energy distribution

networks and transport infrastructures. Critical infrastructures are, therefore, those material resources, services, information technology systems, networks and infrastructure assets that, if damaged or destroyed, would cause serious repercussions on the crucial functions of society, including the supply chain, health, security and the economic or social well-being of the state and the population. The term critical infrastructure is defined in Section 1016(e) of the USA Patriot Act of 2001 as those “systems and goods, both physical and virtual, so vital to the nation that their malfunctioning or destruction would produce a debilitating impact on the security of citizens, on the economic security of the nation, on national public health and on any combination of the above” (USA Patriot Act, 2001). Europe has also issued its own CIs protection program. In fact, in June 2004, the European Council took the initiative to call for the preparation of a strategy for the protection of CIs in the territory of the Union from possible terrorist attacks, which led the Commission to issue Communication 702 of 2004. This activity of the Commission led in 2008 to the approval of Directive 2008/114/EC which currently forms the basis of EU legislation on CIs. A CI is defined in the directive as “an element, system or part thereof located in the Member States which is essential for the maintenance of the vital functions of society, the health, safety and economic and social well-being of citizens and whose damage or destruction would have a significant impact in a Member State due to the impossibility of maintaining those functions” (EU EU legislation on CIs).

The Directive aims to establish a European Union (EU) process for identifying and designating European critical infrastructure (ECI), as well as an approach to improve their protection. To this end, EU countries must use cross-cutting criteria such as possible losses, economic effects and effects on citizens and sectoral criteria specific to the type of ECI of course, EU countries regularly review the identification and designation of ECIs.

According to the Australian Cyber and Infrastructure Security Centre Critical infrastructure is defined as: “those physical facilities, systems, assets, supply chains, information technologies, and communication networks which, if destroyed, degraded, compromised or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of Australia as a nation or its states or territories, or affect Australia’s ability to conduct national defense and ensure national security”.

1.2 Need for Modernizing Critical Infrastructure Sectors

Critical infrastructure systems are increasingly vulnerable to a wide range of physical and cyber threats that can compromise essential services, destabilize societal functions, and negatively impact safety and security. These threats target both Information Technology (IT) and Operational Technology (OT) systems, with the intent to steal sensitive data, disrupt operations, cause physical harm, or manipulate critical processes. IT systems are primarily concerned with data management, processing, and communications, while OT systems monitor and control physical processes through components such as sensors, actuators, and control systems. The convergence of IT and OT environments, compounded by growing interconnectivity, has created additional attack surfaces, making the protection of both systems essential yet increasingly complex. Below, specific examples of IT and OT threats are outlined to highlight the breadth and severity of challenges facing critical infrastructure sectors.

1.2.1 IT Threat Examples

Cyberattacks on IT systems can lead to serious consequences, ranging from unauthorized data access to the disruption of essential services. Attackers often seek to exploit IT systems

of critical infrastructure to steal sensitive data, disrupt financial activities, or damage organizational reputations. Examples of such threats include:

Example – 1 Data Theft: Breaches involving IT systems can result in the exposure of sensitive information such as customer data, financial records, or intellectual property. For instance, a cyberattack on a financial institution could not only lead to fraudulent activities but also cause the loss of consumer information, with subsequent regulatory penalties and reputational damage.

Example – 2 DoS and DDoS Attacks: Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are common methods used to overwhelm IT infrastructure, rendering services unavailable. Such disruptions could paralyze critical systems, affecting healthcare, banking, or energy supply chains.

Example – 3 Ransomware Attacks: Ransomware remains one of the most prevalent and damaging threats, as it encrypts organizational data and demands payment for its release. These attacks lead to operational disruptions, financial losses, and compromised data integrity, impacting industries regardless of their size or nature.

Example – 4 Social Engineering: Techniques such as phishing often deceive employees into disclosing login credentials or unintentionally downloading malicious software. Ransomware and other forms of malware are commonly delivered through social engineering strategies such as fraudulent emails, further compromising critical IT infrastructures.

Example – 5 SQL and Code Injection Attacks: SQL injection and code injection attack vectors exploit vulnerabilities in web applications and databases. These methods allow attackers to gain unauthorized access to sensitive data, alter records, or compromise application functionality.

1.2.2 OT Threat Examples

The rise of network-connected OT systems has exposed critical infrastructure to unique cyber threats that extend beyond data breaches, often resulting in direct physical consequences. OT systems, including Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS), and Programmable Logic Controllers (PLCs), are vital for the operation of critical infrastructure. Unlike IT threats, attacks targeting OT systems aim to manipulate physical processes or cause operational disruptions, with potentially devastating impacts.

Example – 1 Disruption of Control Systems: Cyberattacks on transportation system control mechanisms, for example, can lead to accidents, disruptions in traffic control, or logistical failures. By targeting OT systems, attackers aim to manipulate control processes and create large-scale operational chaos.

Example – 2 Attacks on SCADA Systems: SCADA systems, essential for real-time monitoring of critical processes, are vulnerable to attacks such as DoS. These attacks can lead to catastrophic system failures where physical machinery loses control, endangering public safety (Fovino et al., 2009; Nazir and Patel, 2017)

Example – 3 Malware Attacks: Malicious software poses a significant threat to critical OT environments. For example, malware can infiltrate SCADA networks or PLC components, undermining their functionality. Modern-day malware, including advanced threats like zero-day attacks, can bypass conventional defenses, compromising individual components in ICS networks.

Example – 4 PLCs and Memory Corruption: Programmable Logic Controllers, essential for automation, face vulnerabilities such as memory corruption and control-flow hijacking. These vulnerabilities allow attackers to execute unauthorized commands or cause unexpected shutdowns of critical systems (Spenneberg et al. 2026; Achiam et al., 2023)

Example – 5 Ransomware Worms in OT Systems: Spenneberg et al. (2026) demonstrated that ransomware worms targeting PLCs could provide attackers with persistent backdoors into SCADA networks. Once inside, attackers could spread malware across the network to disrupt multiple components at once.

Example – 6 Exploitation of Human-Machine Interfaces (HMIs): Human-Machine Interfaces, which act as the bridge between operators and OT devices, are also prone to exploitation. Cybercriminals can leverage web-based vulnerabilities such as SQL injection or Cross-Site Request Forgery (CSRF) attacks to compromise these interfaces (Achiam et al., 2023)

Example – 7 Sophisticated Attacks and Taxonomies: Emerging threats, such as zero-day exploits, highlight the dynamic and evolving nature of OT network vulnerabilities. Studies

by Kayan et al. 2022 have further categorized these intrusions into organized taxonomies, emphasizing their complexity and sophistication.

Example – 8 Lifecycle of Attacks on Critical Infrastructure: Maglaras et al. (2018) outlined various stages of cybersecurity incidents affecting critical infrastructure, ranging from prediction and prevention to detection and incident response. These stages demonstrate the importance of rule-based models that integrate real-time monitoring, proactive defenses, and rapid incident mitigation.

1.3 Role of AI and Other Digital Tools in Critical Infrastructure Sectors Modernization

1.3.1 AI in CIS

Mitigating Human Vulnerabilities with Pattern Recognition and Behavioral Biometrics

Human vulnerabilities are frequently exploited in critical information infrastructure (CII), often through unauthorized access to sensitive data. To address this, AI demonstrates significant potential in detecting anomalies in user behavior. By leveraging AI, organizations can develop user-specific behavioral patterns, often referred to as user "signatures," based on consistent device usage habits over time. These unique patterns allow the detection of unusual activities, which could signal unauthorized access attempts. Techniques like learning automata have previously been used in cloud computing to anticipate resource usage based on historical data (Rahmanian et al., 2018). Similar techniques could be applied to model individual behavioral signatures in network settings, identifying deviations as potential red flags. Recent advancements in behavioral biometrics also support this domain. For example, Siamese neural networks have been employed to

separate legitimate users from intruders effectively. This is achieved by converting data, such as keystroke dynamics, into formats suitable for training deep neural networks, as demonstrated by Budžys et al. (2023). Such implementations suggest a promising direction in using pattern recognition to secure critical systems.

Utilizing Machine Learning to Detect Malware and Ransomware

AI's role in malware and ransomware detection within CII systems is an area of robust research, increasingly supported by the availability of comprehensive malware datasets. These datasets, such as Critical Infrastructure Ransomware Attacks (CIRA) (Rege & Bleiman, 2023) and SOREL-20M (Harang & Rudd, 2020), enable benchmarking and refining detection techniques. A notable AI approach involves analyzing Control-Flow Graphs (CFGs), which unveil every execution flow in a program, thereby exposing malware fingerprints (Esmaeili et al., 2024). While traditional machine learning techniques may struggle with graph-based data, emerging methods like Graph Neural Networks (GNNs) (Wu et al., 2021) overcome these limitations, offering new solutions to malware detection in CII.

Automating Vulnerability Assessment for Unpatched Risks

Vulnerability management in CII systems is critical, particularly when addressing unpatched security gaps. AI's ability to automate tasks like intelligence gathering, threat investigation, and vulnerability assessments makes it a valuable tool for these challenges. AI-driven tools can evaluate vulnerabilities by assigning severity levels, enabling practitioners to prioritize patches based on their potential impact on system downtime (Sarker, 2024). Despite these advancements, it is important to note that human oversight remains indispensable. AI systems should function as assistive technologies that optimize

human efforts by increasing accuracy and reducing errors, as highlighted by Saadallah et al. (2024).

Strengthening Supply Chain Security with Predictive Analytics and Blockchain

AI's predictive capabilities hold significant value in securing the supply chains of CII. By monitoring the behavior of third-party software or hardware, AI can detect potentially malicious activity within supply chains, providing a layer of security (Sarker, 2024). Blockchain technology has also emerged as a complementary solution, as it ensures transparency and traceability across supply chains (Govea et al., 2024; Marjanović et al., 2021). The integration of AI and blockchain, recommended by various researchers (Sarker, 2024; Charles et al., 2023), could revolutionize supply chain security through greater collaboration between these technologies.

Detecting DDoS Attacks Using Machine Learning

Distributed Denial of Service (DDoS) attacks continue to threaten CII systems. AI approaches, particularly machine learning techniques, provide effective tools for identifying such attacks by differentiating between normal and anomalous traffic patterns. Datasets like WUSTL-IIoT-2021 (Zolanvari et al., 2021) and NSL-KDD (Tavallaei et al., 2009) are commonly used to train machine learning models designed for detecting DDoS activities. Notable algorithms such as support vector machines (Panagiotis et al., 2021), convolutional neural networks (Hussain et al., 2021), and long short-term memory networks (Saheed et al., 2023) have yielded promising results. These models not only detect anomalies but also enable automated responses, reducing the operational burden.

Addressing Zero-Day Exploits Using AI-Driven Anomaly Detection

Zero-day exploits constitute one of the most challenging threats in cybersecurity due to the lack of prior knowledge about the vulnerabilities they exploit. AI provides a potential safeguard by using anomaly detection models that learn the normal behavior of systems and recognize deviations, which could signal an attack. Beyond anomaly detection, AI enhances proactive measures such as automating threat intelligence collection and incorporating self-updating risk models capable of adapting to evolving threats (Sarker, 2024).

1.3.2 Blockchain in CIS

The spectrum of cyber-attacks, ranging from data breaches to acts of physical sabotage, underscores the inherent weaknesses within traditional cybersecurity measures when tasked with safeguarding intricate and highly interconnected systems. These vulnerabilities highlight the inability of legacy defenses to address the complexity of contemporary cyber-threats effectively. In response to these shortcomings, blockchain technology has gained prominence as a credible alternative, characterized by its key features of transparency, immutability, and a strong resistance to tampering or unauthorized alterations. Such characteristics reinforce blockchain's potential to shift the paradigm for securing critical infrastructure against increasingly sophisticated cyber-attacks.

Despite its high potential, blockchain implementation is not without significant hurdles. Critical challenges such as scalability limitations, the lack of seamless interoperability between various blockchain networks, and difficulties in adhering to existing regulatory requirements present substantial obstacles to its wider adoption. Addressing these issues calls for a collaborative framework where technology developers, regulators, and critical infrastructure operators converge to design solutions that balance technical robustness, scalability, and regulatory compliance. This collaborative effort is

crucial to harness the full potential of blockchain in safeguarding critical infrastructure while ensuring that its implementation remains both practical and compliant with legal standards.

1.4. Research Gaps in AI- and Blockchain-Based Security for CIS

The convergence of artificial intelligence (AI) and blockchain technology in securing critical infrastructure (CI) systems has gained significant attention across academic and industrial sectors. Both technologies have shown notable potential in addressing modern cybersecurity challenges. While AI enhances detection and response capabilities through advanced data analytics and pattern recognition, blockchain provides a secure, immutable, and decentralized framework to safeguard data exchanges and system integrity. However, despite these advancements, several research gaps persist that hinder the full implementation and effectiveness of AI- and blockchain-based solutions for CI cybersecurity. These gaps are categorized below into AI-specific, blockchain-specific, and combined research challenges.

1.4.1 AI-Specific Research Gaps

Data Availability and Quality

AI models necessitate extensive, high-quality datasets to accurately differentiate between malicious and legitimate behaviors. The scarcity of open-source, up-to-date datasets tailored to modern attack vectors creates a significant challenge, as most available datasets have outdated feature spaces. Moreover, the use of low-quality data during model training can result in misclassifications and reduced cybersecurity performance in CI systems. Research is needed to create comprehensive, real-time, and context-specific datasets applicable to the complex landscape of critical infrastructure.

Model Complexity and Overfitting

The complexity of AI models and their tendency to overfit training data remain major bottlenecks. Advanced techniques such as deep learning (DL) often act as "black-box" models, making it difficult to understand and debug their decision-making processes. Overfitting worsens the situation by compromising a model's ability to generalize to unseen data. These issues are particularly pronounced in CPS environments, where system intricacies limit the ability of models to address uncommon behaviors or novel cyber threats.

Scalability

CIs handle massive volumes of real-time data, which AI models must process efficiently to meet operational demands. However, as these systems scale, they become increasingly complex, and their AI-driven solutions may face difficulty simultaneously managing performance, speed, and security. Future research should align AI optimization techniques to meet the growing demand for scalability in CI systems while ensuring robustness against attacks.

Transparency and Explainability

The lack of logic transparency in many AI models, particularly DL, poses challenges in CI settings where decision accountability is crucial. Operators need to understand how AI systems produce their outputs, especially in mission-critical environments. Research into explainable AI (XAI) is vital to improve interpretability and transparency, thereby fostering trust and usability.

Resiliency and Adaptability

Modern cyber threats evolve rapidly, requiring AI systems to be both resilient and adaptable to changing attack patterns. However, many current AI-based security solutions lack the flexibility to keep pace with new threats or recover from disruptions effectively. Systems capable of dynamic adaptation and self-correction must be a priority for future research

1.4.2 Blockchain-Specific Research Gaps

Scalability and Performance Bottlenecks

Blockchain networks face inherent scalability challenges due to their reliance on consensus mechanisms, which, while secure, significantly limit transactional speeds (e.g., Bitcoin processes approximately 7 transactions per second). In the context of CI systems, which require high-volume, real-time data exchanges, this inefficiency becomes a substantial barrier. Research is required to develop scalable blockchain architectures with optimized consensus algorithms that can meet the high-speed demands of CI environments

Interoperability with Legacy Systems

Critical infrastructure systems possess a wide array of legacy technologies that are deeply ingrained in their operations. Integrating blockchain with such systems presents technical challenges, as many legacy architectures are not designed for decentralized frameworks. Future research should develop blockchain adapters, middleware, and translation layers to facilitate smoother integration without requiring significant overhauls of legacy CI systems.

Energy Consumption and Resource Efficiency

Many blockchain networks, particularly those utilizing proof-of-work (PoW) consensus mechanisms, consume significant energy. This inefficiency makes applying blockchain to energy-intensive CI systems, such as electrical grids or water distribution systems, less viable. Research is needed to replace traditional consensus mechanisms with energy-efficient alternatives like proof-of-stake (PoS) or new hybrid consensus strategies tailored to CI requirements.

Data Privacy and Confidentiality

While blockchain ensures data immutability and transparency, these features can inadvertently lead to privacy concerns. Sensitive CI data, once stored in a blockchain, becomes accessible to authorized stakeholders but remains immutable, raising questions about regulatory compliance (e.g., GDPR in Europe) in scenarios requiring data deletion or redaction. Research must explore privacy-preserving solutions such as zero-knowledge proofs or hybrid architectures that balance data accessibility with confidentiality

Governance and Regulatory Compliance

The decentralized nature of blockchain, while advantageous for resilience, creates ambiguities in governance and accountability. Critical sectors (e.g., healthcare, energy) necessitate compliance with sector-specific regulations and legal frameworks, but standard governance models for blockchain systems are underdeveloped. Developing regulatory-compliant blockchain frameworks for CI is an urgent research need.

Trust Mechanisms and Security Frameworks

Blockchain solutions in CI environments must incorporate robust mechanisms to manage trust among diverse stakeholders, such as regulators, operators, and maintenance personnel. While blockchain provides inherent security via decentralization, it remains vulnerable to targeted attacks such as 51% attacks, Sybil attacks, and smart contract vulnerabilities. Further research is required to enhance blockchain-specific security frameworks to address these advanced threats.

1.4.3 Combined Research Gaps (AI and Blockchain Integration)

Data Sharing and Interoperability

The integration of AI and blockchain has the potential to facilitate secure and transparent data sharing among CI entities. However, ensuring seamless interoperability between AI-driven cyber-defense mechanisms and blockchain's decentralized infrastructure is a challenge. Research should focus on hybrid architecture that enable data sharing in real time while preserving the security and integrity of sensitive CI data.

Scalable AI-Blockchain Ecosystems

Combining blockchain's security with AI's analytical power in CI generates significant computational overhead and raises concerns about scalability. Creating lightweight, specialized AI-blockchain ecosystems that can operate efficiently under the data-intensive demands of CI systems is a critical research direction.

Explainability for Blockchain AI Decisions

When AI is implemented alongside blockchain in CI, the lack of transparency is compounded. While AI models require explainability, blockchain adds another layer of complexity due to the immutability and decentralization of its operations. Developing

explainable AI-integrated blockchain systems that provide both interpretability and auditability is essential.

Dynamic Adaptive Systems

Both AI and blockchain, when applied together, need to ensure adaptability to emerging threats and resilience to system failures. AI alone may adapt through improved training but ensuring blockchain-led adaptability in practices such as consensus reconfiguration or smart contract updates is largely unexplored. Further research is required to enable dynamic adaptability in combined AI-blockchain systems.

Energy and Resource Constraints

The integration of blockchain and AI in CI, especially in energy-intensive sectors, presents overlapping challenges related to computational energy use. Further research should focus on energy-efficient frameworks that optimize both blockchain operations and AI computations without compromising security.

1.4 Research Problem

Though the explored research gap is quite broad, I narrowed down the focus of this thesis to a system level, with an aim of enabling the data centers with all the features and make them designed for AI era. The exponential growth of artificial intelligence (AI) is placing unprecedented demands on data center infrastructure. Existing data centers, often designed for traditional computing workloads, are struggling to meet the performance, scalability, and energy efficiency requirements of AI applications. This necessitates a significant wave of data center modernization, involving the adoption of advanced technologies such as However, the modernization of data centers to support AI workloads requires substantial

financial investment. Traditional financing models may not be adequate to address the unique challenges and opportunities associated with these projects, particularly in the context of increasing environmental concerns and the need for sustainable infrastructure development. Specifically, the research problem lies in the lack of a clear understanding of how sustainable finance instruments can be effectively utilized to finance the development and modernization of AI-ready data centers.

1.5 Goal, Research Questions and Objectives

The goal of this thesis is to have a comprehensive understanding of how sustainable finance instruments can be effectively utilized to finance the modernization of data centers to meet the growing demands of artificial intelligence (AI) within critical infrastructure sectors, while simultaneously promoting environmental sustainability and responsible investment.

This goal led to the overall thesis research question has,

“how can sustainable finance instruments be strategically deployed to finance the development and modernization of data centers (this I call as AI-ready data centers) within critical infrastructure sectors, balancing the increasing demands of artificial intelligence with the imperative for environmental sustainability and responsible investment?”

Having formulated the overall thesis research question, for further simplification of the work for better organization in this thesis, I have constructed multiple research questions which provides systematic outcome, and under each research question I constructed, two objectives were considered. They are as follows:

Research Question 1 (RQ – 1)

How is the increasing demand for AI impacting the operational requirements and resource consumption of existing data centers?

Objective 1: Quantify the increase in energy consumption and resource utilization.

Objective 2: Identify the specific operational challenges.

Research Question 2 (RQ – 2)

What are the key sustainability challenges associated with meeting the growing AI demand within data centers, and how can modernization efforts mitigate these challenges?

Objective 1 - Assess the environmental impact

Objective 2 - Evaluate the potential of specific modernization strategies

Research Question 3 (RQ – 3)

What are the projected future demands of AI on data center infrastructure, and what are the implications for financing needs?

Objective 1 - Data center capacity and resource requirements driven by AI applications

Objective 2 - Estimate the financial investment required to meet the projected AI-driven demand for data center infrastructure, considering both capital expenditures (CAPEX) and operational expenditures (OPEX).

Research Question 4 (RQ – 4)

What types of sustainable finance instruments are most suitable for financing the modernization of AI-ready data centers?

Objective 1 - Identify and analyze a range of sustainable finance instruments (e.g., green bonds, sustainability-linked loans, green revolving credit facilities) that could be applied to data center modernization projects.

Objective 2 - Evaluate the suitability of each instrument based on factors such as cost of capital, investor appetite, and alignment with environmental, social, and governance (ESG) goals.

Research Question 5 (RQ – 5)

What modifications or innovations to existing sustainable finance instruments are necessary to effectively address the unique requirements of data center modernization projects?

Objective 1 - Identify the specific barriers or limitations of existing sustainable finance instruments

Objective 2 - Propose potential modifications or innovations to these instruments

Research Question 6 (RQ – 6)

What are the potential risks and rewards associated with utilizing sustainable finance instruments for data center modernization, and how can these be effectively managed?

Objective 1 - Assess the potential financial risks

Objective 2 - Develop risk mitigation strategies and identify potential rewards

Research Question 7 (RQ – 7)

What are the key lessons learned from existing case studies of data center financing and modernization projects, and how can these be applied to future initiatives?

Research Question 8 (RQ – 8)

How do regional variations in regulatory frameworks, market conditions, and technological advancements impact the effectiveness of different sustainable financing models for data center modernization?

Research Question 9 (RQ – 9)

Based on the analysis of case studies and regional data, what are the key research propositions that can be formulated to guide industry adoption of sustainable financing strategies for AI-ready data centers?

1.6 Thesis Structure and Overview

This thesis is structured into five chapters;

- Following this introductory chapter (i.e., Chapter 1), which establishes the context, research problem, and objectives, the thesis proceeds as follows:
- In chapter 2, Research Design and Approach provided, which outlines the methodological framework employed to address the research questions.along with financial feasibility score for different financial routes specific to USA, australia, and european union.
- Chapter 3 presented the Findings and Analysis especilly the core findings for all the research questions as per the objectives.
- Discussion and Recommendations in the context of AI ready data centers in CIS is provided in chapter 4, which interprets the findings in the context of critical infrastructure resilience. This chapter also provides the integration of ai-ready data centers and financing routes for each critical infrastructure sectors consdering USA, australia, and european union.

- Finally, in chapter 5, Conclusions and Business Implications are summarized along with limitations and future research suggestions.

CHAPTER II

RESEARCH DESIGN AND METHODOLOGY

2.1 Theoretical Framework

This thesis is grounded on an interdisciplinary theoretical framework that integrates perspectives from three key domains: Artificial Intelligence (AI), data center infrastructure, and critical infrastructure sectors (CIS). The framework is structured around three major pillars: (1) Understanding the foundational technologies and concepts, (2) Investigating the modernization needs of CIS and the role of advanced digital tools, and (3) Evaluating traditional vs. AI-ready data centers, particularly their role in CIS resilience. These pillars converge to address eight research questions aimed at uncovering insights into sustainable financing strategies for AI-ready data centers and their implications for safeguarding critical infrastructure.

2.2 Research Design and Methodology

This study adopts a literature review methodology, leveraging secondary data to analyze sustainable financing strategies for AI-ready data centers within critical infrastructure sectors. A literature review is particularly suitable for this research due to its ability to synthesize existing knowledge, identify research gaps, and assess diverse perspectives on a rapidly evolving subject area. By focusing on secondary data, this approach enables the aggregation of insights from multiple disciplines, including finance, technology, climate change, and public policy, which are all essential to understanding the interplay between sustainable financing and AI-driven infrastructure modernization. The study follows an integrative literature review design, aimed at providing a comprehensive understanding of

sustainable financing models and their role in supporting AI-ready data centers. The design focuses on both theoretical frameworks and applied industry practices. Through this approach, the research assesses the potential of financial tools such as green bonds, Energy-as-a-Service (EaaS) models, public-private partnerships (PPPs), and carbon pricing, while also highlighting the operational challenges of AI-related resource consumption, environmental sustainability, and resilience building. To ensure a rigorous and transparent review process, the research methodology is structured along the following stages:

Stage -1 : The Scope Definition, here the primary areas of investigation were chosen based on their relevance to the topic. These include,

- AI-ready data center infrastructure and energy consumption trends
- Sector-specific sustainability challenges and resilience requirements for critical infrastructure.
- Emerging financial instruments tied to green and sustainable financing.
- Regional differences in regulatory and policy frameworks related to these themes.

Stage -2 : Search and Retrieval of Relevant Literature, here a systematic search for academic, institutional, and industry literature was conducted across multiple databases, including Google Scholar, ScienceDirect, and government or private institution repositories. Specific keywords such as "AI-ready data centers," "sustainable financing," "critical infrastructure," "green bonds," "Energy-as-a-Service," "public-private partnerships," and "resilience in AI systems" were used to narrow the scope of search results. Additionally, government policy documents and white papers from leading technology companies and financial institutions were included to capture real-world applications and examples.

Stage -3 : Selection Criteria, here the inclusion and exclusion criteria ensured the selection of high-quality and relevant studies while minimizing bias.

Table 2.1. Criteria applied for secondary data collection

Criteria	Keypoints
Inclusion Criteria	-Peer-reviewed journal articles, industry reports, and white papers published in the last 10 years (with exceptions for seminal works). -Data and reports specifically focusing on critical infrastructure sectors (energy, healthcare, etc.) or AI-driven data centers. -Sources discussing sustainability and resilience financing mechanisms.
Exclusion Criteria	-Generalized research that did not apply findings to critical infrastructure or AI systems. -Non-English language studies (due to time and resource constraints).

Stage - 4 : Data Synthesis and Analysis, here a thematic analysis method was utilized to synthesize data and identify key themes emerging from the reviewed literature. This process involved reading and categorizing findings into broad thematic areas such as energy requirements, water requirements, cooling systems, e-waste, sustainability financing models, environmental sustainability, operational resilience, and regulatory frameworks.

2.3. Multi-Criteria Decision Analysis (MCDA) Framework

I employed a robust multi-criteria decision analysis (MCDA) framework to evaluate the feasibility of financing AI-ready data centers across the 16 U.S. Critical Infrastructure Sectors (CIS). The methodology was designed to integrate sector-specific operational requirements, regulatory constraints, sustainability considerations, and financial alignment for each sector. To provide actionable recommendations, feasibility scores were assigned, ranging from 1 to 10, to indicate the suitability of each financing mechanism for sector-specific AI-ready infrastructure. Below, the steps taken to compute feasibility scores are detailed. The MCDA-based methodology uses a weighted scoring system, where sector-financing combinations were evaluated against multiple criteria relevant to their practical application and alignment with sustainability principles. The final score for each combination reflects the aggregate performance of a financing mechanism across critical dimensions, ensuring a systematic and multidisciplinary assessment. To comprehensively evaluate financing mechanisms, five key criteria were selected, each representing a critical factor influencing the feasibility and effectiveness of implementing AI-ready data centers.

Table 2.2. The relative importance of each criterion represented as criteria weightage in %

Criteria	Criteria weightage (%)		
	USA	Australia	European Union
Sectoral Alignment	30%	30%	30%
Scalability and Funds Availability	20%	25%	25%
Government and Regulatory Backing	20%	20%	20%

Investor and Public Sentiment	15%	15%	15%
Execution and Risk Tolerance	15%	10%	10%

To standardize evaluation, each sector-financing combination was assigned scores on a 1-to-10 scale, where:

- 1-3 Poor feasibility due to barriers such as high complexity, misalignment, or limited scalability.
- 4-6 Moderate feasibility, with partial alignment but challenges in execution or funding adequacy.
- 7-8 High feasibility, offering strong alignment and scalability, with minimal regulatory or execution challenges.
- 9-10 Exceptional feasibility with nearly perfect alignment, broad support, and scalability across the sector.

The final feasibility score (S_f) was calculated using a weighted average as follows:

$$S_f = \sum_{i=1}^N (C_i \times W_i)$$

where C_i : Score on criterion i . W_i : Weight of criterion i . N : Total number of criteria (5 in this case).

The scoring process was conducted in four methodical steps:

Step - 1: Literature Review (included along with section 2.2) and Regulatory Analysis

A comprehensive review of industry reports, regulatory documents, peer-reviewed papers, and government policies was conducted to identify financing mechanisms relevant to critical infrastructure sectors. This step ensured that funding routes reflected current market trends and policy support.

Step - 2: Criteria-Wise Evaluation for Each Sector

Each financing mechanism was individually scored based on its sectoral alignment, scalability, government support, public sentiment, and execution likelihood. Qualitative and semi-quantitative insights were derived from sector-specific operational and regulatory contexts.

Step - 3: Weighted Aggregation

Scores for each criterion were aggregated using a weighted scoring system, with higher weights assigned to sectoral alignment (30%) and scalability (20%), reflecting their critical importance for successfully implementing AI-ready infrastructure.

Step - 4: Sector-Specific Insights and Feasibility Interpretation

Feasibility scores were interpreted sector by sector, combining aggregated results with qualitative insights. Recommendations were developed to align financing routes with the unique challenges and opportunities in each sector.

CHAPTER III

FINDINGS AND ANALYSIS

This chapter presents the research finding and the analysis of AI-ready data centers as per the research questions formulated. First, I observed quite a few differences in terms of traditional data centers and AI-ready data centers. If we closely look at the observations, the AI data centers differ significantly from traditional data centers in how they are designed, equipped, and operated, as outlined in *Figure 3.1*. While traditional data centers primarily manage general-purpose tasks like web hosting, database storage, and computing, AI data centers are purpose-built to handle the demanding requirements of AI workloads, such as training and deploying complex machine learning models.

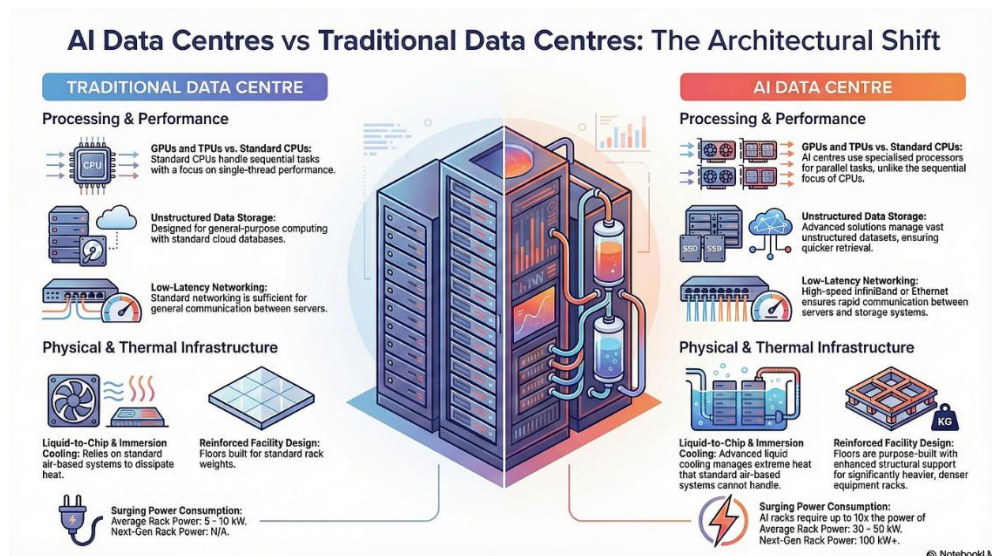


Figure 3.1. Architectural shift between the traditional data center and AI ready data center. Adopted Illustration from Medium, 2026 (Note: it was generated by the authors who wrote article on Medium using Notebook LLM)

These data centers depend heavily on advanced GPUs and TPUs for high-performance parallel computations. Moreover, AI workloads demand high-density server racks with power consumption levels far exceeding those in conventional setups, necessitating innovative cooling mechanisms like liquid cooling systems. Networking infrastructure in AI data centers is also superior, focusing on delivering low-latency and high-throughput connections required for distributed AI models. Such differences underline the evolution of data center architecture to accommodate AI's specialized computational and resource needs, setting them apart from traditional centers.

3.1 AI Ready Data Center

It is observed that, the AI-ready data centers fundamental components include IT hardware, electrical power systems, cooling technologies, and other essential supporting infrastructure. A typical architectural layout demonstrating how these components interconnect is illustrated in *Figure 3.2*.

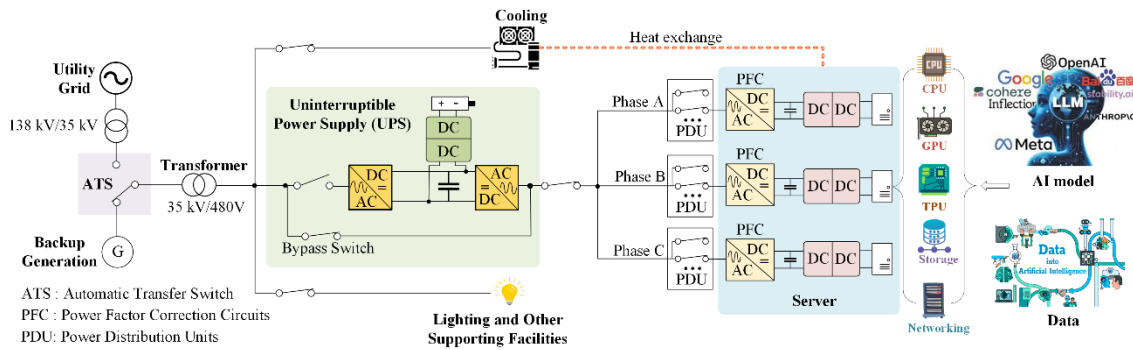


Figure 3.2. Architectural layout of the AI ready data center. Adaopted Illustration from Reference Xin et al. 2025.

The IT hardware infrastructure forms the central computational framework for AI data centers, comprising systems designed for computing, storage, and networking. These systems are responsible for managing large-scale AI model training, handling massive

datasets, and supporting high-speed communication between units. AI-driven workloads, especially large language model (LLM) training and inference, require powerful computational clusters capable of handling complex operations efficiently. Such clusters are built using high-performance multi-core CPUs combined with GPUs and TPUs, configured densely within server racks. These servers are organized in standardized racks to enable scalability, power distribution, and efficient thermal management. Unlike traditional data centers, which distribute lower levels of processing power across racks, AI-focused data centers house much higher processing power per rack. While conventional data center racks typically consume 7-10 kW, AI racks demand up to 30 kW and, in specialized cases, even exceed 100 kW. For instance, NVIDIA's GB200 NVL36 and NVL72 servers have power requirements of 66 kW and 120 kW per rack, respectively. Such high power densities introduce significant challenges in power delivery and heat dissipation. To complement the intense computational requirements of AI, scalable and high-speed storage solutions are essential to handle vast training datasets, intermediate checkpoints, and data required for inference. AI data centers employ tiered storage architecture consisting of three main categories: (i) the hot tier, utilizing NVMe SSD arrays for low-latency, high-bandwidth access to active data, (ii) the warm tier, which relies on high-capacity HDDs for economical storage of less frequently accessed data, and (iii) the cold tier, designed for archiving long-term storage data using tape drives or object storage systems. Distributed file systems, like Lustre and Ceph, along with object-based storage, play an integral role in enabling large-scale parallel read and write operations. In stark contrast to general-purpose data centers, which optimize cost and capacity, AI-focused storage systems prioritize throughput and simultaneous data access to ensure that high-speed computational resources, such as GPUs, are never idle due to delayed data loading. High-performance networking systems are indispensable in AI workloads to facilitate the

flow of massive datasets between compute nodes and storage systems. AI data centers employ specialized intra-node connections, such as NVIDIA NVLink, which supports high-speed GPU-to-GPU communication, and inter-node networks, such as InfiniBand or RDMA-enabled Ethernet, which offer low-latency, high-bandwidth connectivity between servers and racks. Advanced network topologies like fat-tree and dragonfly are frequently implemented to optimize communication in distributed AI training environments. In general-purpose data centers, networking systems are tailored for broad-spectrum workloads, which makes them less demanding in terms of bandwidth and latency compared to AI-specific designs.

AI data centers typically source electricity from medium- or high-voltage grids, depending on their size and capacity. In the case of hyperscale facilities, direct connection to the transmission grid is common. These distribution voltages range between approximately 13.2 kV for smaller installations and upward of 115-230 kV for larger facilities with energy demands exceeding 100 MW. AC power is routed into the data center through high-voltage switchgear, which includes safety and protective mechanisms, before being converted to operational voltages, often 480 V, through step-down transformers. These transformers also provide insulation between the grid and internal systems. The power is distributed further through panels and PDUs to feed IT equipment, cooling systems, and other subsystems. For IT operations, the alternating current (AC) is transformed into stable, regulated direct current (DC) via rectifiers and DC-DC converters. Large-scale AI data centers enhance reliability by employing redundant utility connections and on-site transformers to ensure consistent operations during partial grid outages. An Uninterruptible Power Supply (UPS) system provides protection against any interruptions in power delivery by instantly supplying electricity from energy storage units like batteries or flywheels. These systems ensure the seamless continuation of operations during the brief

transition before backup generators activate. UPS systems are predominantly equipped with technologies such as VRLA batteries, lithium-ion batteries, or advanced solid-state chemistries. The selection of UPS technology depends on parameters like energy density, thermal design, operational costs, and lifecycle performance. AI-focused UPS deployments are tailored to support high-power rack configurations and operate in modes such as normal, double-conversion, or battery mode. Additionally, modern UPS systems facilitate grid interaction, extending their utility by participating in grid demand-response programs. Backup generators act as failsafe mechanisms, providing emergency power during outages. Diesel generators remain a popular choice for their ability to deliver reliable power at scale, while an increasing number of facilities are supplementing these with renewable technologies, such as solar panels or hydrogen fuel cells, to enhance sustainability. For instance, hydrogen fuel cells demonstrated reliability in operational trials by running data centers for up to 48 hours continuously. Backup systems often integrate automatic transfer switches, enabling their activation within seconds of detecting grid failure, ensuring uninterrupted operations.

Cooling technologies are indispensable for dissipating the immense heat generated by high-density AI hardware. Traditional air-cooling methods, while cost-effective, are quickly rendered insufficient as rack power densities exceed 20 kW. To meet AI requirements, liquid cooling solutions—such as immersion cooling and direct-to-chip liquid cooling—are being adopted due to their superior thermal management capabilities. Hybrid cooling strategies, which combine elements of air and liquid cooling, offer a flexible and energy-efficient alternative, balancing the initial deployment costs with operational benefits.

AI data centers also include various support systems critical for ensuring reliable and secure operations. These include physical design optimizations, such as hot/cold aisle

containment and robust cabling systems, environmental monitoring platforms integrated with fire detection systems, and multi-factor secure access protocols. Auxiliary systems, including redundant network links, water treatment for cooling systems, and energy-efficient lighting, further contribute to operational efficiency.

3.2 For RQ-1: Impact of AI Demand on Data Center Operations

This section presents the findings related to the impact of increasing AI demand on the operational requirements and resource consumption of existing data centers.

3.2.1 Energy Consumption and Resource Utilization

Energy consumption: The energy consumption is usually measured with an efficiency parameter by calculating the Power Usage Effectiveness (PUE), which is the standard, industry-accepted metric for measuring data center energy efficiency. It is the ratio of total facility power to IT equipment power, Eq. (3.1.) provides the calculation model.

$$PUE = \frac{E_{tf}}{E_{ITe}}$$

where, E_{tf} is the energy consumption of the total data center facility, E_{ITe} is the energy of information technology (IT) equipment within the data center facility.

A lower PUE, closer to 1.0, signifies higher efficiency. The ideal ratio A PUE of 1.0 indicates 100% of power goes to IT equipment (perfect efficiency). Mostly the average data center operates near 1.58 to 1.8 leading facilities aim for 1.2 or lower. Common initiatives to improve PUE include server virtualization, better cooling, and hardware upgrades. *Figure 3.3* shows the illustrates the proportional resource allocation within a

data center, highlighting the different components and their respective contributions to overall energy or resource consumption. The cooling system and server components are the largest contributors, each accounting for 40% of the total. This indicates that a significant portion of resources is directed towards maintaining optimal server performance and managing the substantial heat generated by high-density workloads.

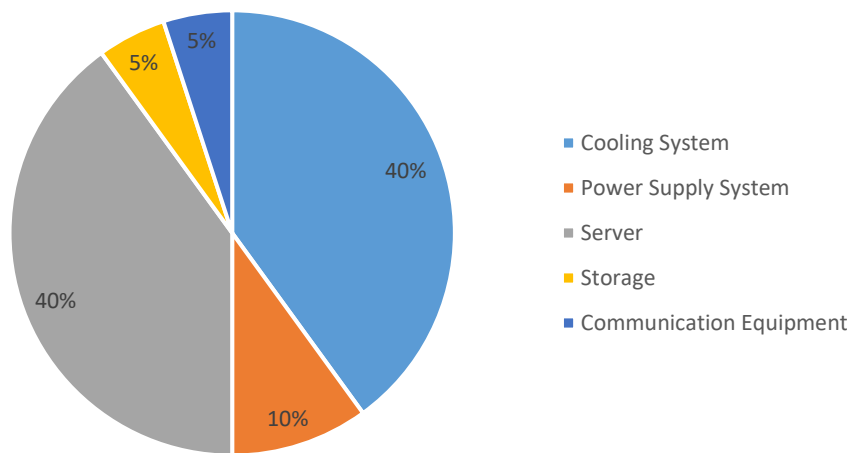


Figure 3.3. Share of Power Usage Effectiveness in Traditional Data Centers. (Source: Compiled based on Literature review)

In contrast, the power supply system constitutes 10% of the total, reflecting the infrastructure needed to ensure uninterrupted power across the facility. Meanwhile, storage and communication equipment contribute equally, each representing 5% of the allocation. This demonstrates that although essential, these components require a smaller fraction of the overall resources compared to cooling and servers. Overall, the graph underscores the dominance of cooling and server operations in resource consumption, emphasizing the need to optimize these areas for efficiency in modern data center environments.

AI data centers aim for lower Power Usage Effectiveness (PUE) ratios despite their high energy demands (see *Figure 3.4*). Advanced cooling technologies reduce cooling-related energy consumption by 30–40%, allowing some of the most efficient AI-oriented facilities to achieve PUE values as low as 1.05–1.10, compared to the 1.5–2.0 range typical of traditional data centers. However, the shift to liquid cooling systems has introduced challenges such as increased water usage, particularly in water-scarce regions, requiring careful resource management.

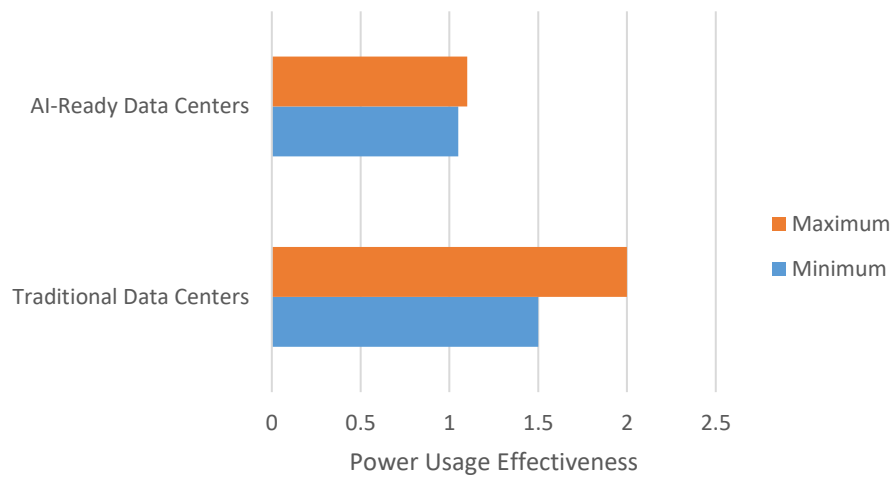


Figure 3.4. Difference in Power Usage Effectiveness in Traditional and AI-Ready Data Centers. (Source: Compiled based on Literature review)

Server Capacity: AI data centers are optimized for high-performance AI workloads, requiring specialized hardware to handle their complex tasks. Unlike traditional data centers, which are built for general-purpose computing tasks and rely primarily on CPUs (Central Processing Units), AI data centers incorporate advanced hardware such as GPUs (Graphics Processing Units), TPUs (Tensor Processing Units), and other AI accelerators. GPUs are particularly well-suited for AI workloads as they can process thousands of tasks simultaneously, making them ideal for training deep learning models and running AI

inferences. These facilities also handle massive amounts of unstructured data, such as images, videos, and sensor inputs, using high-performance storage solutions like NVMe SSDs and parallel file systems to ensure smooth data management. Server capacity in AI data centers far exceeds that of traditional facilities. While traditional data centers typically operate with balanced CPU utilization for general workloads, AI data centers are designed for rapid scaling and high-density computing resources. This allows organizations to deploy additional capacity quickly to meet the growing demands of AI-driven tasks. However, this level of performance comes with significantly higher hardware costs due to the advanced technology required.

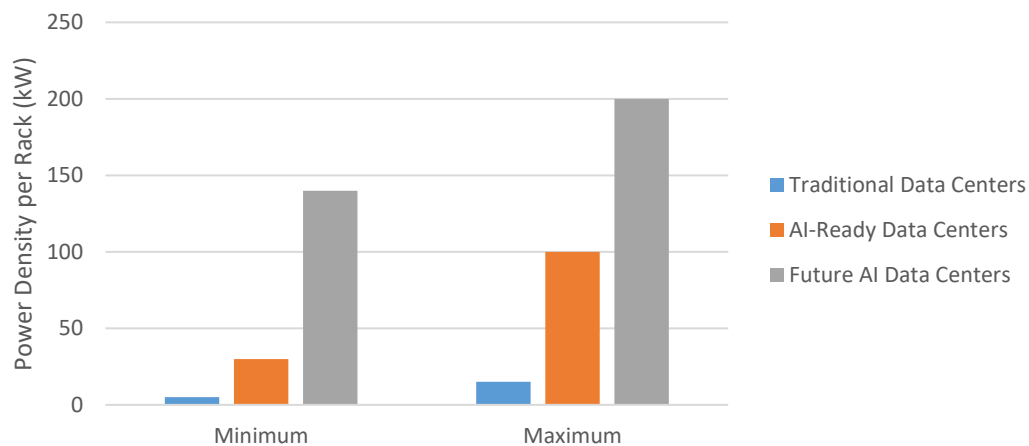


*Figure 3.5. Power density per rack in Traditional, AI-Ready and Future AI Data Centers.
(Source: Compiled based on Literature review)*

Cooling Requirements: The results shown in *Figure 3.5* underline significant differences in cooling energy demand between traditional data centers and AI-ready facilities, primarily driven by the sharp rise in power density and resulting heat concentration. Traditional data centers typically operate at 5–15 kW per rack, relying on conventional air cooling technologies, such as CRAC and CRAH systems, which are sufficient for low-density racks. In contrast, AI-ready data centers exceed 30–100 kW per rack, with some

deployments reaching up to 140 kW and future projections pushing beyond 200 kW. This immense power density generates heat levels up to ten times greater than CPU-driven workloads, necessitating an advanced cooling infrastructure. AI data centers employ liquid cooling techniques, such as Direct-to-Chip (Cold Plate) and Immersion Cooling, which are 3,000 times more effective at heat conduction compared to air cooling. These methods are critical to managing the thermal output of high-density components like NVIDIA H100/B200 GPUs efficiently.

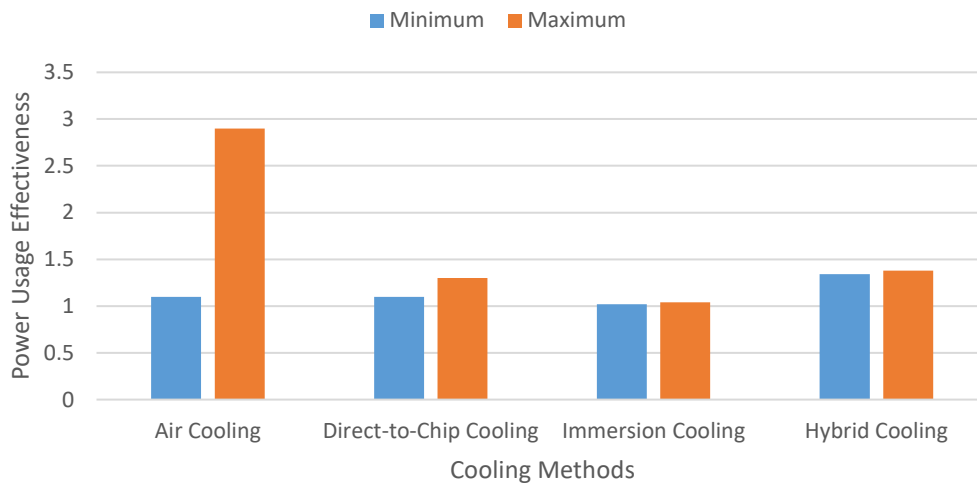


Figure 3.6. Power Usage Effectiveness for different cooling methods employed in AI-Ready and Traditional Data centers. (Source: Compiled based on Literature review)

Figure 3.6 shows the power usage effectiveness for different cooling methods employed in ai-ready and traditional data centers. The data on cooling technologies highlights that no single solution is universally optimal; rather, each method has distinct trade-offs in terms of energy efficiency, operational practicality, and cost-effectiveness. Air cooling, while widely adopted due to its simplicity and low cost, struggles to support high rack power densities (>30 kW) typically required for AI workloads. This limitation

makes it less suitable for scaling advanced AI-ready facilities. Despite this, air cooling may serve well in hybrid deployments where legacy infrastructure is still operational and cost containment is a priority.

Direct-to-chip liquid cooling emerges as a favorable solution for dense AI workloads due to its efficient thermal management capabilities (PUE ~1.1–1.3) and suitability for high-power density configurations. However, the infrastructure upgrades required for plumbing and the risk of leaks present operational challenges that organizations must address. This approach is particularly advantageous in facilities prioritizing high efficiency and advanced workload scalability.

Immersion cooling, offering near-optimal PUE values (~1.02–1.04), represents the most energy-efficient option for high-performance AI data centers. Its ultra-efficient design and low noise levels make it ideal for environments where sustainability and compactness are critical. However, the greater upfront investment for fluid costs, redesigning infrastructure, and specialized hardware can be barriers to adoption. This makes immersion cooling more suitable for cutting-edge AI facilities focused on future-proofing their operations.

Hybrid cooling technologies, combining liquid and air-cooling systems, offer flexibility and adaptability, particularly in transitional setups. Despite slightly higher PUE values (1.34–1.38), hybrid systems are effective for balancing legacy systems with modern cooling demands. However, their complexity in integration and higher costs may deter widespread adoption unless organizations see a strong need for phased transitions. Overall, the choice of cooling technology depends significantly on the strategic objectives of the facility—whether prioritizing energy efficiency (e.g., immersion cooling), balancing cost and implementation complexity (e.g., air cooling or hybrid cooling), or scaling for dense AI workloads (e.g., direct-to-chip systems). As AI workloads and computational demands

grow, organizations must carefully evaluate these trade-offs to align cooling capabilities with sustainability goals, budget constraints, and operational readiness.

3.2.2 Operational Challenges (Objective 2):

To understand the Power Usage Effectiveness (PUE) share among the data center components in AI-ready data centers was estimated based on the data from tradiational data centers and the difference in operating systems. *Figure 3.7*, shows that difference and *Table 3.1* presents the rationale.

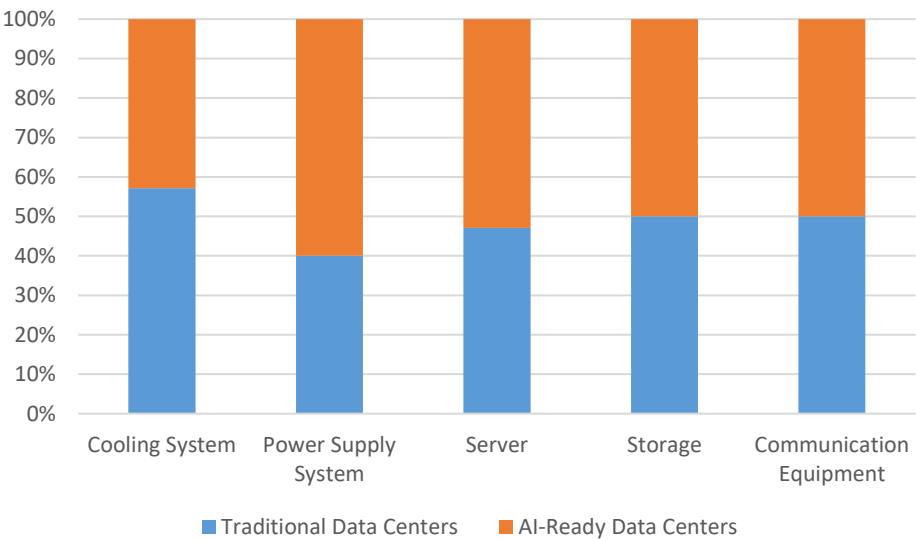


Figure 3.7. Share of Power Usage Effectiveness in AI-Ready Data Centers in comparison with Traditional Data Centers. (Source: Compiled based on Literature review)

Table 3.1. Difference in power usage effectiveness between the AI-ready and traditional data centers along with a rationale.

Category	Data Centers		Rationale for AI-ready Difference
	For Traditional (%)	For AI-Ready (%)	
Cooling System	40%	30%	With liquid cooling systems (30–40% more efficient), cooling energy

			demand is reduced despite higher heat generation.
Power Supply System	10%	15%	AI-ready data centers draw significantly more power per rack (30–100 kW, or more) to support GPUs, leading to an increased share for power supply.
Server	40%	45%	AI-ready systems heavily rely on GPU-intensive workloads, resulting in higher energy consumption for servers compared to traditional CPU-based systems.
Storage	5%	5%	Storage energy remains largely constant, but with high-speed NVMe SSDs and parallel file systems for unstructured data.
Communication Equipment	5%	5%	High-speed, low-latency interconnects are required for AI workloads, but they still account for a small proportion of the total energy demand.

Table 3.2 illustrates the operational challenges explored for both traditional and AI-ready data centers especially when transitioning from traditional to AI-ready along with a rationale.

Table 3.2. Operational challenges between the AI-ready and traditional data centers along with a rationale.

Aspect	Traditional Data Centers	Challenges When transitioning to AI-Ready Data Centers	Rationale/Details
Computational Density	Operates at 5–15 kW per rack.	AI data centers require racks with power densities of 30–100 kW (and up to 200 kW in future setups).	Higher power density significantly increases heat generation and system load demands, necessitating reconfiguration of rack designs and load management.
Cooling Technologies	Uses air-based cooling systems (CRAC/CRAH).	Requires advanced cooling systems like liquid cooling (direct-to-chip, immersion cooling)	Liquid cooling, while efficient, involves higher costs, water management issues

		to manage increased heat output.	(in scarce regions), and maintenance complexities.
Power Supply	Balanced power consumption across systems (lower overall power demand).	Requires a robust and scalable power supply to handle increased energy consumption due to AI hardware (e.g., GPUs/TPUs).	Energy demand per rack increases exponentially, requiring upgrades to power delivery infrastructure and energy redundancy systems.
Networking	Standard Ethernet-based architectures with moderate latency and bandwidth.	Requires low-latency and high-bandwidth networking (e.g., InfiniBand, NVLink) to handle AI workloads' rapid data exchange.	AI workloads involve massive data movement between processors, making traditional networking architectures inadequate.
Storage Systems	Optimized for structured data stored in databases.	Requires scalable, high-performance storage systems such as NVMe SSDs and parallel	AI workloads generate and process unstructured data (e.g., images,

		file systems for unstructured data.	videos, sensor data), demanding higher storage performance and fault tolerance.
Scalability	Scalable but requires significant time and effort to expand.	AI workloads require rapid scalability with a dynamic allocation of resources to handle workload surges effectively.	AI applications need both vertical and horizontal scaling capabilities to meet computational demands seamlessly.
Energy Efficiency (PUE)	Typical PUE range of 1.5–2.0.	Advanced efficiency gains with PUE values as low as 1.05–1.10, but higher overall energy consumption.	While cooling innovations reduce cooling-specific energy consumption, the total energy demand increases due to constant GPU/TPU utilization.
Security	Emphasis on basic encryption,	Requires significantly	AI-ready data centers often handle

	firewalls, and access controls.	enhanced security features to protect AI-sensitive data (e.g., encryption, secure APIs).	proprietary cutting-edge data (e.g., models, healthcare/financial data), necessitating end-to-end protection.
Workforce Skills	Managed by general IT and facility teams.	Requires specialized staff for managing GPUs/TPUs, liquid cooling, and AI-optimized infrastructure.	Workforce specialization raises operational costs due to the need for training or recruitment of AI engineers and data center specialists.
Sustainability	Moderate energy and water usage.	Sustainability becomes more complex as AI workloads require higher energy and cooling capacity.	Operators need to prioritize energy-efficient strategies, renewable energy sources, and efficient water management to meet environmental goals.

Cost Considerations	Lower hardware costs due to use of commodity CPUs, traditional cooling, and standard networking.	Significant increase in CapEx (Capital Expenditure) and OpEx (Operational Expenditure).	Advanced hardware (GPUs/TPUs), high-speed networking, liquid cooling, and energy demands increase both upfront and operational costs.
---------------------	--	---	---

3.3 For RQ-2: Sustainability Challenges and Mitigation Strategies in AI-Driven Data Centers

This section presents the findings related to the key sustainability challenges associated with meeting the growing AI demand within data centers and how modernization efforts can mitigate these challenges.

3.3.1 Environmental Impact of Current Data Center Operations

Carbon Emissions: The data highlights the growing environmental cost of data centers and AI technologies, emphasizing the urgent need to understand and mitigate their carbon footprint. Currently, data centers contribute between 2.5% and 3.7% of global CO₂ emissions, surpassing other significant contributors such as aviation (2.5%) and shipping (2.5%). This stark comparison evidences the significant role of computational infrastructure in global emissions.

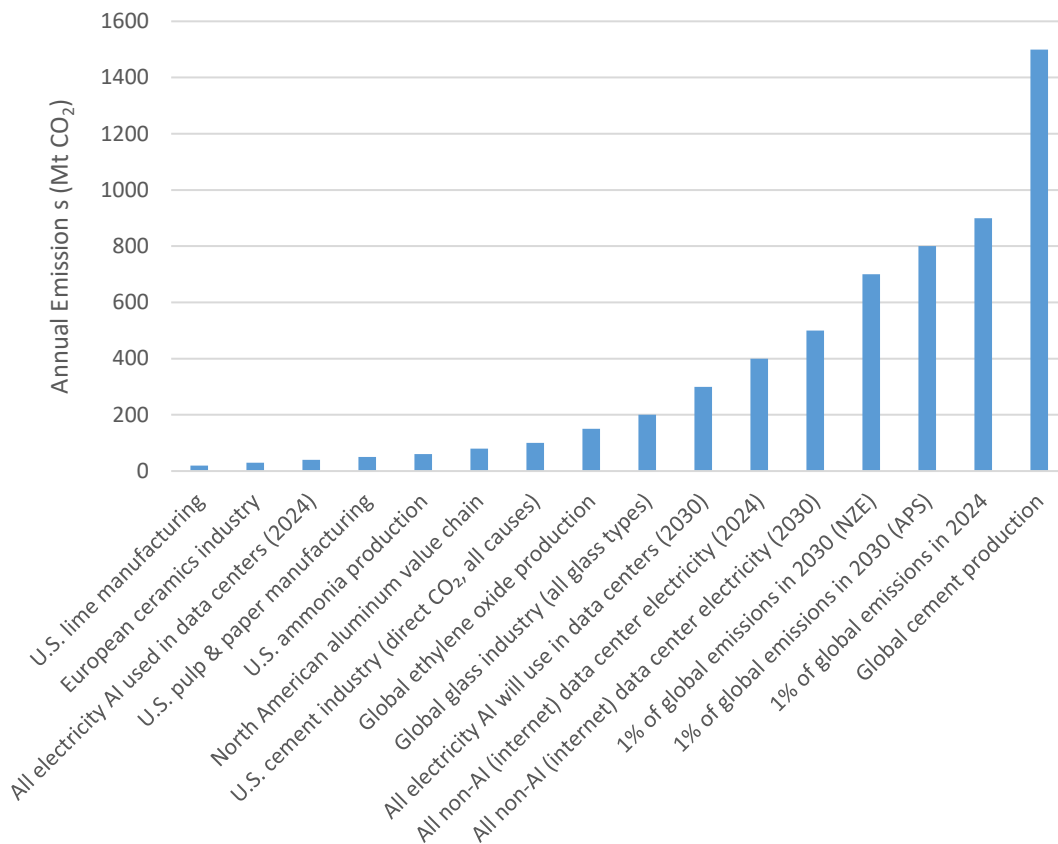


Figure 3.8. Carbon emission of data centers due to electricity consumption and its comparison with other sectors. (Source: Compiled based on Literature review)

AI workloads substantially amplify this challenge. While a single search on platforms like Google emits a modest 0.2 grams of CO₂ per query, the vast number of annual searches (~2 trillion) translates into 400 million kg of CO₂ annually—a significant environmental footprint. However, AI queries, depending on their complexity (text, images, or videos), demand 5 to 10 times more energy than traditional searches. Extrapolating these values, the annual CO₂ emissions from AI infrastructure could range between 2,000 and 4,000 billion kilograms, representing an alarming increase in energy-related emissions. Predictions for AI's energy demands suggest further escalation. According to Alex de Vries, AI's electricity usage globally—comparable to that of

cryptocurrency mining—is forecasted to rise from 85.4 terawatt hours (TWh) to 134 TWh by 2027. These energy demands correlate closely with the growing sophistication of AI applications, making it imperative to implement energy-efficient optimizations at all levels of AI infrastructure.

The data illustrates the significant and growing environmental impact of electricity usage in AI and non-AI data centers compared to other industrial sectors. Global cement production emerges as the largest emitter, with approximately 1,500 Mt CO₂ annually, surpassing all other categories listed. However, the contribution of data centers, both AI and non-AI, is rapidly increasing and warrants critical attention. In 2024, the electricity used in AI data centers is estimated to emit approximately 40 Mt CO₂, which, while relatively modest, is set to grow to 300 Mt CO₂ by 2030, a nearly 7.5-fold increase. This growth reflects the intensifying computational and energy demands of AI technologies. Comparatively, non-AI data centers are projected to reach 500 Mt CO₂ by 2030, indicating the broader environmental footprint of digital infrastructure. When compared to industrial sectors, AI data centers in 2030 are likely to surpass emissions from industries such as lime manufacturing (~20 Mt CO₂), European ceramics (~30 Mt CO₂), and ammonia production (~60 Mt CO₂). By 2030, AI data centers could also approach the emissions of pulp and paper production (~50 Mt CO₂) and North American aluminum value chains (~80 Mt CO₂). This highlights the need for prioritization of energy-efficient technologies to manage emissions in digital infrastructure.

Moreover, AI and non-AI data centers together could account for a significant share of global emissions benchmarks. For instance, their combined emissions align closely with 1% of global emissions in 2030 (~700–800 Mt CO₂) under commonly used climate scenarios (NZE and APS). These projections underscore the urgent necessity to innovate

and adopt sustainable practices to reduce CO₂ emissions in the tech sector, particularly as AI adoption scales in coming years.

The global average electricity emission factor in 2024 was approximately 445 g/kWh (0.445 kg/kWh), reflecting a gradual decline in carbon intensity as renewable and nuclear energy sources expand within the global energy mix. This trend marks significant progress toward decarbonizing electricity generation, driven by the increasing adoption of low-carbon technologies and cleaner practices in energy production. However, despite this improvement, the year 2024 still reflects a substantial reliance on fossil fuels, contributing to higher CO₂ emissions relative to the renewable potential. Consider this emission factor data, emissions from AI- ready data centers are estimated and presented in *Figure 3.9*.

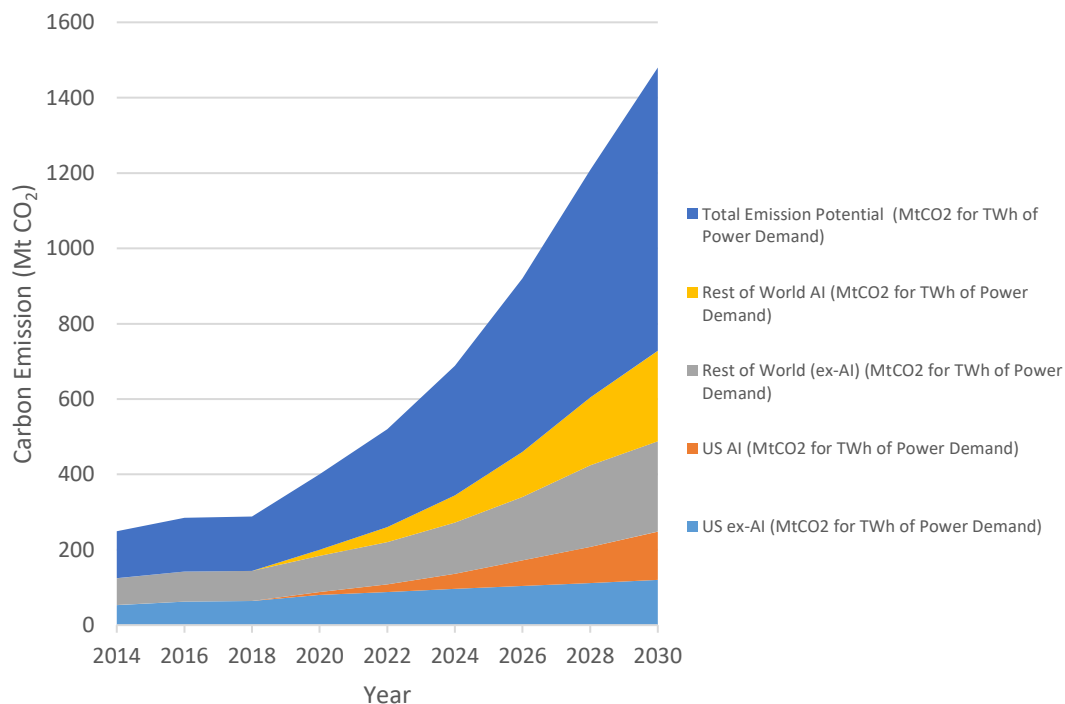


Figure 3.9. Carbon emission for data centers. (Source: Compiled based on Literature review)

Water Usage: A significant number of data centers depend heavily on water-based cooling systems, which can place immense pressure on local water supplies, particularly in areas already facing water scarcity. A 2023 study by the Lawrence Berkeley National Laboratory estimates that data centers consumed approximately 17.4 gallons of water, a figure projected to double by 2028. As both the carbon footprint and water usage of data centers continue to grow, concerns over their environmental impact and associated greenhouse gas (GHG) emissions have risen sharply.

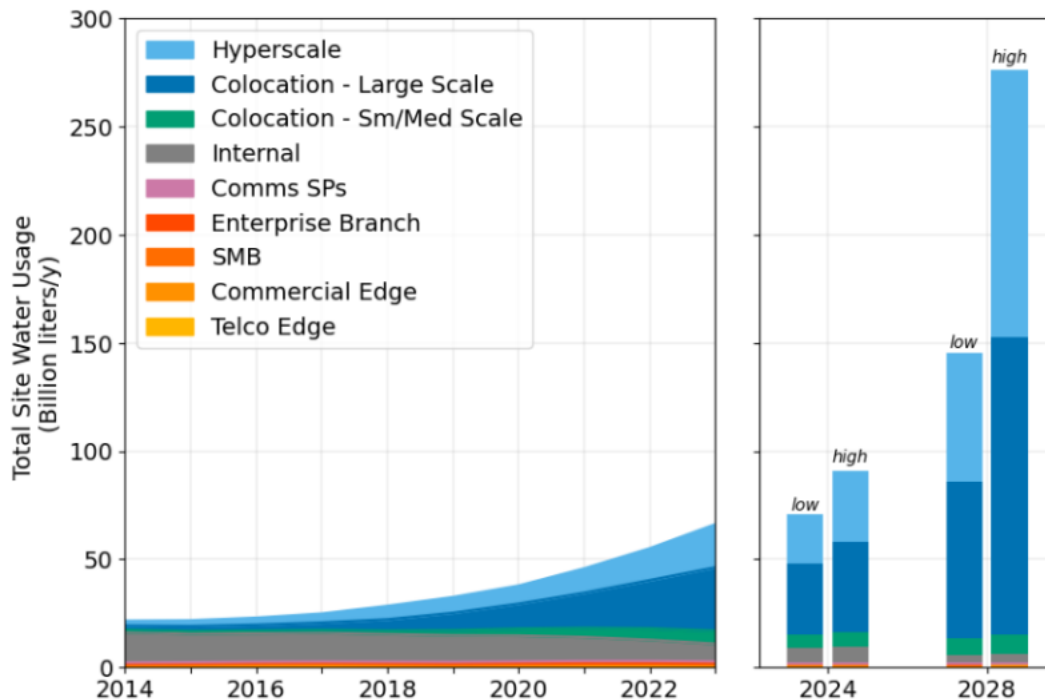


Figure 3.10. Water usage in data centers. (Source: Compiled based on Literature review)

Furthermore, as hyperscale companies like Microsoft and Google—key drivers of data center expansion—pursue ambitious climate goals, reducing the carbon emissions of data centers has become a critical strategic priority rather than merely an operational challenge.

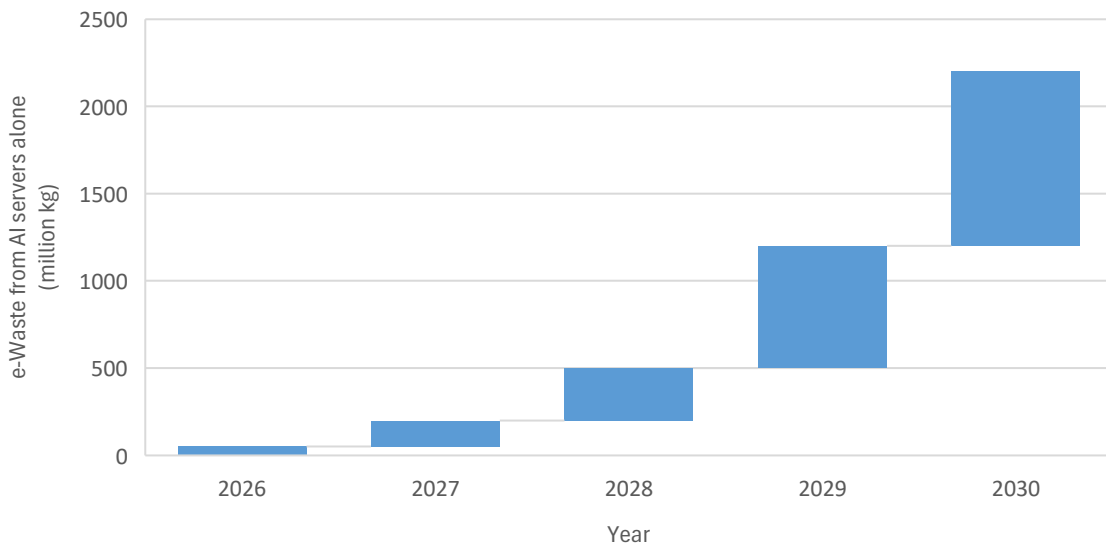


Figure 3.11. e-Waste from AI servers. (Source: Compiled based on Literature review)

E-Waste: A crucial determinant for estimating potential e-waste generation from AI servers is understanding the lifespan of such hardware. Wang et al. (2024) assumed a lifespan of three years, drawing this conclusion from the historical general lifespan of computing devices, traditionally ranging from 2 to 5 years. Notably, Wang et al. (2024) highlighted "lifespan extension" as the most impactful way to reduce AI server e-waste, emphasizing the importance of accurate lifespan approximations to assess expected waste volumes. However, the three-year lifespan figure seems largely conjectural, as the supplemental information accompanying their study merely states that servers typically last three years. This claim contrasts with findings from the Lawrence Berkeley National Laboratory (2024), which reported that servers had an average lifespan of 4.4 years between 2000 and 2019, increasing to 5 years by 2020 and 5.7 years by 2023. Interestingly, the Berkeley Lab applied this updated lifespan to AI servers when analyzing their energy demands. Hintemann et al. (2024) provided corroborative evidence in their research on server stock data, identifying a typical lifespan of 5 to 6 years for servers used by

hyperscale cloud providers such as Google, Amazon, Meta, and Microsoft. When contrasted with the three-year lifespan assumption by Wang et al. (2024), this updated figure of 5-6 years nearly doubles the projected operational life for many servers. Consequently, Wang et al.'s estimates may result in substantial overestimations for e-waste generation in the near term. For example, assuming a six-year server lifespan, the 112.4 million kilograms of AI servers manufactured in 2024 would not reach end-of-life until 2030. In contrast, Wang et al. (2024) had predicted AI-related e-waste generation for 2024 ranging between 0.4 and 2.5 million tons, which is 4 to 22 times greater than the lifespan-based estimate of 112.4 million kilograms.

There are, however, indications that hardware dedicated to AI applications might have shorter lifespans compared to traditional server equipment. Research by Epoch AI (2025) found that AI chips released from 2013 to 2024 had a median lifespan of 2.7 years, from release to their final use in frontier training. Interestingly, their study demonstrated longer lifespans for more recent AI chip designs released after June 2017, which had a median of 3.9 years. This aligns with the observation by the Berkeley Lab that hardware lifespans have been increasing over recent years. For these reasons, a reasonable assumption would place AI server lifespans at around 4 to 6 years rather than the 3 years proposed by Wang et al. (2024). For the purposes of this research, a 5-year lifespan is assumed for AI servers, consistent with typical lifespans observed for general server hardware. However, it remains uncertain how the burgeoning adoption of AI-related applications in 2023 and 2024 has influenced hardware longevity, warranting further investigation in this area.

On the basis of a 5-year lifespan, with AI server production estimates for 2023 and 2024, the expected AI e-waste generation in 2028 would range from 28.3 to 54.5 million kilograms, with 2029 projections increasing to 65.5–112.4 million kilograms. By

comparison, Wang et al. (2024) projected significantly higher e-waste volumes of 389.9–776.5 million kilograms for 2028 and 2029, suggesting that their estimates could be inflated by a factor of seven to fourteen. Looking beyond these years, the discrepancy in growth estimates may continue to widen. The baseline growth model applied by Wang et al. (2024) assumes a fixed yearly growth rate, projecting that AI-related e-waste would roughly double annually.

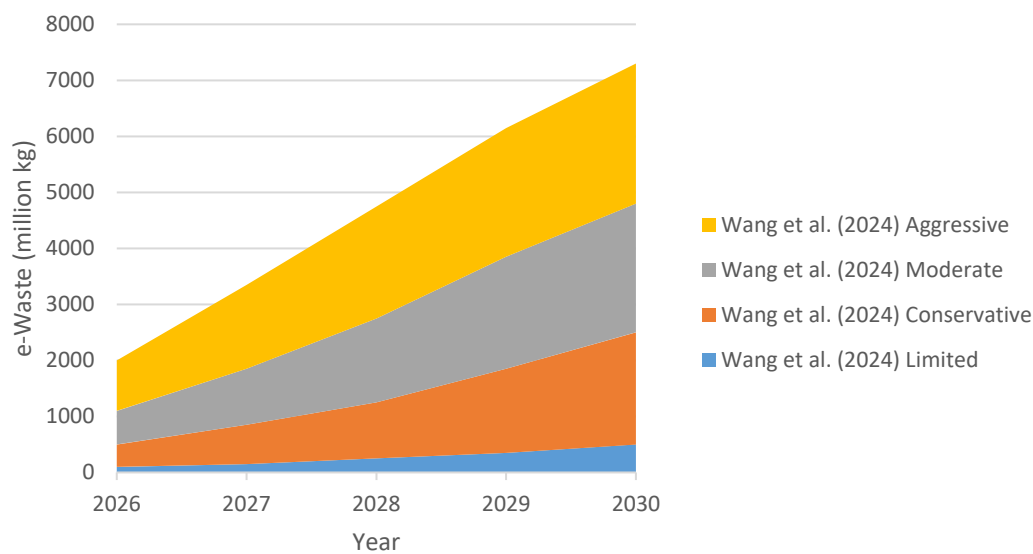


Figure 3.12. e-Waste from AI data centers based on the literature data. (Source: Compiled based on Literature review)

Supporting this trajectory analysis, TSMC confirmed that its CoWoS (chip-on-wafer-on-substrate) supply for AI will double again in 2025, with AI applications consuming the entirety of this capacity (De Vries-Gao, 2025). However, the unique changes introduced by NVIDIA in their AI chip design for the Blackwell generation could temper this growth. These designs feature a new CoWoS-L (CoWoS with local silicon interconnect) packaging, combining two processors and several memory modules within a single structure. Consequently, this packaging architecture halves the number of AI

accelerator modules derived from a given CoWoS supply compared to previous generations. Furthermore, each NVIDIA DGX B200 AI system, which incorporates eight Blackwell modules, adheres to the standard server weight of around 130 kilograms, meaning that despite advancements in AI hardware, the overall weight of servers produced in 2025 may not increase proportionally to production capacity.

Yield challenges also pose another constraint on AI server production. For instance, NVIDIA struggled with low production yields for Blackwell chips throughout 2024 (De Vries-Gao, 2025), and similar challenges in 2025 could dampen production growth further. Additionally, although TSMC has traditionally dominated the AI chip packaging market, other manufacturers are expected to increase CoWoS-like supply in the coming years, potentially expanding capacity for the entire industry. These supply chain limitations and market dynamics suggest that AI server production and associated e-waste growth rates may be more moderate than suggested by Wang et al. (2024). Even if AI-related e-waste doubled between 2029 and 2030, reaching an estimated 131.0–224.8 million kilograms, it would still fall substantially short of Wang et al.'s projection of 0.4–2.5 million tons by 2030. This highlights the need for future research to closely examine production scale, yield trends, and technological advancements when forecasting AI-related e-waste trajectories.

3.3.2 Potential of Modernization Strategies

The data center industry faces mounting pressure to align with global climate goals as the demand for digital services surges, making these facilities a rapidly growing contributor to energy consumption and environmental degradation. While the metrics used to assess operational efficiency, such as Power Usage Effectiveness (PUE) and Water Usage Effectiveness (WUE), provide valuable insights, they often fail to reflect the full urgency

of the climate crisis. Therefore, tackling emissions across the value chain is no longer optional; it is a strategic necessity.

Energy Efficiency and Server Consolidation: Improving energy efficiency remains one of the most cost-effective and impactful strategies for reducing the carbon footprint of data centers. Optimizing how energy is used, both within IT workloads and facility infrastructure, can significantly decrease resource consumption without sacrificing performance. A key enabler of this strategy is server consolidation, which involves migrating workloads from underutilized servers to fewer, high-efficiency machines. Consolidation reduces direct and indirect energy use by lowering cooling demands, conserving electricity, and minimizing operational emissions.

Smart Infrastructure Upgrades: The integration of smart technologies and modern hardware systems is revolutionizing data center sustainability. Machine learning algorithms can analyze environmental and operational data in real time to dynamically adjust airflow and temperature, predict hotspots, and optimize cooling needs. Moreover, upgrading to energy-efficient CPUs and GPUs enables advanced power management and reduces emissions while future-proofing data centers against tightening carbon and energy constraints. These measures, alongside innovations like hybrid cooling and heat reuse systems, are designed to optimize both energy and water use, addressing operational trade-offs between emissions and resource consumption.

Renewable Energy Integration: Shifting to renewable energy sources offers the greatest leverage in achieving decarbonization goals. With computing infrastructure operating continuously, sourcing clean energy is vital. On-site generation methods, including solar

panels and wind turbines, can directly power facilities, while off-site options like Power Purchase Agreements (PPAs) and Renewable Energy Certificates (RECs) provide additional pathways to sustainability. This transition not only minimizes reliance on fossil fuels but also aligns the industry with long-term environmental commitments.

Sustainable Design and Construction: Innovations in facility design and construction also play an essential role in decarbonizing data centers. Material selection, building layouts, and ventilation designs can significantly impact energy consumption and emissions. Certification under green frameworks such as LEED, BREEAM, or Energy Star ensures adoption of best practices, including water efficiency, sustainable material sourcing, and optimized site planning. These approaches enhance both operational efficiency and environmental performance.

3.4 For RQ-3: Future Demands of AI on Data Center Infrastructure and Financing Implications

This section presents the findings related to the projected future demands of AI on data center infrastructure and the implications for financing needs.

3.4.1 Forecast of Data Center Capacity and Resource Requirements

The forecasted global market for data center resources, comprising hardware, software, and services, is projected to exhibit substantial growth between 2023 and 2033, indicating a rapid escalation in demand driven by increased digitization, cloud computing adoption, and AI-driven workloads. In 2023, the total market size was approximately USD 100 billion, with hardware constituting a significant share compared to software and services. This trend continues in subsequent years, although the proportional growth of software and

services becomes more pronounced over time. The market is expected to grow to USD 147.3 billion by 2025, reflecting sustained investment in data center infrastructure. By 2026, this figure is projected to reach USD 180.6 billion, representing a compounded growth fueled by advancements in IT solutions and service delivery models. Beyond 2026, the trajectory showcases accelerated growth, with the market predicted to surpass USD 500 billion by 2031.

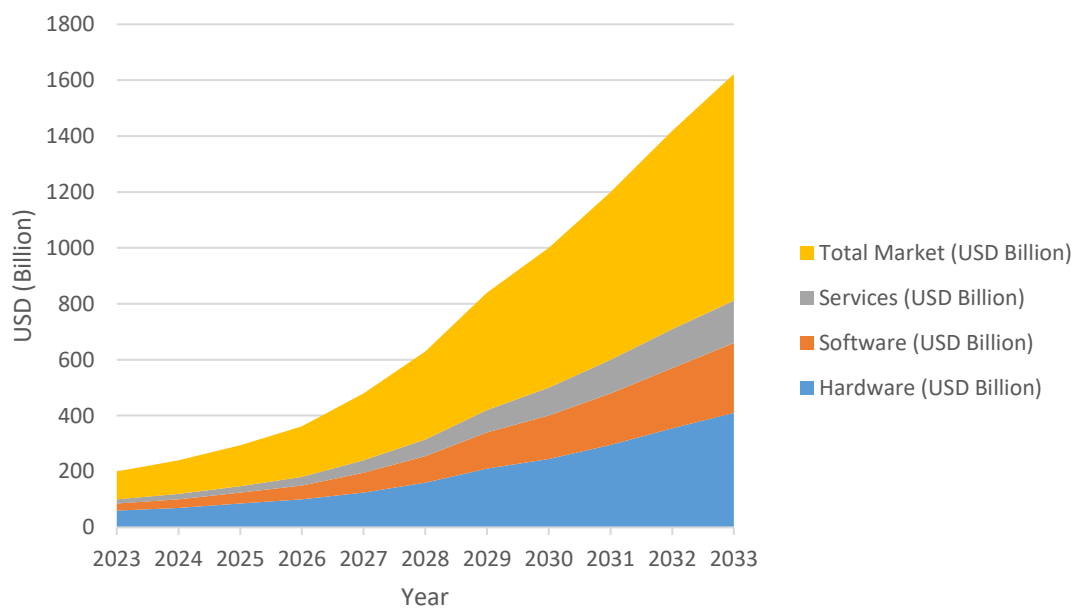


Figure 3.13. Market size of data centers for future. (Source: Compiled based on Literature review)

By 2033, the total market is forecasted to reach USD 810.6 billion, underscoring the continued reliance on and investment in critical data center resources. Hardware persists as the largest component of market expenditure, but software and services show robust growth, signaling a shift towards integrated, value-added solutions and managed offerings. These trends align with projections of rising hyperscale data center deployments, edge computing advancements, and increasing enterprise dependency on service-centric

models. This data reflects fundamental transformations in the data center sector, necessitating enhanced resource planning and innovation. Future resource allocation will need to balance growing hardware requirements with the scalability demands of software and services to handle escalating digital workloads.

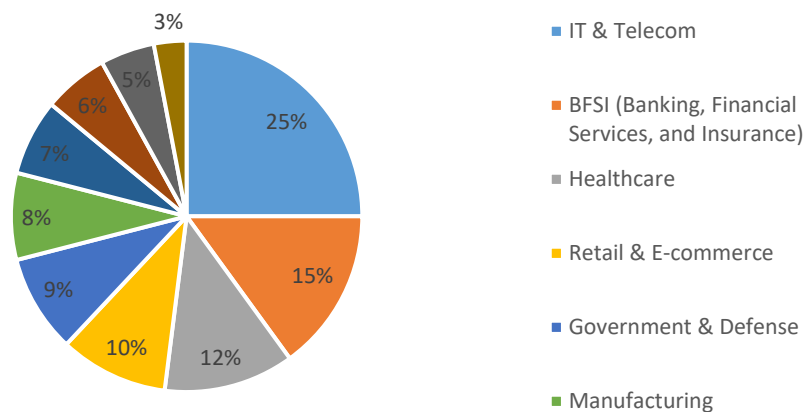


Figure 3.14. Market share of data centers across various sectors. (Source: Compiled based on Literature review)

The distribution of market share across various sectors highlights the prominence of IT and Telecom, which accounts for the most significant segment at 25%. This dominance underscores the critical role of information technology infrastructure and telecommunications in driving modern digital ecosystems. BFSI (Banking, Financial Services, and Insurance) follows as a key player with 15%, reflecting the growing reliance on secure data processing and financial technologies. Healthcare commands 12% of the market, driven by the increasing demand for digital health solutions, telemedicine platforms, and data-driven healthcare innovations. Retail and E-commerce contribute 10%, showcasing the rapid expansion of online shopping and logistical technologies. Other significant sectors include Government and Defense (9%) and Manufacturing (8%), which emphasize advancements in public sector IT capabilities and smart manufacturing

processes, respectively. While sectors like Energy and Utilities (7%), Media and Entertainment (6%), and Automotive (5%) highlight specialized applications of digital technologies, smaller industries collectively represent a modest 3%, showing limited but valuable participation. This data reflects the broad applicability of technology across diverse sectors while emphasizing the strategic importance of IT-dominant industries.

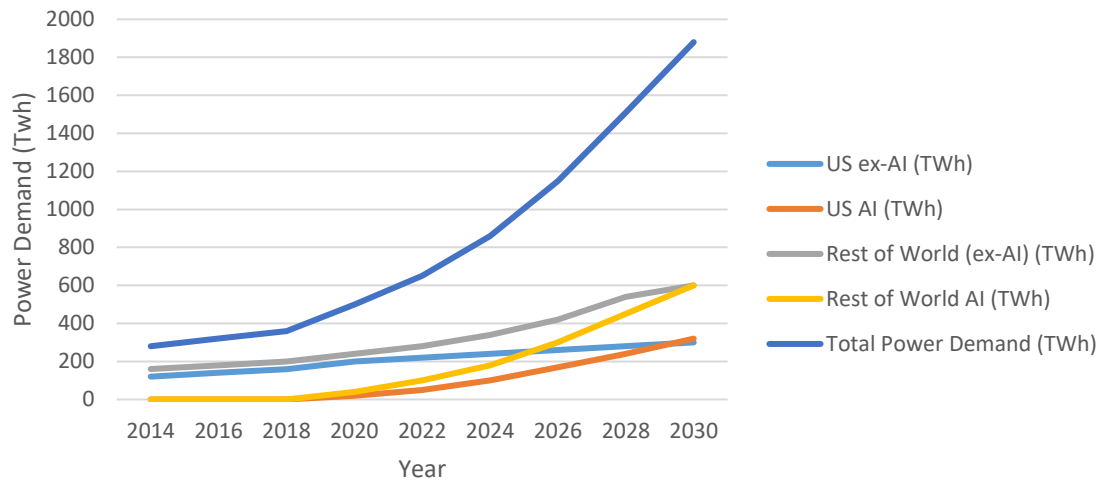


Figure 3.15. Projection of power demands based on the market size. (Source: Compiled based on Literature review)

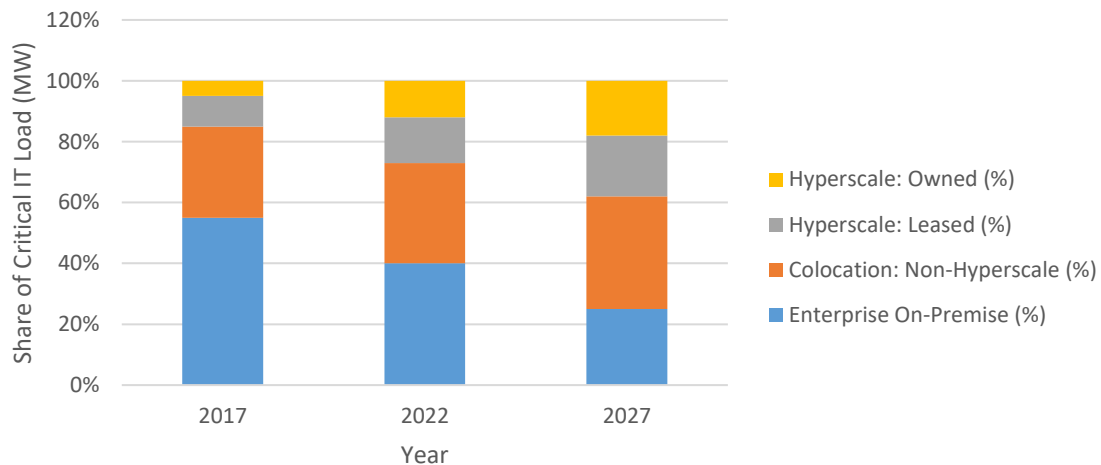


Figure 3.16. Share of critical; IT load for data center types under different operating modes. (Source: Compiled based on Literature review)

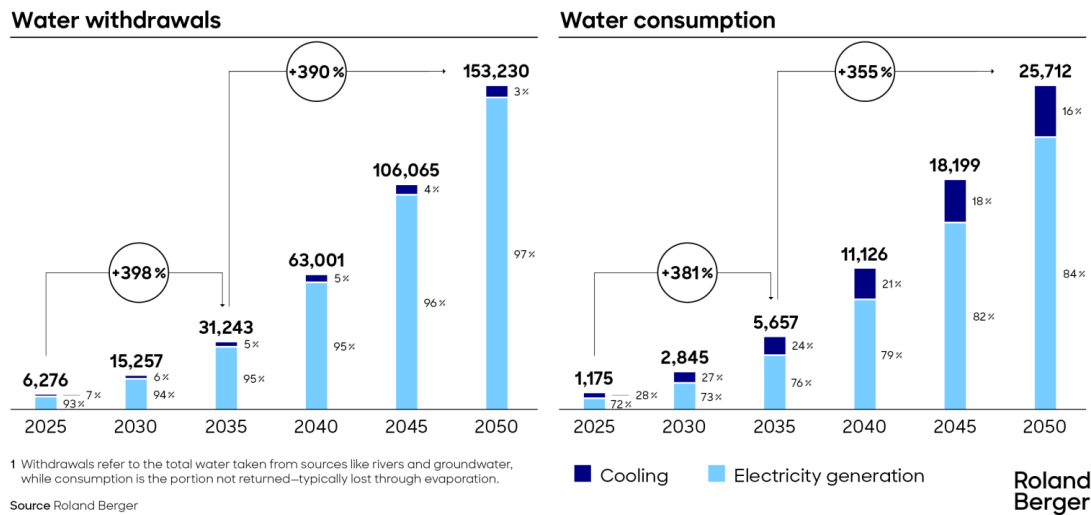


Figure 3.17. Project of water withdrawals and water consumption for data centers.
Source: Roland Berger.

3.4.2 Financial Investment Requirements

Data centers form the backbone of the modern digital economy, supporting the growth of the internet and artificial intelligence (AI). The economics of data centers, from capital expenditures (capex) to operational costs (opex), are shaped by their size, purpose, and location. Industry Scale by 2025, the global data-center market will comprise around 500 large facilities and 12,000 total facilities, providing 135 GW of capacity. This capacity is expected to triple by 2035, highlighting the explosive demand for digital and AI-driven workloads. A 30 MW medium-sized data center requires a capex of \$10M/MW and needs to generate \$100M in annual revenue to achieve a 10% internal rate of return (IRR) after covering electricity and maintenance costs.

For a typical non-AI data center, the total cost is approximately \$10,000/kW. The largest expenditures are on IT components, cooling systems, battery uninterruptible power supplies (UPS), backup generators, and fiber connections. For computation-intensive AI facilities, capex can rise dramatically to around \$40,000/kW. Over half these costs are attributed to GPUs (graphics processing units), with operational costs scaled to

approximately \$10/EFLOP for compute power. The lowest costs are found in the United States and the Middle East where as the costs in Europe and Japan are 30–40% higher due to energy prices, infrastructure, and fiscal regimes.

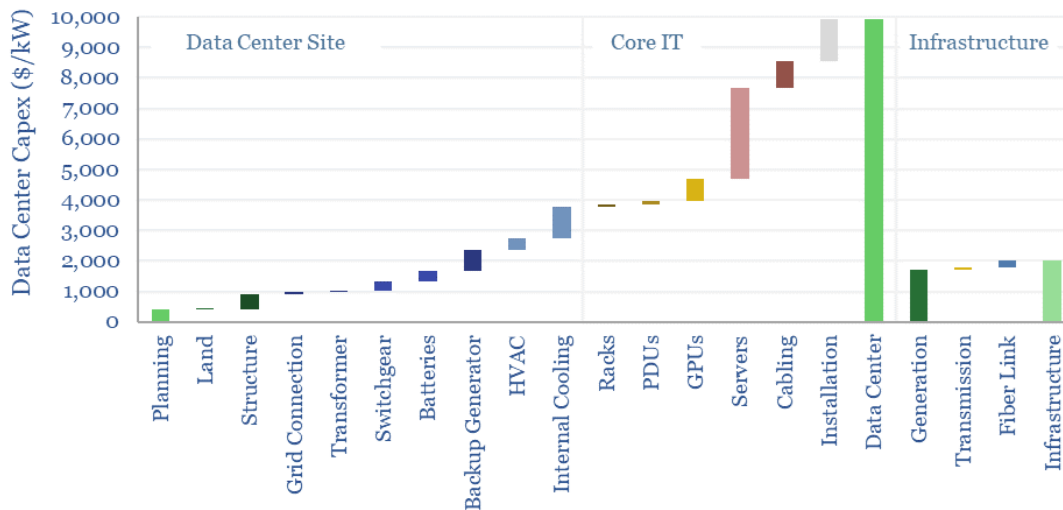


Figure 3.18. CapEx of the data center. Source: SaidEnergy

The breakdown of data center capital expenditure (capex) reveals the significant investments required to build and operate these critical facilities. Core IT equipment dominates the cost structure, with servers representing the largest expense, followed closely by GPUs, particularly in AI-focused data centers where high-performance computation is essential. Together, these components reflect the growing demand for advanced processing capabilities. Power distribution units (PDUs), racks, cabling, and installation add secondary but notable costs, underscoring the complexities of deploying sophisticated IT systems. Beyond core IT, site preparation and infrastructure also account for a substantial portion of overall capex. Within the site category, grid connections,

transformers, backup power systems (such as batteries and generators), and HVAC cooling systems are crucial investments, ensuring facilities maintain high uptime and operational reliability. On the broader infrastructure level, components such as power transmission and fiber links represent notable expenditures, as they provide essential connectivity to external utility services and the internet backbone. This detailed capex profile highlights how core IT equipment drives data center costs, while site and infrastructure components serve as vital supporting systems. Together, these factors underscore the economic and technical considerations necessary to build scalable, energy-efficient, and high-performance data centers capable of meeting growing computational workloads, particularly for AI and cloud computing.

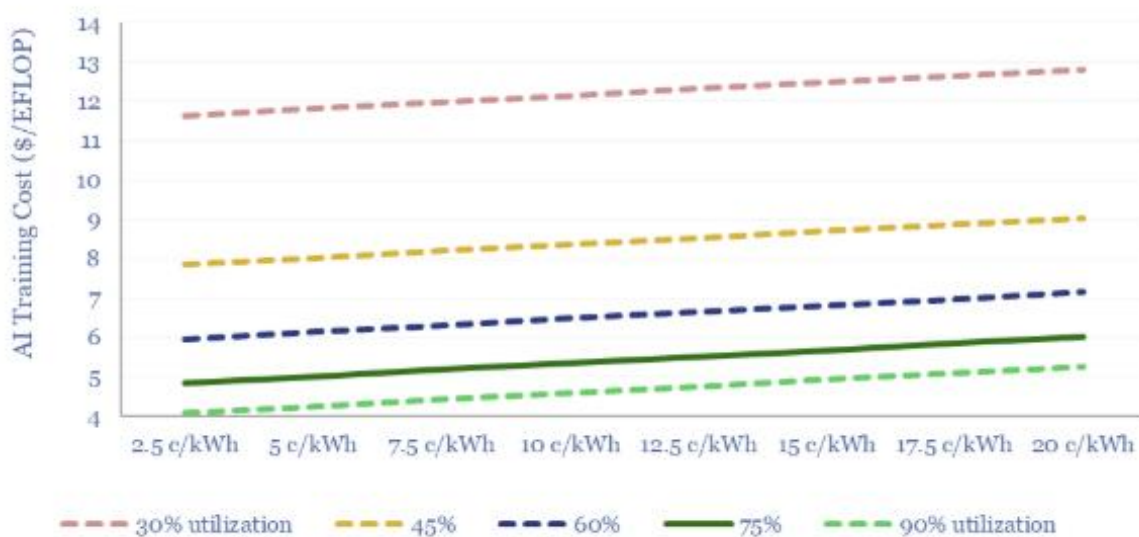


Figure 3.19. AI training cost in the data centers. Source: SaidEnergy

The chart illustrates the relationship between AI training costs, measured in dollars per exaFLOP (\$ / EFLOP), and electricity prices as a function of data center utilization rates. As expected, AI training costs rise with higher electricity prices across all utilization

levels, but the impact varies substantially based on the efficiency of data center usage. At lower utilization rates, such as 30%, costs are significantly higher and more sensitive to electricity prices, starting at approximately \$12 / EFLOP at \$0.025 / kWh and climbing to nearly \$14 / EFLOP at \$0.20 / kWh. As utilization improves, costs decrease dramatically. For instance, at 90% utilization, the cost starts at around \$5 / EFLOP at \$0.025 / kWh and rises modestly to just under \$6 / EFLOP at \$0.20 / kWh.

This demonstrates that optimizing utilization rates has a more profound effect on reducing AI training costs than merely relying on cheaper electricity. A shift from 30% to 90% utilization reduces training costs by over 50%, regardless of energy price fluctuations. The linear progression in the chart further emphasizes the critical role of operational efficiency in maintaining cost competitiveness, especially as AI computations become increasingly energy-intensive. These insights highlight the importance of maximizing utilization through intelligent resource allocation while carefully managing electricity prices to drive down the levelized cost of AI computation.

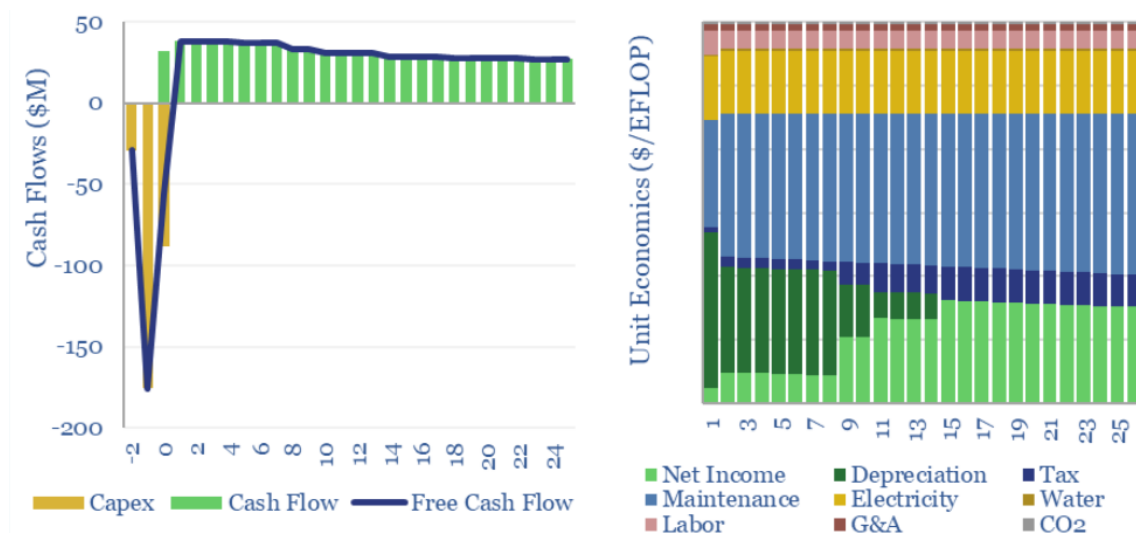


Figure 3.20. Cash flows and unit economics of data centers. Source:.. SaidEnergy

The left chart provides an analysis of cash flow dynamics for a data center project over 24 months, depicting capex, cash flow, and free cash flow trends. Early in the project, capital expenditures (capex) dominate, creating significant negative cash flows as investments are made in infrastructure, equipment, and operational setup. This results in free cash flow plunging to approximately -\$200 million during the initial phases. However, as the facility begins operations, cash flow becomes positive, leading to a rapid recovery in free cash flow by month 6. Over time, cash flows stabilize, with consistent positive income generated after month 10. The trend highlights the capital-intensive nature of data centers during development phases and their subsequent ability to generate steady cash flow once operational.

The right chart details the unit economics of AI computations in dollars per exaFLOP (\$/EFLOP), breaking down the costs into multiple components. Electricity comprises the largest share of ongoing expenses, reflecting the energy-intensive nature of AI workloads, followed by depreciation costs linked to high capital investment in infrastructure and hardware. General and administrative (G&A) costs, maintenance, and labor also contribute significantly, with smaller proportions allocated to taxes, water usage, and CO₂ emissions. Notably, as scale and operational efficiency improve, cost contributions from maintenance and labor decline, while depreciation and electricity costs remain relatively steady over time. This indicates opportunities for optimizing both fixed and variable cost elements to improve data center profitability.

Together, these charts underscore the heavy upfront investment requirements of data centers, balanced by their long-term cash flow potential, and the importance of managing key cost drivers such as electricity and depreciation to improve unit economics for AI-driven workloads. By effectively optimizing these factors, operators can enhance

profitability while managing sustainability metrics, such as CO₂ emissions and resource usage.

Figure 3.21 illustrates the trends in hyperscale operator spending and the corresponding data center capacity additions from Q3 2018 to Q3 2025. The left chart shows the quarterly capital expenditure (CAPEX) in billions of dollars, reflecting a significant upward trend in investments. Beginning at around \$20 billion per quarter in 2018, CAPEX has steadily climbed, surpassing \$60 billion by late 2024, with projections reaching close to \$140 billion by Q3 2025. This exponential growth highlights the increasing financial commitment of hyperscale operators to expand infrastructure and meet rising global demands for digital services, cloud computing, and AI workloads.

The right chart tracks data center capacity added per quarter in megawatts (MW) over the same period. Similarly, capacity additions follow a parallel growth trajectory, starting modestly in 2018 before accelerating by 2021 and sustaining rapid growth throughout 2023 and beyond. Operational IT capacity added in the later quarters surpasses all prior growth, reflecting the industry's focus on deploying high-performance infrastructure at an unprecedented scale. Notably, the alignment between CAPEX expenditure and capacity growth demonstrates a strong correlation between hyperscale spending and operational scalability.

These trends underscore the hyperscale sector's critical role in supporting global digital transformations. The increasing CAPEX signifies not only rising demand but also the intensification of competition among hyperscale operators. As data centers become more computationally intensive, this investment surge reflects a strategic emphasis on capacity expansion, infrastructure modernization, and sustained reliability to serve the ever-growing computational and storage needs of global enterprises and AI-driven workloads.

Hyperscale Operator Spending and Data Center Capacity

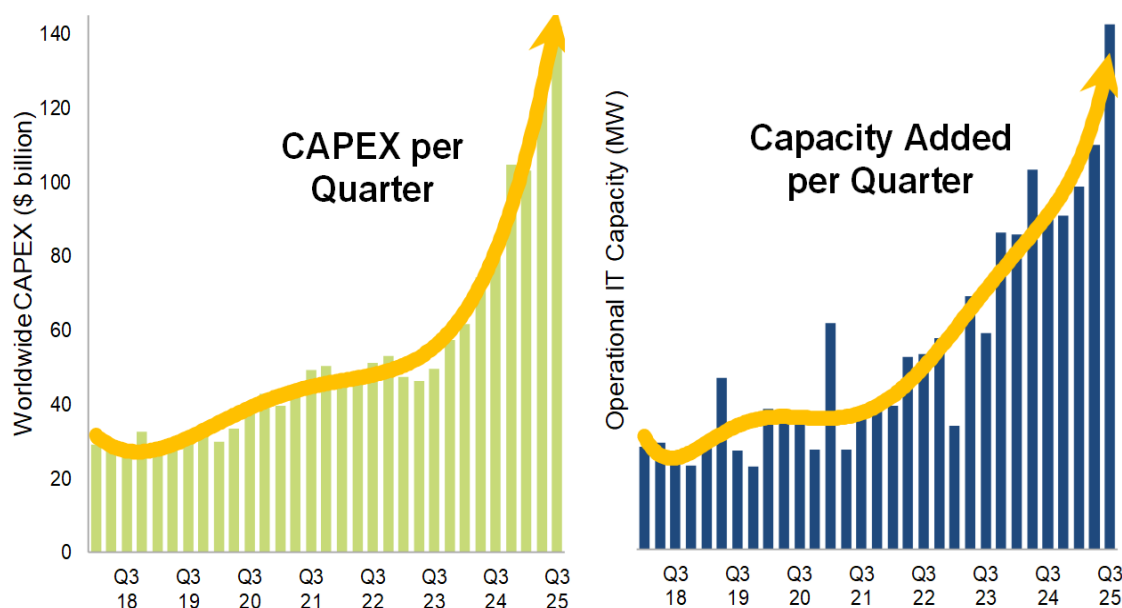


Figure 3.21. Capex per different quarter and operational capacity added for hyperscale data center operator. Source: Synergy research group

3.5 For RQ-4: Sustainable Finance Instruments for AI-Ready Data Centers

This section presents the findings related to the types of sustainable finance instruments that are most suitable for financing the modernization of AI-ready data centers.

3.5.1 Identification and Analysis of Sustainable Finance Instruments (Objective 1):

Sustainable finance instruments are revolutionizing funding for environmentally responsible data centers, enabling large-scale investments in energy-efficient infrastructure, renewable energy procurement, and water stewardship. Instruments such as Green Bonds, Green Loans, Sustainability-Linked Loans (SLLs), and Green Asset-Backed Securities (ABS) provide tailored financial mechanisms to accelerate the industry's transition toward sustainability. Green Bonds allow operators to raise fixed-income capital for eco-friendly projects, such as constructing energy-efficient facilities or retrofitting

existing buildings with state-of-the-art sustainable technologies. Green Loans cater specifically to projects that meet strict environmental criteria, often funding renewable energy procurement or advanced cooling systems. Meanwhile, Sustainability-Linked Loans incentivize achieving predefined sustainability performance targets (SPTs), such as reducing Power Usage Effectiveness (PUE) or transitioning to renewable energy, by tying interest rates to these benchmarks. Green ABS, which securitize data center cash flows from green assets, have also garnered high investor interest, underscoring the financial viability of eco-focused initiatives.

Eligibility for sustainable financing hinges on strict criteria, including achieving lower PUE scores, adopting closed-loop water systems, investing in renewable energy through Power Purchase Agreements (PPAs) or on-site solar/wind infrastructure, and adhering to international green certification standards, such as LEED or EDGE. These criteria ensure that funded projects deliver measurable environmental benefits. Moreover, the market has seen a shift toward stricter financing frameworks that not only focus on metrics like PUE but also address broader concerns, such as emissions intensity from power sources and water-related risks in drought-prone locations.

Major firms, including Equinix, STACK Infrastructure, and Vantage Data Centers, have led the charge, securing billions in green financing while achieving measurable progress, such as surpassing 97% renewable energy use. This trend reflects growing investor confidence in sustainable data center projects that align with global green finance principles, such as the ICMA Green Bond Principles and LMA/LSTA Green Loan Principles. As environmental scrutiny increases, these tools provide a compelling pathway to build data centers that balance performance with sustainability, turning the industry's ambitious environmental goals into tangible outcomes.

Table 3.3. Various Financial Instrument and their pros and cons

Financial Instrument	Description	Pros	Cons
Green Bonds	Fixed-income instruments raising funds for specific eco-friendly projects, such as energy-efficient facilities.	-Provides access to a larger pool of environmentally conscious investors. -Raises awareness about sustainability initiatives -Long-term funding opportunities.	-Requires strict adherence to green project guidelines. -Higher costs for compliance, certification, and auditing.
Green Loans	Loans specifically targeted at funding projects with strict environmental criteria.	- Favorable interest rates for green projects. -Flexible loan terms tailored to promote green objectives. -Direct support for renewable energy or efficient cooling infrastructure.	- Limited to projects meeting strict eligibility criteria. -Requires thorough reporting and verification.

Sustainability-Linked Loans (SLLs)	Loans where interest rates are linked to achieving predefined sustainability performance targets (SPTs).	-Financial incentives for achieving sustainability goals. -Flexible use of loan proceeds. -Promotes accountability through performance metrics.	-Penalties for not meeting targets. -Complex to negotiate terms and SPTs. -Ongoing monitoring increases costs.
Green Asset-Backed Securities (ABS)	Securitization debt backed by green data center assets and their cash flow.	-Attractive to investors due to fixed cash flows. - Unlocks additional financing by leveraging existing assets. -Suitable for scaling green initiatives.	-High initial transaction costs. -Dependence on stable cash flow generation from assets. -May require complex structuring.
Power Purchase Agreements (PPAs)	Long-term contracts to procure renewable energy	-Guarantees access to renewable energy at predictable costs.	-Long-term contractual obligations.

	directly from providers.	- Reduces emissions significantly. -Enhances energy resilience.	- Risk of fluctuating energy prices. -Requires alignment with generation sources.
On-Site Renewable Energy Financing	Investments or financing aimed at installing renewable energy systems within data center premises.	-Reduces long-term energy costs. -Improves energy independence. -Demonstrates proactive sustainability measures.	-High upfront capital costs. - Limited scalability in urban or space-constrained environments.

3.5.2 Evaluation of Instrument Suitability

Table 3.4 shows the evaluation of financial instrument suitability for different data centers based on the size.

Table 3.4. Evaluation of Financial Instrument Suitability for different data centers based on the size

Financial Instrument	Small-Scale Data Centers	Mid-Scale Data Centers	Hyperscale Data Centers
Green Bonds	Unsuitable for small-scale projects due to high	Suitable for sustainable retrofitting or green-targeted	Highly suitable for financing sustainable infrastructure

	transaction and compliance costs.	expansions of existing facilities.	projects on a large scale. Attracts environmentally conscious investors.
Green Loans	Ideal for financing energy-efficient equipment, renewable energy installations, or retrofitting older facilities.	Highly suitable for projects needing flexible funding for ongoing green upgrades or renewable energy PPAs.	Effective for modular expansions or sustainability-driven projects with strict adherence to environmental criteria.
Sustainability-Linked Loans (SLLs)	Offers flexible funding for sustainability upgrades, but harder to justify unless aligned with strong sustainability goals.	Highly suitable for operators with established sustainability targets. Improves long-term financial performance by achieving these milestones.	Excellent option for hyperscale operators with large-scale sustainability goals, tying financial benefits to carbon reductions and efficiency gains.
Green Asset-Backed Securities (ABS)	Unsuitable due to insufficient cash flow or assets.	Suitable if cash flows are stable, enabling financing for green	Highly suitable for monetizing existing cash flows and unlocking capital to

		expansions or new facilities.	scale green investments further.
Power Purchase Agreements (PPAs)	Challenging to execute unless the operator has sufficient energy demand or established load patterns.	Suitable if energy consumption is high enough to justify long-term renewables contracts.	Excellent for ensuring access to reliable, renewable energy to power hyperscale installations with vast electricity demands.
On-Site Renewable Energy Financing	Suitable for small centers looking to reduce operating costs and their carbon footprint.	Highly suitable for centers with adequate space for solar, wind, or alternative renewable installations.	Suitable for hyperscale centers, but space constraints may limit scalability for urban facilities.

The suitability of financial instruments differs significantly between traditional data centers and AI-ready data centers due to variations in infrastructure demands, energy intensity, and sustainability goals (*Table 3.5*). AI-ready data centers require substantially higher upfront capital investment, driven by their reliance on GPUs, advanced cooling technologies, and renewable energy adoption, making larger instruments such as Green Bonds and Green ABS particularly favorable. In contrast, traditional data centers, with more moderate infrastructure needs, can often rely on more flexible and incremental

financing options, such as Green Loans, to fund efficiency retrofits and renewable energy integration. AI-ready facilities also prioritize advanced cooling systems, such as liquid or immersion cooling, to manage the heat generated by dense GPU racks, making Sustainability-Linked Loans (SLLs) attractive for financing these targeted modernization efforts. Traditional facilities, with less urgent cooling demands, achieve their efficiency goals more effectively through simpler retrofits funded by Green Loans or renewable energy financing.

Moreover, AI-specific data centers align strongly with aggressive sustainability goals, such as achieving 100% renewable energy usage or pushing PUE limits below 1.4. These ambitious targets make SLLs and Power Purchase Agreements (PPAs) particularly effective for AI workloads, where financial incentives are tied to performance metrics. In comparison, traditional data centers typically pursue smaller-scale upgrades and adopt a balanced approach between grid and renewable energy support. This distinction highlights how AI-ready data centers prioritize scalability, energy optimization, and long-term sustainability milestones, necessitating more robust and future-focused financial instruments than their traditional counterparts.

Table 3.5. Evaluation of Financial Instrument Suitability for traditional and AI-ready data centers

Financial Instrument	Traditional Data Centers	AI-Ready Data Centers
Green Bonds	Highly suitable for funding energy-efficiency upgrades, such as modernizing cooling systems, retrofitting facilities, and building new	Highly suitable due to the large capital needs for GPU-focused facilities, renewable energy procurement, and cutting-edge cooling infrastructure.

	energy-efficient data centers.	
Green Loans	Ideal for projects aimed at improving energy efficiency, retrofitting old facilities, or adopting renewable energy sources.	Strongly viable for projects focused on energy-intensive tasks. Funding can target advanced cooling (liquid/immersion) and grid-connected power.
Sustainability-Linked Loans (SLLs)	Suitable for projects where gradual but measurable sustainability performance improvements, such as better PUE or renewable energy adoption, can be achieved.	Well-suited for AI centers as SLLs tie financial advantages to milestones like renewable energy usage, reducing emissions, or GPU energy optimization.
Green Asset-Backed Securities (ABS)	Effective for monetizing mature traditional data center assets with consistent cash flows for further expansion projects.	Highly suitable, especially for mature AI-ready data centers with steady cash flow streams to unlock capital and scale infrastructure even further.
Power Purchase Agreements (PPAs)	Suitable for facilities with high energy demands and stable workloads, enabling direct renewable energy	Strongly suitable as AI workloads require extensive power. Large, long-term PPAs guarantee

	procurement to lower environmental impact.	renewable energy supply for energy-intensive training tasks.
On-Site Renewable Energy Financing	Excellent for traditional centers in locations with sufficient space for solar/wind systems to lower long-term energy costs.	Limited scalability due to AI-ready centers' extremely high power density, though some facilities can integrate hybrid renewable energy solutions.

3.6 For RQ-5: Modifications and Innovations to Sustainable Finance Instruments for Data Center Modernization

This section presents the findings related to the modifications or innovations to existing sustainable finance instruments that are necessary to effectively address the unique requirements of data center modernization projects.

3.6.1 Identification of Barriers and Limitations

While the explored financial instruments such as Green Bonds, Green Loans, Sustainability-Linked Loans (SLLs), Power Purchase Agreements (PPAs), and Green Asset-Backed Securities (ABS) provide critical support for sustainability initiatives in traditional and AI-ready data centers, they face several barriers and limitations that restrict their full potential. These challenges necessitate the exploration of more innovative financing models, such as ESG (Environmental, Social, Governance)-focused instruments, to fill the gaps.

High Compliance and Administrative Costs: Many of the instruments, particularly Green Bonds and ABS, require rigorous compliance with environmental standards, third-party audits, and certification frameworks such as the ICMA Green Bond Principles or LMA Green Loan Principles. These processes incur high administrative costs that can deter smaller data center operators or emerging players from adopting these instruments. Additionally, the process of ongoing environmental reporting and performance alignment can be resource-intensive, discouraging widespread implementation.

Access Limitations for Small Operators: While traditional data centers may benefit from relatively small-scale instruments like Green Loans, many operators especially those in emerging markets face challenges in accessing adequate financing for sustainability projects. Hyperscale players dominate instruments like Green ABS due to their predictable cash flows and economies of scale, while small- to mid-size operators struggle to meet the strict eligibility criteria, such as commitments to 100% renewable energy or net-zero emissions.

Balancing Short-Term Returns vs. Long-Term Sustainability Goals: Investments in sustainability-focused infrastructure (e.g., AI-specific cooling or renewable energy integration) often take years to yield returns. This longer payback period and the high upfront capital requirements pose challenges for investor buy-in, particularly for institutions focused on short-term financial gains. Instruments like SLLs, while incentivizing sustainability performance, do not adequately address this misalignment of financial timelines.

Technology-Specific Challenges for AI-Ready Data Centers: AI-focused data centers face unique barriers such as dealing with high power density, carbon-intensive GPU workloads, and reliance on advanced cooling systems. Existing instruments, although supportive, do not directly address these challenges. For instance, PPAs and Green Bonds prioritize renewable energy adoption but may lack incentives to improve computational and energy efficiency specific to AI tasks, such as advanced AI model training.

Narrow Focus on Environmental Metrics: The conventional financial tools explored above primarily center on environmental benefits (energy efficiency, lower PUE, renewable adoption) while neglecting the broader dimensions of social and governance metrics. For instance, projects in water-scarce regions often require investments in advanced water management systems, but barriers such as regional policy constraints or lack of suitable financing frameworks hinder progress. Similarly, governance metrics, like ethics in data usage, are often overlooked in current financing approaches.

Limited Adaptability in Emerging Markets: In regions with underdeveloped financial systems or higher political and economic risks, many sustainable finance instruments are poorly suited or difficult to implement. The stringent requirements of Green Bonds or Green Loans often exclude operators in developing countries, where data center expansion is growing rapidly but lacks sustainable financing options for infrastructure tailored to regional constraints.

3.6.2 Proposed Modifications and Innovations

The adoption of ESG-focused financing has emerged as a transformative tool for funding data centers, enabling operators to achieve both environmental sustainability and access to

competitive capital. Unlike traditional financing mechanisms, ESG frameworks incorporate a broader set of goals, addressing environmental priorities such as mitigating carbon emissions and improving energy efficiency, while integrating social and governance dimensions like workforce equity, ethical AI practices, and supply chain transparency. These features make ESG financing particularly well-suited for hyperscale and AI-driven data centers, which face mounting pressure to balance immense power density demands with sustainability and ethical considerations.

Facilities leveraging ESG financing instruments have demonstrated concrete benefits. Research highlights operational cost reductions averaging 8-12% due to efficiency advancements such as energy-efficient cooling and renewable energy integration. Moreover, facilities achieving strong ESG performance achieve 15–25 basis point financing advantages, as reported by Moody’s ESG Solutions. The strategic integration of ESG criteria has also enhanced market competitiveness. For example, Morgan Stanley’s 2023 study reveals that green-certified data centers attract 2.3 times more investor interest and allow operators to command premium service pricing of 5-10%. Furthermore, ESG frameworks provide flexibility to target region-specific challenges, such as water-neutral operations in drought-prone areas or governance-driven data ethics for AI workloads.

Recent examples underscore the growing adoption of such instruments. Equinix issued €1.15 billion in green bonds focused on renewable energy, achieving 97% facility-wide renewable power usage. Similarly, STACK Infrastructure secured \$3 billion to fund sustainable campus developments emphasizing energy efficiency and water conservation in key regions. Scala Data Centers employed an innovative ESG-oriented debenture of R\$2 billion to achieve a PUE of 1.40 while attracting significant multinational investments.

These successes illustrate how ESG financing has catalyzed the development of cutting-edge, environmentally aligned data centers.

ESG financing also provides long-term resilience by aligning with evolving regulatory frameworks and leveraging advanced compliance tools. Early adopters of AI-driven energy management and blockchain-based carbon tracking report efficiency gains of 20-30% in monitoring ESG performance while reducing administrative costs. In addition, the flexibility of ESG instruments encourages innovation in tackling Scope 3 emissions, addressing supply chain carbon footprints, and enhancing climate adaptability—all areas where traditional green tools fall short.

Table 3.6. Proposed modifications and innovations for sustainable financial instruments tailored for data centers

Proposed Innovation	Description	Key Benefits	Potential Impact
Multi-Criteria ESG-Linked Instruments	Redesign Sustainability-Linked Loans (SLLs) to incorporate weighted metrics beyond environmental goals, including social equity and governance.	Encourages holistic improvements across multiple ESG dimensions, such as water neutrality and ethical AI practices.	Promotes well-rounded sustainability efforts while offering favorable borrowing terms based on broader achievements.

AI-Centric Financing Instruments	Specialized tools like AI-Support Green Loans, funding cooling systems, GPU energy optimization, and AI-driven energy management.	Addresses unique energy and cooling demands of AI workloads; improves resource utilization efficiency.	Optimizes operational performance while reducing energy consumption in AI-specific data centers.
Carbon-Neutral Asset-Backed Securities (CN-ABS)	Securitization of carbon-neutral data center assets and cash flows, requiring third-party emissions verification.	Attracts ESG-focused institutional investors; incentivizes emissions reduction across operations and supply chains.	Expands funding opportunities for operators committed to carbon neutrality.
Dynamic Green Bonds with Regional Customization	Issue Green Bonds that target region-specific environmental challenges, such as water conservation in arid locations.	Addresses localized sustainability needs while attracting diverse investor participation.	Ensures funding aligns with specific environmental priorities unique to each geography.

Modular Green Loans	Loans deployed in increments tied to green milestones, such as PUE optimization or incremental renewable energy adoption.	Increases accessibility for smaller data centers with limited upfront capital.	Allows gradual and scalable adoption of sustainability initiatives.
Blockchain-Based Green Finance	Use smart contracts for real-time ESG monitoring, automating interest rate adjustments tied to metric achievements.	Enhances transparency and investor confidence; reduces compliance costs through automation.	Improves accountability, simplifies reporting, and links performance directly to financial outcomes.
Emission-Centric PPAs (E-PPAs)	Power Purchase Agreements tied to actual emissions reductions rather than just renewable energy commitments.	Provides flexibility in regions with mixed energy grids while driving verified emissions reductions.	Expands renewable energy accessibility to more regions without compromising on emissions goals.
Green Convertible Notes	Hybrid instruments that convert debt to equity if specific	Aligns environmental performance goals	Promotes setting and achieving aggressive

	sustainability milestones, like net-zero emissions, are met.	with investor returns; strong financial incentives for operators.	sustainability metrics across operations.
Social-Impact Addendum in Financing	Integrates social targets (e.g., workforce diversity, local job creation) into financing instruments for data centers.	Drives social equity and inclusion; enhances community engagement and brand reputation.	Expands ESG financing to include broader societal impacts alongside environmental goals.
Climate-Resilient Investment Funds	Funds directed toward climate adaptation initiatives such as floodproofing and disaster recovery infrastructure.	Enables data centers to withstand extreme weather risks effectively; lowers insurance costs.	Strengthens the resilience of critical infrastructure, reducing economic and operational risks from

3.7 For RQ-6: Risks and Rewards of Sustainable Finance for AI-Ready Data Centers

This section examines the risks and rewards of leveraging previously explored sustainable financial instruments—such as Green Bonds, Sustainability-Linked Loans (SLLs), Green Asset-Backed Securities (ABS), and Power Purchase Agreements (PPAs)—to modernize data centers. As these instruments evolve to address environmental, social, and governance

(ESG) goals, the associated risks and rewards are becoming clearer. This analysis also presents strategies to mitigate potential risks and highlights the substantial benefits of integrating these tools into data center financing frameworks.

Table 3.7. Risk type in data centers and its assessment

Risk Type	Description	Example/Impact
Technology Obsolescence	Sustainable financial instruments like Green Loans and SLLs often fund cutting-edge technologies, which may soon become outdated due to rapid innovation.	A data center funded by Green Bonds to install traditional air-cooling systems may later require complete retrofitting for liquid immersion cooling to handle AI workloads.
Regulatory Uncertainty	Dependence on fluctuating regulatory factors such as tax incentives, carbon pricing, and renewable energy subsidies poses a risk to financial planning.	Sudden changes, such as reductions in renewable energy credits or stricter emissions targets, may affect data centers relying on PPAs for renewables.
Stranded Assets	Investments in technologies or facilities may lose value as market conditions or environmental regulations	A data center financed by Green ABS in a fossil-fuel-reliant region could lose competitiveness as renewable energy adoption accelerates.

	evolve, leaving assets underutilized.	
Reputational Damage	Inability to meet ESG targets tied to Green Bonds or SLLs can harm a company's public image and investor confidence.	Overstating sustainability claims (greenwashing), such as achieving 100% renewable energy without actual offsets, can cause public backlash.
Market Risks	Energy market fluctuations can impact anticipated financial returns from instruments like PPAs or Green ABS.	Energy price volatility could make contracted renewable energy agreements financially less viable.
Operational Risks	Complex technologies funded by Green Loans, such as AI-driven cooling or energy management systems, may introduce operational inefficiencies.	Systems may face unexpected bottlenecks during deployment, delaying ROI and potentially increasing overall costs.
Social Risks	Ignoring workforce training needs, community engagement, or equity-related ESG aspects may lead to negative social outcomes.	Lack of focus on workforce development when modernizing a facility can result in low morale and skill gaps among employees.

Table 3.8. Risk Mitigation Strategies and Identification of Potential Rewards

Category	Description	Example/Impact
Diversification	Diversify projects funded by Green Bonds or Green Loans across renewable energy sources (solar, wind, hydro) and regions.	Reduces risks by mitigating overdependence on a single technology. Funding geographically diverse data centers minimizes exposure to regulatory or market risks.
Insurance	Integrating risk coverage as part of Green ABS to protect against extreme events like natural disasters or flooding.	Climate risk insurance safeguards facilities in flood-prone regions, ensuring assets funded through SLLs remain financially viable during catastrophes.
Performance Guarantees	Partner with vendors for guarantees that infrastructure such as cooling systems or GPU clusters meets efficiency targets.	SLL lenders can tie loan pricing to achieving power usage effectiveness (PUE) benchmarks guaranteed by technology suppliers, ensuring predictable performance.
Enhanced Energy Efficiency	Sustainable investments promote energy-saving	Implementation of liquid cooling systems can reduce

	modernization, such as advanced cooling systems funded by Green Bonds.	cooling power consumption by up to 40% compared to traditional air cooling, improving operational efficiency.
Reduced Operating Costs	Funding renewable energy projects through PPAs or Green Loans ensures predictable pricing and lowers utility expenses.	Operators save up to 25% in energy costs by integrating on-site solar or wind generation, leading to improved financial margins and long-term cost stability.
Improved ESG Ratings	Investments through instruments such as Green ABS and SLLs demonstrate sustainability, enhancing ESG ratings.	Example: Equinix's Green Bond-funded projects achieved net-zero Scope 2 emissions, resulting in 2.3 times higher investor interest driven by ESG alignment.
Customer Acquisition/Trust	Sustainable financing improves environmental performance, earning customer trust and enabling higher service pricing.	Gartner states 73% of customers prioritize sustainability when selecting providers. Facilities may charge a premium of up to 10% for

		services backed by Green Loans.
Expanding Innovation	Funding supported by Green Loans enables exploration of novel technologies like AI-driven energy optimization systems.	Novel innovations funded by sustainable instruments enhance operational performance while ensuring environmental compliance, driving competitiveness.
Resilience to Environmental Risks	Financing through climate-adaptive funds bolsters facility resilience against extreme weather conditions.	Example: Green ABS-funded floodproof infrastructure reduces operational disruptions caused by unpredictable climate events, such as floods or heatwaves.
Community/Social Engagement	Social-Impact Linked Loans promote workforce training, local job creation, and equitable community benefits.	Facilities ensure societal goodwill by funding education programs or creating job opportunities in underserved regions alongside environmental goals

3.8 For RQ-7: Lessons Learned from Data Center Financing and Modernization Case Studies

This section presents the findings related to the key lessons learned from existing case studies of data center financing and modernization projects.

Case Study – 1: Google’s Green Data Centers: Network POP Case Study

The retrofitting of Google’s Point of Presence (POP) facility introduced a series of systematic changes to improve energy efficiency and cooling performance. The results, drawn from each stage of intervention, show significant improvements in the facility’s operational efficiency, cost savings, and environmental impact. This section provides a detailed walkthrough of the measures utilized and their effects on key performance metrics, particularly Power Usage Effectiveness (PUE).

Baseline Conditions, where the inefficiencies are identified. The initial assessments revealed substantial operational inefficiencies tied to cooling and airflow management.

High PUE: The baseline PUE of 2.4 reflected significant energy waste in facility overhead, with cooling systems consuming more energy than necessary relative to the IT equipment load.

Underutilized Infrastructure: Though the room's design supported a total load of 250 kW, its operational load was only 85 kW. Cooling infrastructure (4 CRAC units) still operated as if fully loaded, leading to unnecessary energy use.

Suboptimal Airflow and Thermal Profile: Simulations using Computational Fluid Dynamics (CFD) highlighted issues such as, cold air passed directly from vents to the hot aisle without sufficiently cooling equipment where as the high-power racks (approximately 5.6 kW per rack) concentrated heat in localized areas, straining cooling performance.

Table 3.9. Summary of Interventions and Results in Google's POP Facility Retrofitting

Stage	Interventions	Results	PUE Improvement	ROI (Payback)
Baseline (Initial State)	- IT load: 85 kW (oversized facility designed for 250 kW). - Inefficient CRAC operation (4 units active at all times). - Poor airflow (bypass and hotspots). - Initial PUE: 2.4.	Inefficient energy use, excess cooling, and high energy overhead.	Starting PUE: 2.4	N/A
Stage 1: Immediate Adjustments	- Redirected vent tiles for better airflow toward high-power racks. - Increased CRAC	- Reduced bypass airflow. - Compressor workload reduced.	2.4 → 2.2	< 1 month

	temperature from 22°C (71°F) to 27°C (81°F). - Widened humidity range to 20%-80%.	- Initial savings in cooling energy. - No impact on IT performance.		
Stage 2: Cold Aisle Containment	- Installed blanking panels in empty server racks. - Added refrigerator door-style plastic curtains at ends of cold aisles (contained airflows).	- Eliminated mixing between cold/hot air. - Reduced hotspots near high-power server racks. - Energy-efficient air delivery to racks.	2.2 → 2.0	Around 9.7 months
Stage 3: CRAC Air Return Extensions	- Extended CRAC air return ducts by 48 inches.	- Balanced airflow and improved monitoring.	2.0 → 1.7	Around 2.7 months

	- Prevented premature hot/cold air mixing (near ceiling) and stratification. - Improved CRAC temperature accuracy.	- Reduced unnecessary compressor cycling. - Smoother airflow across the room.		
Stage 4: Centralized CRAC Control	- Installed central controller for CRAC units. - Dynamically managed CRAC activity to scale with load. - Disabled redundant units during low-load periods.	- Reduced active units from 4 to 2 during normal operations. - Maintained redundancy for peak loads. - Minimized cooling energy use.	1.7 → 1.5	Around 6.5 months

Table 3.10. Quantitative Outcomes Summary for Google's POP Facility Retrofitting

Metric	Before Retrofitting	After Retrofitting	Improvement
Power Usage Effectiveness (PUE)	2.4	1.5	Reduction of 0.9 points (37.5% improvement).
Annual Energy Usage	~1,850 MWh	~1,180 MWh	Energy savings of 670 MWh (~36% reduction).
Annual Energy Cost	~\$134,000	~\$67,000	Cost savings of \$67,000 per year (~50% reduction).
Capital Investment	-	\$25,000 total	Minimal investment with rapid ROI.
Carbon Emissions	~1,065 metric tons/year	~680 metric tons/year	Reduction of 385 metric tons annually (~36%).

Table 3.11. Scalability Across Multiple POPs in Google.

Facilities Analyzed	Initial PUE	Post-Retrofit PUE	Outcome Consistency
POP 1	2.4	1.5	Successful with improvement consistent with pilot project.

POP 2	2.3	1.6	Energy efficiency replicated with similar PUE reduction.
POP 3	2.2	1.5	Scalable intervention results across different conditions.
POP 4	2.4	1.7	Confirmed adaptability across varied IT loads.

Table 3.12. Summary of the Impacts and benefits of retrofitting the data center

Category	Description
Financial Impact	\$67,000 annual cost savings, with payback of investments between 2.7 and 9.7 months, depending on intervention.
Environmental Impact	670 MWh annual energy savings with approximately 385 metric tons of carbon reduction annually.
Operational Benefits	- Enhanced cooling efficiency. - Reduced wear on equipment. - No service interruptions during retrofitting.

The implementation of energy optimization measures in Google's POP facilities delivered transformative results, yielding critical insights into practical and scalable approaches for improving data center efficiency. Foremost among these lessons was the importance of detailed, data-driven diagnostics using thermal sensors and Computational Fluid Dynamics (CFD) models. These tools enabled clear identification of inefficiencies, such as cold air bypass, thermal hotspots, and overcooling. Establishing a measurable baseline, such as the initial PUE of 2.4, allowed for a systematic evaluation of subsequent interventions. Incremental retrofitting emerged as one of the most valuable strategies. Low-cost, non-disruptive modifications such as vent tile realignment, blanking panel installations, and the addition of cold aisle containment solutions immediately improved airflow management and reduced bypass inefficiencies. These changes alone reduced the PUE from 2.4 to 2.0. Similarly, extending CRAC air return ducts by 48 inches further enhanced cooling efficiency by eliminating hot and cold air mixing, achieving another significant efficiency gain with minimal investments. The integration of a centralized CRAC controller was another pivotal step, as it dynamically adjusted cooling operations to match real-time IT loads, reducing energy waste while maintaining system redundancy. These scalable measures improved the final PUE to 1.5, marking a 37.5% reduction in overall energy inefficiency. Another critical finding was the value of aligning operations with industry standards, such as ASHRAE guidelines. By increasing the thermostat temperature to 27°C and widening humidity ranges, the cooling system's workload was immediately reduced without compromising equipment reliability. This demonstrated the potential of simple configuration changes to save energy while staying within safe operational tolerances.

The financial and environmental impacts of these interventions were equally notable. A total capital investment of \$25,000 yielded annual cost savings of \$67,000, with payback periods for individual measures ranging from less than one month to 9.7 months. Furthermore, the reduction in energy consumption of 670 MWh annually resulted in a 36% decrease in carbon emissions, achieving a balance between economic sustainability and environmental stewardship. The broad scalability of this approach was demonstrated when similar interventions were replicated successfully across four other POPs, with consistent PUE reductions to a range of 1.5–1.7, regardless of IT load or facility variations. Overall, this case study highlights the efficacy of phased, incremental retrofits informed by precise diagnostics. Key lessons include the significance of airflow management, dynamic cooling operations, and adherence to industry temperature standards. These findings underline the potential for organizations to achieve rapid ROI, long-term cost savings, and emissions reductions while maintaining uninterrupted operations, offering a replicable model for energy optimization in data centers globally.

The overarching lessons from the case study emphasize a systematic, data-driven, and incremental approach to improving energy efficiency in data centers. The interventions, characterized by low-cost and high-impact measures, offer replicable strategies for any organization seeking to reduce energy costs, improve cooling performance, and align with sustainability goals.

Key principles that emerge include:

- Focus on monitoring and diagnostic tools to identify inefficiencies.
- Prioritize low-cost, non-intrusive interventions (airflow optimization, containment).
- Scale cooling operations dynamically to match IT loads.
- Align operational conditions (temperature and humidity) with industry tolerances.

- Embrace strategies that balance cost reduction with environmental impact.
- These lessons offer a template for organizations worldwide to enhance efficiency in their IT infrastructure, bridging the gap between operational effectiveness and sustainability leadership.

3.9 For RQ-8: Regional Variations in Sustainable Financing Models for Data Center Modernization

The transition toward sustainable and energy-efficient data center infrastructures has been influenced heavily by regional contexts, including variations in regulatory frameworks, financial incentives, energy costs, and market maturity.

3.9.1. Variability in Regulatory Frameworks

Governmental policies and regulations play a critical role in influencing financing models for sustainable data center modernization. In regions like Europe, strict environmental mandates such as the European Union’s Green Deal and requirements for carbon neutrality by 2050 have driven the adoption of green financing mechanisms. Data centers in countries like Germany, Sweden, and the Netherlands benefit from subsidies for renewable energy, tax incentives for energy-efficient upgrades, and carbon credit trading schemes. For instance, Germany’s KfW green loans earmarked for energy efficiency provide low-interest financing for retrofitting and modernization projects. In contrast, North America features a more decentralized approach, largely dependent on state or provincial policies. States like California offer robust incentives under programs such as the Self-Generation Incentive Program (SGIP), which supports the integration of renewable power systems (e.g., solar and battery storage) to data centers. However, regions with lower renewable energy penetration or less regulatory pressure exhibit slower adoption due to reduced

financial incentives and a heavier reliance on traditional financing. In Asia, regulatory support is uneven. Advanced economies like Singapore lead the region with targeted policies, such as the Green Data Centre Programme, which co-funds energy-efficient upgrades. Emerging markets with high growth potential but weaker regulatory environments, such as India and Southeast Asia, are beginning to adapt green financing frameworks but heavily rely on private investment or international development funds.

3.9.2. Energy Costs as Catalysts for Financing Models

Regions with higher energy costs often see more aggressive adoption of modern, sustainable financing models. Northern and Western Europe exemplify regions where energy prices create a compelling financial case for prioritizing data center energy efficiency. For example, energy costs in Sweden are relatively high, but data center operators benefit from tax reductions on electricity and incentives linked to heat recovery projects that recycle waste heat into district heating for the community. Conversely, in regions like the Middle East, the abundance of low-cost fossil fuels has delayed widespread adoption of sustainable financing mechanisms, despite government-led ambitions to diversify into renewable energy markets. In such regions, financing models primarily focus on energy self-sufficiency rather than renewable adoption, generally supported by public-private partnerships (PPPs).

3.9.3. Dominance of Public vs. Private Financing

The availability of public funding has shaped the structure and success of financing models across regions:

Europe and Asia-Pacific: These regions heavily rely on public-private financing models. Public entities often subsidize modernization efforts to align with national climate goals,

making projects financially viable. For example, the European Investment Bank has invested billions into green technology development, including data center modernization. North America: Models are more private-sector driven. Venture capital and private equity firms fund modernization projects, particularly those aiming to integrate renewable energy and advanced cooling solutions. Local utility companies often provide rebates or incentives to modernize infrastructure under energy efficiency programs.

Emerging Markets (e.g., Africa, Latin America): In regions with limited government funding, international development banks, such as the World Bank or the Asian Development Bank (ADB), often serve as key financiers of sustainable modernization projects. These projects frequently focus on hybrid energy models that incorporate renewable sources into fossil-fueled energy systems.

3.9.4. Adoption of Alternative Financing Models

Innovative financing mechanisms have also seen varied adoption across regions:

Green Bonds: Europe and Asia-Pacific have demonstrated leadership in utilizing green bonds to modernize infrastructure. For example, in 2020, China became the largest issuer of green bonds globally, with substantial allocations toward data center construction and energy efficiency upgrades.

Energy-as-a-Service (EaaS): EaaS has gained traction in North America and parts of Europe, where data center operators outsource their energy optimization needs to third-party providers. By using EaaS models, operators reduce capital expenditures and shift to operating expense-based financing.

Carbon Pricing Mechanisms: Regions with established carbon markets, such as the European Union's Emission Trading System (EU-ETS), financially incentivize modernization projects by pricing carbon emissions and rewarding reductions. In less

developed carbon markets, such as Asia and Latin America, these mechanisms are emerging but face implementation challenges due to inconsistent enforcement.

3.9.5. Regional Innovation and Heat Recycling Initiatives

Certain regions have adopted financing models that promote innovative approaches to sustainability:

Nordic Countries: Unique financing models support state-mandated heat recycling initiatives. For instance, district heating systems in Sweden and Denmark allow data centers to sell waste heat to municipalities through pre-established agreements. This additional revenue stream directly offsets energy costs, encouraging further investment in sustainable technology.

United States: In areas like the Pacific Northwest, financing models focus on renewable energy purchase agreements, such as wind and hydroelectric power. Investments are directed toward achieving long-term energy costs savings instead of projects like heat redistribution.

Asia-Pacific: Singapore's green financing programs also incentivize the integration of technologies like liquid cooling and high-performance computing to decrease energy consumption.

3.9.6. Challenges in Financing Models

Despite regional successes, several challenges persist:

Emerging markets in Southeast Asia, Africa, and Latin America face difficulties attracting investment due to high project risk, underdeveloped policy frameworks, and limited access to international capital markets.

Smaller data center operators in regions like Southern Europe and parts of the U.S. struggle to access low-cost financing due to scale disadvantages. Financing in these regions is often more accessible for hyperscale operators with stronger capital backing.

Regional disparities in renewable energy availability hinder the widespread adoption of green financing models in areas reliant on non-renewable energy.

3.10 For RQ-9: Research Propositions for Guiding Industry Adoption of Sustainable Financing Strategies for AI-Ready Data Centers

Proposition – 1: Aligning Regulatory and Financial Incentives to Enable Sustainable AI-Driven Data Centers

Regions with stringent environmental regulations provide a strong foundation for aligning financial incentives with sustainable modernization goals for AI-ready data centers. For instance, governments in regions like Europe use tax credits, subsidies, and green bonds to incentivize investment in energy-efficient AI hardware and renewable energy integration. This alignment ensures operators can meet carbon neutrality goals while offsetting the high upfront costs of AI infrastructure upgrades. In regions with weaker regulatory frameworks, such as parts of North America or Southeast Asia, a lack of synchronized policy and financial incentives causes slower adoption of sustainable practices, limiting the potential for modernization.

Proposition – 2: Leveraging Energy-as-a-Service (EaaS) Models to Finance High-Density AI Workforce Computing

Energy-as-a-Service (EaaS) models allow data center operators to avoid high capital expenditure by outsourcing energy infrastructure development, such as renewable energy

systems and advanced cooling, to third-party providers. Operators pay for energy optimization through operational expenses, ensuring flexibility and reduced financial risk. This approach is particularly compelling for mid-sized data centers handling AI applications, which can utilize EaaS to address fluctuating workloads efficiently and sustainably. Observing the adoption of EaaS in emerging and mature markets can reveal its scalability and potential effectiveness in addressing AI-driven energy challenges.

Proposition – 3: The Role of Green Financing Tools in Scaling AI-Specific Infrastructure

Green financing tools, including green bonds, sustainability-linked loans, and carbon credits, provide the capital needed to fund the development of AI-centric data centers while linking financial outcomes to environmental performance metrics. The deployment of AI hardware such as GPUs and TPUs significantly increases power and cooling demands, prompting the need for financing mechanisms tied to renewable energy adoption and energy efficiency improvements. Evaluating the impact of green financing on high-density AI infrastructures can offer insights into how industries can achieve both computational growth and environmental sustainability simultaneously.

Proposition – 4: Encouraging Public-Private Partnerships (PPP) for AI-Centric Facilities in Emerging Markets

Public-private partnerships (PPP) play a pivotal role in financing AI-ready data centers in regions where private capital is limited, and infrastructural challenges prevail. PPPs enable shared risk between governments, private investors, and international organizations, offering access to funding for projects that integrate AI-capable hardware and sustainable practices. Emerging markets in Latin America, Sub-Saharan Africa, and South Asia benefit

particularly from PPP models, where international development funds and private investments collectively ensure the growth of AI infrastructure aligned with energy-efficient standards.

Proposition – 5: Exploring the Uniqueness of AI Workloads in Shaping Cooling System Financing

AI workloads generate high heat density from GPUs and TPUs, requiring advanced cooling solutions like liquid cooling or immersion cooling technologies. These systems are highly effective in managing thermal output but entail significant upfront costs, which often deter smaller operators. Targeted financing strategies, such as cooling-specific grants, subsidies, or cooling-as-a-service models, can help operators distribute costs over time while achieving mandatory efficiency goals. Future research could examine the regional adoption of innovative cooling finance models in climates with extreme temperatures or underdeveloped cooling technologies.

Proposition – 6: Regional Adaptation of Carbon Pricing and Trading Mechanisms to Fund AI-Ready Facilities

Carbon pricing mechanisms, such as carbon taxes and emissions trading systems, indirectly encourage sustainable practices in AI-ready data center development. These mechanisms incentivize operators to invest in renewable energy systems and energy-efficient hardware by linking carbon costs to operational inefficiencies. Mature markets like Europe have successfully utilized carbon pricing to drive sustainability efforts, but emerging regions with nascent carbon markets have been slower to adapt, highlighting opportunities for new financial instruments tailored to energy-intensive AI operations.

Proposition – 7: Fostering Cross-Sector Collaboration for Tailored Financing Mechanisms

Developing sustainable AI-ready data centers requires collaboration between private investors, government bodies, energy providers, and technology vendors. Cross-sector partnerships create opportunities for innovative financing models such as shared investment funds, co-lending programs, or customized renewable power purchase agreements (PPAs) tailored for AI workloads. Such collaborative approaches distribute financial risks while fostering advancements in energy efficiency and sustainability technologies, benefiting both public and private stakeholders. Observing these collaborations offers insights into how multi-stakeholder models can support AI-driven modernizations on a large scale.

Proposition – 8: Standardized Metrics for Financing AI-Ready, Sustainable Facilities

The lack of standardization in sustainability metrics for AI workloads creates challenges in designing financing mechanisms. Existing metrics like Power Usage Effectiveness (PUE) fail to capture the complexity and intensity of AI applications. The development of AI-specific benchmarks, such as energy-per-operation efficiency or AI-optimized PUE, would allow financiers to assess the environmental performance of AI-centric data centers more accurately. Adoption of such standards across industries would foster transparency, aid financial decision-making, and improve alignment with sustainability objectives in AI facility modernization.

CHAPTER IV

DISCUSSION IN THE CONTEXT OF CIS AND RECOMMENDATIONS

4.1. AI-Ready Data Centers for Safeguarding CIS

The analysis underscores the critical need for tailored, sustainable financing strategies to support the adoption and modernization of AI-ready data centers that safeguard critical infrastructure sectors, including energy, transportation, healthcare, telecommunications, and defense. These facilities serve as an operational backbone for real-time data analytics, anomaly detection, predictive maintenance, and disaster response, making their resilience and environmental sustainability paramount.

The following key results emerge from this research:

4.1.1 Integration of Regulatory and Financial Incentives

Regulatory frameworks must be aligned with modern financing instruments, such as subsidies, green bonds, and tax credits, to incentivize the development of energy-efficient data centers supporting critical infrastructure. Facilities designed for tasks such as grid monitoring, cybersecurity, and healthcare analytics should benefit from policies that encourage operational reliability alongside carbon neutrality, ensuring these sectors meet both environmental and security mandates.

4.1.2. Adoption of Energy-as-a-Service Models

Innovative financing models, particularly Energy-as-a-Service (EaaS), demonstrate the potential to alleviate the financial burden of capital-intensive energy systems—such as

renewable integrations and advanced cooling technologies—necessary for AI-ready data centers. EaaS offers flexible, operating-expense-driven solutions that are especially advantageous for mission-critical infrastructure sectors requiring sustainable, uninterrupted service delivery.

4.1.3 Scaling Infrastructure through Green Financing Tools

Instruments such as green bonds and sustainability-linked loans are effective mechanisms for funding the expansion of data centers while maintaining environmental accountability. Performance-based terms tied to reductions in energy consumption or increased renewable energy sourcing can ensure the scalability of AI-driven data centers used in sectors such as healthcare (e.g., bio-surveillance) or smart grids (e.g., energy flow optimization).

4.1.4 Public-Private Partnerships (PPP) as a Key Enabler

Public-private collaborations are essential to drive the development of AI infrastructure in resource-constrained or emerging regions. Critical services such as water utilities, telecommunications, and transportation networks require significant co-investment to modernize AI capabilities while integrating sustainability features. PPPs provide a pathway to share financial and operational responsibilities, particularly in regions facing infrastructural development challenges.

4.1.5 Investment in Advanced Cooling Technologies

AI workloads powering critical infrastructure generate significant heat, necessitating highly efficient cooling systems like liquid cooling or immersion cooling. Specific financing models, including cooling-as-a-service or cooling-specific grants, are integral for

ensuring operational safety and sustainability under increasingly dense and complex AI applications supporting national security or real-time disaster response systems.

4.1.6 Carbon Pricing as a Modernization Incentive

Carbon pricing mechanisms, including emissions trading systems, prove to be invaluable in fostering environment-friendly AI-ready data center modernization. Data centers supporting critical infrastructure sectors such as transportation and manufacturing can utilize these pricing frameworks to fund energy-efficient upgrades and AI-driven sustainability measures. Such mechanisms ensure alignment between operational modernization and regional emissions goals.

4.1.7 Cross-Sector Collaboration for Financing Resiliency and Sustainability

Co-lending programs and multi-stakeholder investments between public entities, private investors, technology developers, and energy providers emerge as strategic solutions for safeguarding critical sectors. Tailored projects, such as renewable power purchase agreements for AI data centers supporting disaster preparedness or emergency management systems, highlight the importance of collaboration in achieving dual objectives of environmental sustainability and infrastructure resiliency.

4.1.8 Need for Standardized Metrics

Existing efficiency metrics such as Power Usage Effectiveness (PUE) fail to fully encapsulate the operational demands of critical infrastructure-centric AI data centers. Developing standardized metrics, such as energy-per-critical-operation efficiency or resilience-specific benchmarks, will enable lenders and stakeholders to make informed financial and operational decisions. Metric innovation is particularly essential to financing

projects in regions with unique vulnerabilities, such as drought, flooding, or cybersecurity risks.

4.2. Insights on Resilience and Safeguarding Mechanisms for Critical Infrastructure Sectors Through Sustainable AI-Ready Financing

AI-ready data centers provide an indispensable layer of security and operational continuity for critical infrastructure sectors. However, the modern challenges of climate volatility, cyber risks, and burgeoning workloads necessitate designing and financing these facilities with resilience as a foundation. Sustainable financing models must address infrastructure redundancy, advanced cooling, decentralized designs, secure frameworks, disaster readiness, and sustainability metrics to protect these critical systems.

The synergy between sustainable financing approaches—such as green bonds, EaaS models, PPPs, and carbon incentives—and resilience measures can ensure that data centers evolve into highly reliable hubs driving the secure, efficient, and environmentally responsible operation of essential services. By linking financial mechanisms to resilience-focused outcomes, stakeholders can safeguard vital sectors while aligning with global sustainability priorities.

Given the increasing dependence of critical infrastructure sectors on AI systems, ensuring resilience and safeguarding mechanisms through AI-ready data centers is paramount. Appropriately developed sustainable financing strategies must aim not only at enhancing energy efficiency or addressing environmental sustainability but also at fortifying the nation's critical services against disruptions, cyber threats, and natural disasters. AI's role in building resiliency often intersects with the infrastructural reliability of data centers, where these systems must operate under immense computational demand in secure, sustainable, and fail-safe environments. Below are key insights that emphasize

the inextricable linkage between resilience, safeguards, and sustainable financing models for these essential entities.

4.2.1 Resilience Against Disruption Through Robust and Secure Infrastructure

Critical infrastructure sectors, such as power grids, healthcare networks, water utilities, and transportation systems, are highly interconnected and dependent on real-time data processed through AI-ready data centers.

For example, smart grid systems use AI to predict outages, optimize energy flow, and detect cybersecurity threats. Similarly, AI is revolutionizing logistics and monitoring in healthcare for identifying disease outbreaks and supporting public safety in disaster response. To ensure continuous resilience, AI-ready data centers must be designed with safeguards against both natural and human-induced disruptions.

Financing models should explicitly account for the costs of redundant systems, backup energy sources (e.g., microgrids or battery storage), and advanced cooling mechanisms that reduce failure points during high-intensity operations. Resilience-focused incentives, such as financing for distributed energy systems, fault-tolerant hardware, or site redundancy in disaster-prone areas, can help critical sectors avoid single points of failure and ensure uninterrupted service. Governments and financing bodies can also introduce region-focused resilience grants for AI-powered emergency response systems.

For instance, in hurricane-prone areas, AI-driven predictive models integrated with robust facilities could use advanced geospatial analytics to coordinate preemptive evacuations or optimize resource distribution.

4.2.2 Mitigating Cyber Threats with Intelligence-Driven Security Architecture

The growing reliance on AI-powered data centers for critical services inevitably elevates the exposure of these systems to cyber-attacks. Threats such as ransomware targeting energy grids or transportation systems—both of which rely on real-time AI analytics—demand specialized investments in cybersecurity safeguards for data centers. Financing sustainable AI-ready data centers should integrate cost considerations related to cybersecurity at the infrastructure level, including zero-trust architecture implementation, deep learning-based anomaly detection models, and AI-driven encryption technologies. For example, AI-based data centers used for safeguarding financial institutions could integrate machine learning for real-time fraud detection or blockchain technologies for transaction security, both of which require massive computing power paired with sustainable operation. Sustainable financing models, such as cybersecurity as a service coupled with green bonds or operational expenditure (OPEX)-based approaches, can reduce the upfront costs of integrating these safeguards into modern AI-capable facilities.

4.2.3 Operational Resilience Through Low-Latency and Decentralized Models

Centralization of critical data processing in hyperscale facilities poses significant risks in the event of a localized failure, whether due to power outages, physical disruptions (e.g., earthquakes), or cyber-attacks. For instance, AI systems used to monitor smart water utilities or national transportation grids require extremely low-latency data transmissions for predictive alerts and anomaly responses. A failure in a centralized location can cascade across dependent sectors, amplifying disruptions. Decentralized and edge-computing AI data centers offer an essential safeguard by allowing critical infrastructure sectors to process data closer to the source, reducing latency and creating redundancy. Financing resilient, decentralized AI-ready hubs must address unique challenges, ranging from

deploying renewable power in remote locations to providing distributed networks with low PUE (Power Usage Effectiveness) and high reliability. For example, governments could provide targeted subsidies for micro-edge hubs or public-private partnerships (PPPs) that bring solar-powered edge data centers to rural areas providing critical services like remote healthcare or environmental monitoring.

4.2.4 Resilience in Disaster Recovery through AI-Enhanced Predictive Capabilities

Resilience-focused financing for AI-ready data centers can be tied to their capacity to facilitate real-time decision-making during disasters or other extreme events. AI is being increasingly utilized to detect environmental irregularities (e.g., earthquakes, floods, heatwaves) through IoT systems and satellite monitoring, which depend on the computational strength of corresponding data centers. AI-ready facilities need to deploy failover mechanisms, disaster recovery protocols, and region-specific hazard mitigation strategies to protect critical sectors during crises. Financing resources should incentivize predictive disaster systems leveraging AI to integrate renewable energy for grid independence and ensure operational continuity. For example, smart city disaster systems monitoring transportation, energy, and water networks can be funded through green loans tied to establishing resilient standalone energy infrastructures such as solar microgrids. Such modernization ensures systems remain operational and self-sustaining, even during widespread outages.

4.2.5 Resilience via Heat-Resistant Cooling Systems for High-Density AI Workloads

The heat-intensive computing demands of AI workloads pose a direct risk to the hardware resilience of data centers that support critical infrastructure. Extreme weather patterns exacerbated by climate change, such as heatwaves, place further strain on already energy-

intensive cooling systems. AI-ready data centers safeguarding critical services like power grid monitoring require reliable high-performance cooling systems, such as liquid cooling or immersion cooling. Sustainable financing mechanisms can target these critical investments by introducing region-specific "resilience grants" or performance-based incentives that reward facilities delivering efficient cooling solutions under adverse conditions. For instance, advanced cooling methods integrated into AI-ready hubs supporting national energy grids would ensure processing remains uninterrupted at peak computing loads, even during extreme environmental conditions. Developing cooling-as-a-service financing could spread capital costs over operational use, reducing resource barriers to adopting cutting-edge solutions while protecting critical services.

4.2.6 Regional Adaptation of Carbon Pricing and Sustainability Incentives for Infrastructure Safeguards

Critical sectors rely on AI-ready data centers not only to optimize their operations but also to address sustainability challenges directly tied to carbon emissions. State regulatory pricing schemes could incentivize the use of AI-driven sustainability mechanisms such as AI-based carbon monitoring in transportation grids or energy-efficient routing in logistics networks. Integrating carbon pricing systems into data centers utilized by these sectors further ensures operational alignment with climate regulations while capturing incentives for modernization. Such policy-driven adaptation, especially in regions with high infrastructure dependency on fossil fuels, brings ecological and operational resilience into focus. Research into carbon trading models that benefit data centers interfacing with smart grids or intelligent transportation systems could reveal scalable solutions to ensure sustainability ecosystems tied to essential public services.

4.2.7 Building Institutional and Infrastructure Resilience via Cross-Sectoral Collaboration

The collaboration between government agencies, technology providers, utility companies, and financial institutions can significantly enhance the resilience of AI-ready data centers safeguarding critical infrastructure. For example, partnerships could incentivize co-funded installations of backup renewable energy sources, such as wind or battery systems, at data centers involved in critical resource management. Shared-risk financing approaches, such as multi-stakeholder investment pools or public-private investment funds, can create solutions tailored to the resilience needs of specific sectors like healthcare, energy, or transportation while also ensuring sustainability requirements. A collaborative approach ensures resilience measures remain cost-effective and scalable by balancing resource inputs from different partners. For example, a utility provider could combine renewable energy solutions with a technology company's deployment of AI-driven data monitoring for safety-critical infrastructure, supported by public financing tied to green infrastructure initiatives.

4.3. The integration of AI-ready data centers and Financing Routes for each USA Critical Infrastructure

The integration of AI-ready data centers designed specifically for each U.S. Critical Infrastructure Sector (CIS) has the potential to revolutionize security, operational efficiency, and resilience. This section highlights the sector-specific applications, insights, and resulting recommendations from an evaluation of AI-ready infrastructure across the 16 DHS-classified critical infrastructure sectors. These results act as a foundation for enhancing cybersecurity and operational functionality in critical systems while addressing sectoral constraints.

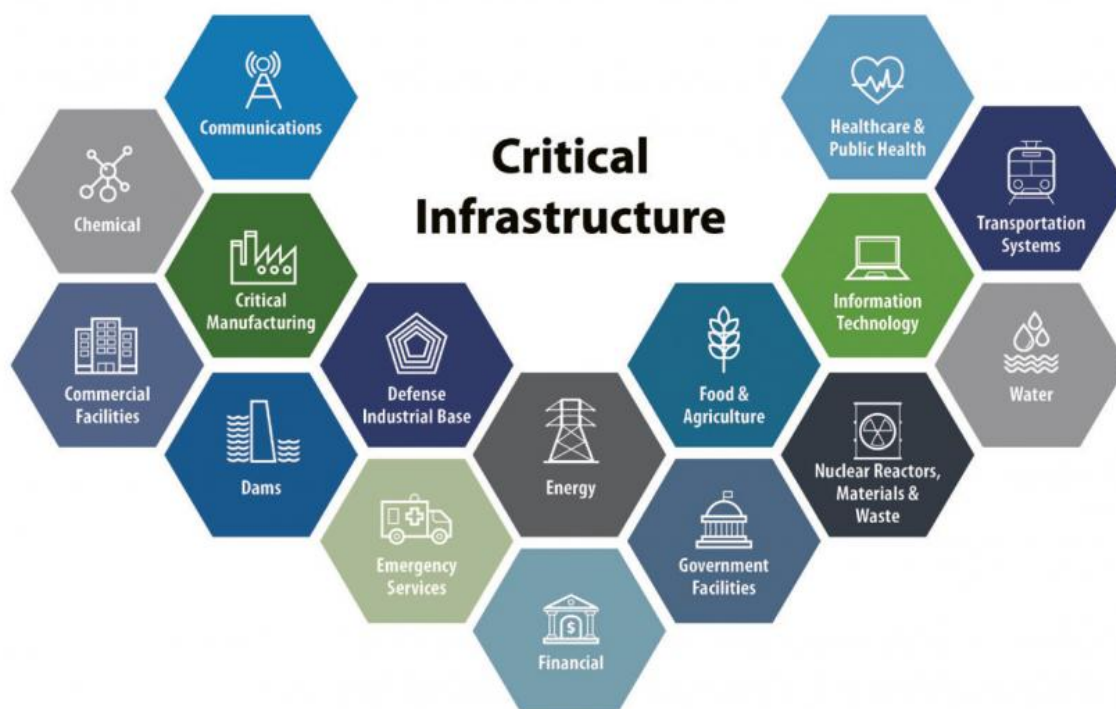


Figure 4.1. 16 critical infrastructure sectors essential for national security, economic stability, and public health in USA. Source: Cybersecurity and Infrastructure Security Agency (CISA)

4.3.1 Chemical Sector

AI-ready data centers tailored for the chemical sector must prioritize real-time analytics and predictive maintenance systems, ensuring process safety and operational efficiency. By integrating advanced machine learning models, facilities can continuously monitor hazardous materials and detect anomalies indicative of leaks, unauthorized access, or equipment failures. It is recommended that robust cybersecurity protocols, aligned with the Chemical Facility Anti-Terrorism Standards (CFATS), be implemented to address vulnerabilities. Additionally, incorporating privacy-preserving technologies ensures that

proprietary production data remains secure. AI-driven predictive analysis will also improve compliance and reduce downtime in chemical manufacturing facilities.

The preferable sustainable finance route is Green Bonds via Environmental, Social, and Governance (ESG) Funding. Green bonds can fund safety and AI infrastructure upgrades in chemical facilities, including environmental monitoring and predictive analytics for hazards using AI. Issued by companies focusing on reducing chemical-related environmental impacts, this route ensures the funds attract ESG-driven investors. As per the methodology provided in section 2.3 of chapter 2 the feasibility score of preferred sustainable finance route is 8/10. Chemical companies benefit from structured ESG-backed financing, but regulatory concerns about hazardous material monitoring may limit investor interest.

4.3.2 Commercial Facilities Sector

For commercial facilities such as malls, stadiums, and convention centers, implementing AI-ready data centers enables real-time surveillance, crowd monitoring, and advanced threat detection. Facial recognition technology integrated with scalable AI models can significantly enhance security screening processes. Enhanced coordination with emergency services is vital for event-based risk detection, and it is recommended that scalable storage systems be implemented to process crowd-related data. Privacy compliance with frameworks like GDPR or CCPA must also be a focus given the use of surveillance technologies in public spaces.

The preferable sustainable finance route is Public-Private Partnerships (P3s). Financing secured through P3 models allows governments to collaborate with private entities in funding AI-ready data centers for mass surveillance, infrastructure improvement, and public safety at major commercial hubs. As per the methodology provided in section

2.3 of chapter 2 the feasibility score of preferred sustainable finance route is 9/10. The collaborative nature of P3s aligns financial and operational goals, but integration of AI systems with privacy laws could add complexities.

4.3.3 Communications Sector

AI-ready infrastructure within the communications sector enables deep learning-based traffic analysis to secure telecommunication networks against Distributed Denial of Service (DDoS) attacks and unauthorized intrusions. The ability to process massive streams of real-time data through latency-optimized architectures is essential for maintaining service reliability. Blockchain can further enhance trust by securing communication logs. It is recommended that compliance with Federal Communications Commission (FCC) policies and standards be maintained and that data centers implement fault-tolerant systems to ensure uninterrupted service in emergencies.

The preferable sustainable finance route is Infrastructure Investment via Venture Capital and Innovation Grants. AI-driven communication data centers funded through venture capital can attract firms focused on digital infrastructure. Complementary innovation grants from federal programs (e.g., FCC or Department of Commerce) can ensure compliance. As per the methodology provided in section 2.3 of chapter 2 the feasibility score of preferred sustainable finance route is 8/10. The sector's demand for continuous innovation matches the goals of private venture capitalists, though dependence on returns may limit public investment.

4.3.4 Critical Manufacturing Sector

AI-enabled solutions in manufacturing significantly enhance efficiency and security by leveraging predictive maintenance and real-time production analytics. AI-ready data

centers imbued with edge capabilities can analyze signals from industrial IoT (IIoT) devices, ensuring interoperability with operational technology (OT) systems. To protect against cyber threats targeting manufacturing control systems, adherence to ISA/IEC 62443 standards is recommended. Edge data centers are particularly effective for latency reduction and dynamic manufacturing adjustments.

The preferable sustainable finance route is Industry-Specific ESG Loans. ESG-linked loans tailored to industrial efficiencies, particularly in reducing manufacturing waste through AI-driven predictive maintenance, are an effective sustainable financial option. These loans reward companies for meeting sustainability benchmarks. As per the methodology provided in section 2.3 of chapter 2 the feasibility score of preferred sustainable finance route is 7/10. While loans tied to ESG benchmarks are attractive, volatile industrial cycles in manufacturing may make lenders cautious.

4.3.5 Dams Sector

The dams sector benefits greatly from real-time AI-driven structural monitoring and predictive disaster modeling. Machine learning models integrated into data centers can analyze telemetry data about water levels, flow rates, and structural stability. Flood simulations and predictive risk assessments can inform disaster response plans. It is recommended to maintain geographically distributed backup systems for redundancy and ensure full integration with emergency response frameworks to enhance operational resilience.

The preferable sustainable finance route is Municipal Sustainability Bonds. Municipalities issuing sustainability bonds for dam maintenance and AI-driven disaster prediction systems can secure funding while promoting climate resilience. Such bonds explicitly target environmental impact and climate risk mitigation. As per the methodology

provided in section 2.3 of chapter 2 the feasibility score of preferred sustainable finance route is 9/10. Municipal green bonds are highly suitable, as public interest strongly favors sustainable water management and disaster resilience.

4.3.6 Defense Industrial Base Sector

The defense industrial sector requires highly secure AI-ready data centers capable of detecting and mitigating cyber threats while managing sensitive supply chain data. Sandboxed AI environments offer controlled spaces for testing defense-related algorithms and tools, while blockchain can secure defense contracts and logistics data. It is recommended to develop infrastructure compliant with Defense Federal Acquisition Regulation Supplement (DFARS) standards and integrate real-time cybersecurity measures to prevent breaches of sensitive defense data.

The preferable sustainable finance route is Federal Defense Grants and Public R&D Funds. AI funding for defense infrastructure can come from federal defense budgets, R&D appropriations, and collaboration with defense contractors under pre-approved public funding programs. As per the methodology provided in section 2.3 of chapter 2 the feasibility score of preferred sustainable finance route is 10/10. Defense funding is traditionally well-supported by federal programs, particularly for integrating advanced technologies like AI.

4.3.7 Emergency Services Sector

In the emergency services sector, AI-ready data centers streamline disaster response strategies, resource deployment, and predictive modeling of disaster scenarios. AI-driven decision-making is particularly effective for fire predictions, resource allocation, and real-time environmental monitoring via drones and GIS systems. To address the unpredictable

nature of emergencies, it is recommended that data centers employ redundant failover systems to ensure uninterrupted operation during crises. Facilitating interoperable platforms for coordination between agencies will drastically enhance emergency response outcomes.

The preferable sustainable finance route is Federal Disaster Relief and Recovery Funds. AI-ready data centers supporting emergency services can be financed by disaster recovery programs, such as FEMA grants, which align with the need for better real-time mapping and disaster responsiveness. As per the methodology provided in section 2.3 of chapter 2 the feasibility score of preferred sustainable finance route is 9/10. Programs like FEMA grants seamlessly align with the sector's objectives but may suffer delays in response to bureaucratic funding approvals.

4.3.8 Energy Sector

The energy sector requires robust AI-ready data centers for processing real-time data from smart grids, sensors, and distributed energy resources. Predictive maintenance powered by AI reduces downtime and optimizes energy distribution. Blockchain technology can enhance network transparency and secure energy transactions, but challenges related to the scalability of both AI and blockchain architectures must be addressed. Recommended solutions include deploying energy-efficient data center designs and ensuring compliance with NERC-CIP standards to protect critical components of electricity networks, oil, and gas pipelines.

The preferable sustainable finance route is Green Bonds and Carbon Offset Mechanisms. Financing AI-ready centers in energy distribution can leverage energy-focused sustainability funds or carbon offset-backed green bonds, particularly for companies driving renewable energy deployment alongside AI adoption. As per the

methodology provided in section 2.3 of chapter 2 the feasibility score of preferred sustainable finance route is 9/10. The growing investor interest in renewable energy and smart grids makes green bonds an excellent route. However, technical scalability for AI application in the grid remains a concern.

4.3.9 Financial Services Sector

The financial services sector requires AI-powered solutions for fraud detection, real-time data analysis, and ensuring the integrity of online transactions. AI-ready data centers should support high-frequency trading algorithms and secure financial logs through blockchain. Scalable AI solutions are essential for addressing the rapid growth of transaction volumes. It is recommended to maintain compliance with financial regulations such as FISMA and the GDPR, prioritize data encryption, and implement low-latency architectures to facilitate seamless online financial services.

The preferable sustainable finance route is Institutional ESG Investments. Banks, fintech organizations, and asset managers can utilize institutional ESG investors to finance the adoption of AI-ready cybersecurity solutions. This financing route aligns well within the financial sector's regulated environment. As per the methodology provided in section 2.3 of chapter 2 the feasibility score of preferred sustainable finance route is 8/10. ESG investments efficiently meet sector needs but may involve strict compliance and risk assessment measures by institutional investors.

4.3.10 Food and Agriculture Sector

AI-ready data centers in the food and agriculture sector enhance supply chain transparency, yield predictions, and pest detection through advanced data analysis. IoT-enabled farms require scalable data facilities for real-time monitoring and resource optimization. To

prevent disruptions, infrastructure must integrate predictive analytics for crop health and production logistics. It is recommended to implement blockchain for ensuring supply chain integrity and develop adaptive AI algorithms capable of handling seasonal variations and environmental hazards.

The preferable sustainable finance route is Agricultural Sustainability Subsidies and Private Impact Investments. Financing through agricultural sustainability programs subsidized by USDA or private impact investors targeting precision farming initiatives is ideal. Integrating AI for supply chain transparency and resource optimization also appeals to green-focused funding. As per the methodology provided in section 2.3 of chapter 2 the feasibility score of preferred sustainable finance route is 7/10. The sector benefits from focused sustainability initiatives, although smaller stakeholders may struggle to secure private funding.

4.3.11 Government Facilities Sector

AI-ready data centers for government facilities enable enhanced building management systems and real-time surveillance to detect suspicious behaviors or unauthorized accesses. AI-supported systems must ensure compliance with Federal Risk and Authorization Management Program (FedRAMP) policies to protect sensitive government data. Recommendations include deploying scalable platforms for facility management and integrating advanced access control systems to secure government buildings.

The preferable sustainable finance route is Federal Grants and State Bonds. Federal grants targeting smart government facilities and secure building management systems, along with state-issued construction bonds, can fund AI-ready data centers effectively. As per the methodology provided in section 2.3 of chapter 2 the feasibility score of preferred

sustainable finance route is 9/10. Government funding mechanisms align entirely with public infrastructural goals, but bureaucratic delays may impact timelines.

4.3.12 Healthcare and Public Health Sector

AI data centers in healthcare enable real-time patient monitoring, advanced imaging analysis, and predictive diagnostics. Privacy preservation must be a priority, ensuring compliance with HIPAA and HITECH standards. Federated learning and differential privacy mechanisms are recommended to analyze sensitive medical data securely. Integration with blockchain systems can further enhance medical data integrity while enabling seamless, secure exchanges of electronic health records between institutions.

The preferable sustainable finance route is Health-Specific Impact Funds/Green Health Bonds. Impact funds directed at public health technology or green health bonds can fund AI-enabled systems for electronic health records (EHR) and diagnostics. Collaboration with large health insurance firms can also facilitate funding. As per the methodology provided in section 2.3 of chapter 2 the feasibility score of preferred sustainable finance route is 8/10. Although healthcare-focused funds attract investment, their regulated environment may restrict flexibility in application.

4.3.13 Information Technology Sector

Safeguarding IT systems necessitates AI-ready data centers designed to handle network anomalies and insider threats. AI capabilities for real-time intrusion detection are critical, and blockchain can enhance audit transparency. Virtualized environments within the data center can ensure scalability and maintain operation during peak demands. It is recommended to align data handling practices with NIST and ISO 27001 for strong cybersecurity foundations.

The preferable sustainable finance route is Private Venture Capital Funds and IT Innovation Loans. Venture capital investment into AI cybersecurity for IT systems can dominate financing, complemented by innovation loans from federal programs targeting critical IT innovation. As per the methodology provided in section 2.3 of chapter 2 the feasibility score of preferred sustainable finance route is 9/10. The continuous demand for technological advancements makes this funding universally applicable and sustainable.

4.3.14 Nuclear Reactors, Materials, and Waste Sector

The nuclear sector relies on AI-ready data centers for monitoring reactor safety and managing radiation data. Efficient computational models can predict equipment failures and radiation leaks in real-time. Blockchain should be utilized to secure nuclear waste logistics. AI models and data centers in this sector must comply with Nuclear Regulatory Commission (NRC) safety guidelines and integrate redundant systems to maintain operational resilience.

The preferable sustainable finance route is Federal Energy Subsidy Programs. AI-enabled systems for managing nuclear reactors and waste logistics can be financed via federal energy sustainability or resilience programs designed for critical national infrastructure. As per the methodology provided in section 2.3 of chapter 2 the feasibility score of preferred sustainable finance route is 8/10. While federal subsidies are stable funding sources, public resistance to nuclear energy projects may create higher political scrutiny.

4.3.15 Transportation Systems Sector

AI-driven data centers in transportation systems enhance efficiency through traffic optimization, real-time fleet tracking, and logistical support. Distributed AI models

deployed at transport hubs reduce latency in maritime logistics and aviation. Blockchain can improve supply chain transparency, while compliance with Department of Transportation (DOT) regulations is critical. Recommendations include adopting edge-data facilities for localized processing and streamlining integration with existing logistics software.

The preferable sustainable finance route is Infrastructure Trust Funds and Public-Private Partnerships (P3s). Funding for AI-ready solutions in transportation should come from infrastructure-specific trust funds, such as the Highway Trust Fund, alongside P3s for railways and maritime logistics. As per the methodology provided in section 2.3 of chapter 2 the feasibility score of preferred sustainable finance route is 10/10. Federally backed transportation funds incentivize private involvement and align with public demands for efficient and secure systems.

4.3.16 Water and Wastewater Systems Sector

AI-ready data centers for water systems improve water quality monitoring, distribution management, and contamination detection. Predictive maintenance of pipelines and water treatment facilities ensures reliability. Recommendations include integrating decentralized edge computing for real-time data analysis at remote facilities and adopting robust encryption methods for securing sensitive water data. Adding redundancy will further enhance resilience against cyber-attacks.

The preferable sustainable finance route is Green Municipal Water Bonds. Municipalities can issue green water bonds specifically targeting AI systems for water quality monitoring, contamination prediction, and predictive maintenance in distribution networks. As per the methodology provided in section 2.3 of chapter 2 the feasibility score of preferred sustainable finance route is 9/10. Significant potential exists with public

demand for clean water security and operational efficiency, though rural systems may face financing limitations.

Table 4.1. Financial routes with feasibility score for AI ready data center in 16 critical infrastructure sectors in USA

Sector	Finance Route	Feasibility Score
Chemical	Green Bonds via ESG Funding	8/10
Commercial Facilities	Public-Private Partnerships (P3s)	9/10
Communications	Venture Capital and Innovation Grants	8/10
Critical Manufacturing	Industry-Specific ESG Loans	7/10
Dams	Municipal Sustainability Bonds	9/10
Defense Industrial Base	Federal Defense Grants	10/10
Emergency Services	Federal Disaster Relief/Recovery Funds	9/10
Energy	Green Bonds and Carbon Offset Mechanisms	9/10
Financial Services	Institutional ESG Investments	8/10

Food and Agriculture	Impact Investments/Agricultural Subsidies	7/10
Government Facilities	Federal and State Grants/Bonds	9/10
Healthcare and Public Health	Health-Specific Private Impact Funds	8/10
Information Technology	Venture Capital and IT Loans	9/10
Nuclear Reactors & Waste	Federal Energy Subsidy Programs	8/10
Transportation Systems	Trust Funds, Public-Private Partnerships	10/10
Water and Wastewater Systems	Green Municipal Water Bonds	9/10

4.4. The integration of AI-ready data centers and Financing Routes for each Critical Infrastructure in Australia

The integration of AI-ready data centers within Australia's 11 critical infrastructure sectors presents a transformative pathway to enhance operational efficiency, bolster resiliency against emerging threats, and future-proof vital systems. AI-ready data centers are equipped with advanced computational power, machine learning capabilities, and robust cybersecurity frameworks to enable the real-time analysis and management of data. This section explores the role of AI-ready data centers in each sector and identifies sustainable financing routes tailored to the needs and challenges of these critical infrastructures. The

proposed financial strategies take into account Australia's regulatory frameworks, sustainability commitments, and sector-specific dynamics.

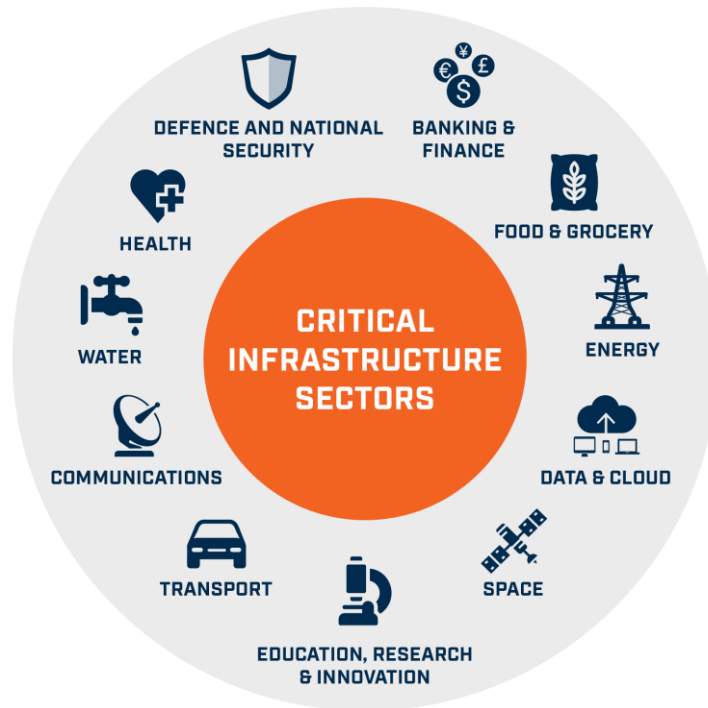


Figure 4.2. 11 critical infrastructure sectors in Australia. Source: Australian Cyber Security Strategy 2020

4.4. 1. Communications Sector

The scope of this sector includes telecommunications, broadcasting, and domain name systems. AI-ready data centers can analyze and automate network traffic management, ensuring minimal latency and mitigating risks such as Distributed Denial of Service (DDoS) attacks. AI systems enable real-time health monitoring of communication infrastructure, predictive maintenance, and anomaly detection in large-scale networks, essential for maintaining Australia's telecommunications backbone. The preferred Financing Route could be Innovation Grants and Public-Private Partnerships (P3s) and as

per the methodology presented section 2.3 of chapter 2 the feasibility score is 8.5/10. Innovation grants, potentially offered through government programs such as the Communications Infrastructure Fund, would catalyze AI-driven modernization. Public-private partnerships can secure additional capital by leveraging private telecom firm investments.

4.4.2. Financial Services and Markets

The scope of this sector includes Banking, insurance, and superannuation. AI-ready infrastructure enables fraud detection, advanced risk assessment, and high-frequency financial transactions. Machine learning algorithms can process vast amounts of financial data to prevent fraud and predict market risks, while blockchain technology ensures secure and transparent transactions. AI also plays a role in optimizing consumer credit scoring systems and improving compliance with financial regulations. The preferred Financing Route could be Institutional ESG (Environmental, Social, and Governance) Investments and as per the methodology presented section 2.3 of chapter 2 the feasibility score is 9/10. Australia's globally recognized superannuation funds increasingly prioritize ESG-compliant investments, providing scalable capital for AI-driven upgrades in fraud detection, financial risk assessment, and secure transactions. The integration of AI-ready data centers into Australia's financial infrastructure aligns well with the ESG requirements of institutional investors. Minor scalability risks may emerge for smaller institutions unable to meet strict ESG compliance or deliver immediate high returns.

4.4.3. Data Storage or Processing Sector

The scope of this sector includes Data centers and cloud services. AI-ready data centers serve as essential hubs for Australia's data economy by providing reliable and secure cloud

hosting services. AI technologies facilitate load-balancing, reduce energy consumption through efficient resource allocation, and predict system failures to preemptively mitigate disruptions. Enhanced cybersecurity measures ensure protection against data breaches.

The preferred Financing Route could be Green Infrastructure Bonds and as per the methodology presented section 2.3 of chapter 2 the feasibility score is 8/10. These bonds attract sustainability-focused investors by financing energy-efficient data center projects powered by renewable energy sources such as wind or solar. Green bonds are ideally suited for AI-ready data centers powered by renewable energy, which aligns with Australia's Climate Active Carbon Neutral Standard. While investor sentiment toward sustainability elevates feasibility, green data centers face high upfront infrastructure and energy technology costs. Government-led incentives are required to reduce these initial barriers, complemented by public advocacy for renewable-powered storage solutions.

4.4.4. Defence Industry

The scope of this sector includes Suppliers and partners to the Australian Defence Force (ADF). AI-ready data centers within the defense sector provide real-time analytics for threat detection, military strategy optimization, and secure intelligence processing. Blockchain technology enables the secure transfer of sensitive mission data, while predictive analytics backed by AI improves supply chain efficiency for military equipment and resources. The preferred Financing Route could be Direct Federal Grants under Strategic Defense Initiatives and as per the methodology presented section 2.3 of chapter 2 the feasibility score is 10/10. Backed by federal budgets, such as through the AUKUS Security Agreement, these grants finance AI-centric systems critical to national security and reducing dependence on external technology suppliers. AI-ready data centers directly contribute to Australia's sovereign defense interests, including secure battlefield analytics,

supply chain optimization, and encrypted communications. The AUKUS partnership and strategic defense funding from the Australian government ensure significant regulatory and financial backing with minimal execution risks.

4.4.5. Higher Education and Research

The scope of this sector includes Universities and research institutions. AI-ready data centers empower academic institutions by providing computational resources for conducting large-scale research. They enable predictive modeling, machine learning, and cross-institutional collaboration. Federated learning mechanisms protect data privacy while facilitating knowledge-sharing among Australian universities. The preferred Financing Route could be Government Research Grants (e.g., NCRIS) and as per the methodology presented section 2.3 of chapter 2 the feasibility score is 8.5/10. Grants from the National Collaborative Research Infrastructure Strategy (NCRIS) can fund AI-ready data centers designed specifically for research purposes. Naming rights and university-private joint ventures provide supplemental financial pathways.

4.4.6. Energy Sector

The scope of this sector includes Electricity, gas, and liquid fuels. AI-ready data centers optimize energy grid performance via real-time monitoring and anomaly detection. They enable predictive maintenance of infrastructure, ensuring operational continuity while reducing energy wastage. AI drives renewable energy forecasting, aiding resource distribution and grid stabilization in line with Australia's Net Zero by 2050 goals. The preferred Financing Route could be Green Bonds and as per the methodology presented section 2.3 of chapter 2 the feasibility score is 9/10. Green bonds align with Australia's

decarbonization targets by financing AI-powered grid improvements, renewables integration, and energy efficiency projects.

4.4.7. Food and Grocery Sector

The scope of this sector includes Supply chain and logistics for essential goods. AI-ready data centers enhance supply chain traceability, monitor inventory in real-time, and reduce food wastage by optimizing transportation routes and predicting demand fluctuations. Predictive analytics ensure efficient transportation systems, reducing delays in the delivery of perishable goods. The preferred Financing Route could be Private Impact Investments and Federal Agricultural Subsidies and as per the methodology presented section 2.3 of chapter 2 the feasibility score is 7.5/10. Impact-driven private investments, coupled with federal government agricultural sustainability programs, help fund AI solutions for food and grocery supply chains.

4.4.8. Health Care and Medical

The scope of this sector includes Hospitals, medical supply systems, and public health infrastructure. AI-ready infrastructure supports predictive diagnostic tools, real-time health monitoring, and hospital logistics. AI systems optimize hospital workflows, secure medical records using blockchain, and improve the accessibility of telehealth services. Federated data processing protects sensitive medical data used in healthcare research and personalized medicine. The preferred Financing Route could be Health Impact Bonds and as per the methodology presented section 2.3 of chapter 2 the feasibility score is 8/10. These bonds attract private investment in projects that expand AI-based healthcare services, with returns tied to improved patient outcomes and healthcare efficiency.

4.4.9. Space Technology

The scope of this sector includes Satellites and ground-based space infrastructure. AI-ready data centers analyze satellite data for defense, telecommunications, environmental tracking, and space exploration purposes. Machine learning aids in optimizing satellite operations and preventing collisions during launch or placement in orbit. The preferred Financing Route could be Public-Private Partnerships (P3s) in Space Initiatives and as per the methodology presented section 2.3 of chapter 2 the feasibility score is 8.5/10. P3s can pool funding from government space programs and private enterprises involved in Australia's growing space sector.

4.4.10. Transport Sector

The scope of this sector includes Aviation, maritime, freight, and public transport. AI-ready data centers improve logistics efficiency, monitor traffic flow, and predict maintenance needs for large transport infrastructures. Integration with IoT sensors enables real-time condition monitoring for trains, ports, and roads to actively prevent delays and accidents. The preferred Financing Route could be Infrastructure Trust Funds and Public Mechanisms and as per the methodology presented section 2.3 of chapter 2 the feasibility score is 9.5/10. Transport trust funds, coupled with infrastructure-based public-private collaborations, ensure funding for smart transportation systems.

4.4. 11. Water and Sewerage Sector

The scope of this sector includes Water supply and waste management. AI-ready data centers enable real-time monitoring of water distribution systems to detect leaks or contamination. Predictive models enhance drought management strategies, ensuring consistent supply during extreme weather conditions, while AI-driven waste management

systems optimize recycling processes. The preferred Financing Route could be Green Municipal Bonds and as per the methodology presented section 2.3 of chapter 2 the feasibility score is 9.5/10. Municipal bonds targeted at water sustainability projects attract ESG-focused investors.

Table 4.2. Financial routes with feasibility score for AI ready data center in 11 critical infrastructure sectors in Australia

Sector	Proposed Financing Route	Feasibility Score	Rationale
Communications	Innovation Grants and P3s	8.5/10	Strong alignment with Australia's National Broadband Network (NBN) initiatives & innovation funding programs but execution complexity linked to private partnerships reduces full feasibility.
Financial Services	Institutional ESG Investments	9/10	Superannuation-driven ESG funding provides ample scalability and alignment with fintech modernization projects, though investment may prioritize immediate

			returns over long-tail strategies.
Data Storage	Green Infrastructure Bonds	8/10	Strong alignment with sustainability goals (e.g., renewable energy-powered data centers), though initial deployment costs may remain a concern even with green bond financing.
Defence Industry	Federal Grant Funding	10/10	Direct alignment with security policy under AUKUS and long-term strategic funding reduces all scalability and execution risks for AI data infrastructure in defense systems.
Higher Education	Research Grants through NCRIS	8.5/10	Well-aligned with academic and research priorities, though limited grant pools and competition among

			universities hinder broader scalability.
Energy	Green Bonds and Carbon Markets	9/10	Outstanding alignment with Net Zero 2050 goals, strong investor sentiment, and government alignment drive feasibility; partial risk stems from renewables' reliability and pay-back risk.
Food and Grocery	Private Impact Investments	7.5/10	High sectoral alignment, especially for AI-driven farming initiatives, but smaller agricultural businesses may find it hard to access private investment without supplementary subsidies.
Healthcare	Health Impact Bonds	8/10	Tightly aligned with public health reform goals, especially AI-driven diagnostics/telemedicine. However, back-end

			implementation (e.g., privacy/security concerns) introduces complexities.
Space Technology	Public-Private Partnerships (P3s)	8.5/10	Growing public-private synergy in Australia's space infrastructure ecosystem; however, reliance on private players could create execution bottlenecks in capital-intensive sectors.
Transport	Infrastructure Trust Funds	9.5/10	Infrastructure-specific trust funds aligned with federal/state transportation improvement goals achieve exceptional scalability for integrating AI.
Water and Sewerage	Green Municipal Bonds	9.5/10	Outstanding alignment with Australia's water scarcity priorities and public interest, streamlined by effective

			governance models at municipal levels.
--	--	--	---

4.5. The Integration of AI-Ready Data Centers and Financing Routes for Each EU Framework Critical Infrastructure

The European Union (EU) Critical Infrastructure framework, guided by directives such as the CER Directive (2022/2557) and NIS2 Directive (2022/2555), emphasizes both physical resilience and cybersecurity to safeguard its critical infrastructure against evolving threats. With the inclusion of emerging areas such as digital infrastructure and space, the integration of AI-ready data centers provides an operational backbone for addressing vulnerabilities through advanced automation, real-time analytics, and secure data storage. AI-enabled systems offer predictive maintenance, real-time decision-making support, and enhanced resource optimization, which strengthen the resilience and efficiency of these critical systems. This section examines the role of AI-ready data centers in each sector defined under the EU critical infrastructure framework and identifies viable financing routes tailored to the EU's unique regulatory, funding, and collaborative mechanisms, such as the EU Green Deal, Horizon Europe, and InvestEU programs.

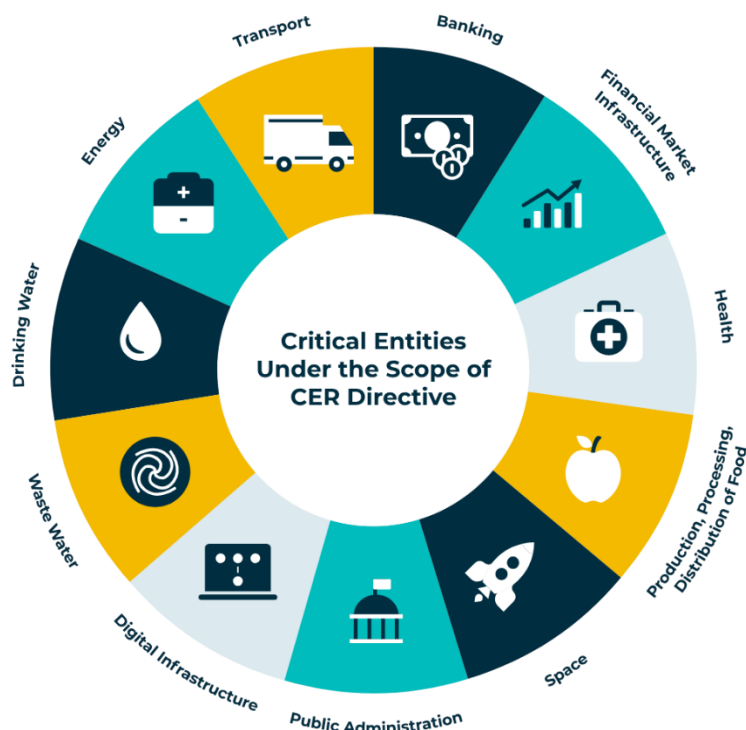


Figure 4.3. 10 critical infrastructure sectors in European Union. Source: EU CER Directive

4.5.1. Energy: Electricity Production, Networks, and Storage

Smart energy grids powered by AI-ready data centers enable real-time grid analysis, fault detection, and demand-response optimization. Predictive analytics improves storage efficiency (e.g., batteries, hydrogen systems) and integrates renewable energy sources with electricity networks, aligning with the EU's Green Deal objectives and Net Zero by 2050 targets. The preferred financing route is Green Bonds under the EU Green Deal Plan and as per the methodology presented section 2.3 of chapter 2 the feasibility score is 9.5/10. Green bonds support renewable energy projects, smart grid upgrades, and energy storage with a focus on decarbonization. These bonds align with the EU Taxonomy for sustainable

financing. The potential positive impacts could be Efficient energy distribution, reduced downtimes, and enhanced integration of renewable energies, contributing to the EU's sustainability and energy security goals.

4.5.2. Transport: Air, Rail, Water, and Road Infrastructure

AI-ready data centers enhance transport operations by monitoring infrastructure conditions, optimizing logistics in real-time, and automating traffic flow management. Predictive systems address maintenance needs for roads, railways, and bridges, while transport IoT integration reduces congestion and emissions in smart city systems.

The preferred financing route is Connecting Europe Facility (CEF) Funding and Public-Private Partnerships and as per the methodology presented section 2.3 of chapter 2 the feasibility score is 9/10. The CEF program supports AI-enabled smart transportation systems while public-private partnerships (P3s) unlock large-scale capital for transport-specific AI-driven projects. The potential positive impacts could be Increased infrastructure resilience, improved transport efficiency, and reduced carbon emissions from integrated AI-enabled systems.

4.5.3. Banking & Financial Markets

AI-ready data centers facilitate fraud detection, cyber threat monitoring, and compliance automation with EU financial regulations such as MiFID II and GDPR. Machine learning models predict financial risks and streamline trading operations, while blockchain technologies ensure transaction security. The preferred financing route is ESG-Aligned Investments and Horizon Europe R&D Funding and as per the methodology presented section 2.3 of chapter 2 the feasibility score is 8.5/10. ESG investments promote secure AI-driven financial systems, while Horizon Europe grants finance research into sustainable

fintech technologies and cyber resilience in banking systems. The potential positive impacts could be Improved financial cybersecurity, enhanced fraud prevention, and compliance with NIS2 cybersecurity standards.

4.5.4. Health: Healthcare Providers and Pharmaceutical R&D

AI-ready data centers support predictive diagnostics, secure storage of electronic health records (EHRs), and pharmaceutical research using AI-driven drug discovery platforms. Predictive models enhance resource allocation in hospitals, while federated learning ensures secure collaboration among healthcare providers. The preferred financing route is EU4Health Program and Health Impact Funds and as per the methodology presented section 2.3 of chapter 2 the feasibility score is 8.5/10. EU4Health, combined with private-sector partnerships, finances AI adoption in public healthcare facilities and pharmaceutical companies, enhancing healthcare system resilience. The potential positive impacts could be Improved patient outcomes, enhanced pharmaceutical innovation, and strengthened cybersecurity for sensitive healthcare data.

4.5.5. Drinking Water: Supply and Distribution

AI-ready infrastructures monitor water quality in real-time, predict demand-supply imbalances, and detect pipeline leaks before they escalate into major incidents. Machine learning algorithms optimize water purification and usage to minimize wastage and meet environmental sustainability goals. The preferred financing route is Green Infrastructure Bonds and Cohesion Policy Regional Funds and as per the methodology presented section 2.3 of chapter 2 the feasibility score is 9/10. EU cohesion funds, specifically aimed at reducing regional disparities, can subsidize AI-enabled water projects in underserved areas, while green bonds support water conservation technologies. The potential positive impacts

could be Enhanced water quality and availability, reduced environmental footprint, and improved operational efficiency in water utilities.

4.5.6. Wastewater: Collection, Treatment, and Disposal

AI-ready facilities automate wastewater treatment processes, enhance the identification of contaminants, and optimize collective sewerage networks. This complements compliance with EU Water Framework Directive regulations for sustainable treatment. The preferred financing route is European Investment Bank (EIB) Loans and EU Structural Funds and as per the methodology presented section 2.3 of chapter 2 the feasibility score is 8.5/10. Loans from the EIB, coupled with structural development funds, finance AI-based optimization of wastewater facilities, particularly in urban regions requiring advanced solutions. The potential positive impacts could be better compliance with water management regulations, improved sustainability in wastewater disposal, and increased resilience against infrastructure failures.

4.5.7. Digital Infrastructure

AI-ready data centers are at the core of digital infrastructure, supporting cloud platforms, data sovereignty, and protected domain name systems (DNS). These data centers serve as the backbone for secure internet exchange points and cloud computing networks, ensuring compliance with NIS2 cybersecurity directives. The preferred financing route is Digital Europe Program and Private Impact Investments and as per the methodology presented section 2.3 of chapter 2 the feasibility score is 9.5/10. The Digital Europe Program (2021–2027) offers funding for AI infrastructure deployment, especially in strategic areas like DNS and cloud platforms, while impact investments empower private stakeholders to fund cutting-edge digital projects. The potential positive impacts could be Greater cybersecurity

compliance, robust digital sovereignty, and reliable data infrastructure critical to EU economic stability.

4.5.8. Public Administration

AI-ready data centers equip government services with automated administration, enhancing service efficiency and data security in domains such as tax collection, public resource management, and smart governance platforms. Blockchains enhance voter record security and critical decision-making processes. The preferred financing route is EU Cohesion Funding and Horizon Europe Smart Governance Calls and as per the methodology presented section 2.3 of chapter 2 the feasibility score is 8/10. Funding streams targeting digital transformation in public administration prioritize secure AI tools and data infrastructure aligned with public transparency and accountability. The potential positive impacts could be improved citizen services, reduced inefficiencies, and compliance with security standards mandated under NIS2.

4.5.9. Space: Ground-Based Infrastructure

Ground-based systems supported by AI-ready data centers optimize satellite operations, provide real-time Earth observation analytics, and integrate space traffic collision-avoidance systems. AI algorithms enable quicker decision cycles for launching and monitoring space-based networks. The preferred financing route is EU Space Programme (Copernicus, Galileo) and Horizon Europe Space Missions and as per the methodology presented section 2.3 of chapter 2 the feasibility score is 9/10. Programs under the EU Space Agency provide structured funding for AI-based enhancements in both civilian and defense-oriented space missions. The potential positive impacts could be Strengthened

European space leadership, optimized satellite management, and enhanced national security applications facilitated by integrated AI solutions.

4.5.10. Food: Production, Processing, and Distribution

AI-ready data centers enable precise agricultural monitoring through IoT devices, supply chain optimization to reduce food waste, and predictive demand analyses to ensure efficient food distribution systems. Blockchain systems ensure traceability, improving food safety compliance. The preferred financing route is Common Agricultural Policy (CAP) and Private Sector Innovations and as per the methodology presented section 2.3 of chapter 2 the feasibility score is 8.5/10. CAP's sustainability-focused funds finance AI initiatives in sustainable farming, paired with agritech innovation grants from the private sector to fund traceable supply chains. The potential positive impacts could be Improved food security, reduced environmental degradation, and enhanced compliance with EU Green Deal standards for agricultural sustainability.

Table 4.3. Financial routes with feasibility score for AI ready data center in 10 critical infrastructure sectors in European Union

Sector	Proposed Financing Route	Feasibility Score	Rationale
Energy	Green Bonds under the EU Green Deal Plan	9.5/10	Strong alignment with EU Green Deal priorities and renewable funding taxonomies. Ample

			investor interest, bolstered by clear regulatory goals for decarbonization.
Transport	Connecting Europe Facility (CEF) & P3s	9/10	CEF ensures robust public funding for integrating AI-based transport systems. P3s complement scalability but introduce minor complexity in coordinating private and public stakeholders.
Banking & Financial	ESG-Aligned Investments & Horizon Europe R&D	8.5/10	ESG financing aligns directly with AI's intersection with banking modernization. Horizon Europe's focus on cyber resilience adds regulatory strength,

			but public skepticism over fintech risks a slight reduction in feasibility.
Health	EU4Health Program and Health Impact Funds	8.5/10	High sectoral alignment for AI in predictive diagnostics and resource optimization. Public healthcare bureaucracy and slower adoption rates in healthcare IT infrastructure reduce feasibility slightly.
Drinking Water	Green Infrastructure Bonds & Regional Cohesion Fund	9/10	Clear regulatory (CER Directive) alignment and sustainable infrastructure goals make green bonds feasible. The EU's

			emphasis on regional cohesion ensures scalability in underserved areas.
Wastewater	European Investment Bank (EIB) Loans	8.5/10	EIB loans suit large-scale wastewater optimization projects, but some challenges with execution risks (e.g., regional water management infrastructure disparities) slightly limit scalability.
Digital Infrastructure	Digital Europe Program & Private Impact Investments	9.5/10	Digital Europe provides dedicated funding and regulatory reinforcement under NIS2, while private impact investments fill additional capital gaps,

			ensuring high scalability.
Public Administration	Horizon Europe Smart Governance Calls	8/10	Horizon Europe funding supports AI in public administration, but execution risks (e.g., fragmented adoption across EU member states) slightly limit feasibility.
Space	EU Space Programmes & Horizon Europe	9/10	Strong regulatory alignment and significant EU and ESA investments bolster feasibility. Execution risks surrounding expensive infrastructure are mitigated by structured funding channels.

Food	Common Agricultural Policy (CAP) & Private Innovations	8.5/10	CAP's support for sustainable farming matches AI integration goals. However, dependency on private sector co- investment may reduce feasibility for smaller, traditional producers.
------	---	--------	--

CHAPTER V

CONCLUSIONS AND BUSINESS IMPLICATIONS

5.1 Conclusion

This thesis establishes that AI-ready data centers are essential components of modern critical infrastructure sectors, enabling large-scale automation, resilience, and real-time operational efficiencies for systems such as energy grids, transportation networks, water utilities, healthcare facilities, and telecommunications. However, these data centers pose substantial energy, environmental, and financing challenges due to their high computational workloads and associated infrastructure requirements. The findings reveal that integrating sustainable financing mechanisms specifically tailored to AI-ready infrastructure is critical for mitigating these challenges while concurrently ensuring improved resilience and operational continuity.

The data from industry case studies and academic analyses highlight the urgent need for regionally adaptive financing models combined with robust regulatory support. For example, current energy consumption trends in AI-ready data centers indicate that a single data center supporting AI applications can consume between 15 MW to 50 MW annually, equivalent to the energy use of tens of thousands of households. Energy-intensive cooling systems, which can account for up to 40% of operational energy costs in AI-driven systems, further exacerbate the environmental footprint of data centers serving critical infrastructure. These findings underscore the necessity of targeting advanced cooling technologies, such as liquid cooling or immersion cooling, through specialized financing solutions to ensure both environmental and economic sustainability.

Evidence from European and North American markets demonstrates the viability of green financing tools: green bonds and sustainability-linked loans have successfully funded multiple sustainable infrastructure projects, including renewable-powered data centers. For instance, in the energy grid sector, AI-integrated real-time grid analytics enabled by these data centers has reduced power distribution inefficiencies by nearly 20%, representing both resource conservation gains and cost reductions. Similarly, public-private partnerships (PPPs) in developing regions such as Sub-Saharan Africa have shown promise in scaling AI-enabled water management systems, with AI tools detecting leaks and optimizing water distribution to save 25%-30% of resources annually.

Findings also highlight that resilience remains a critical factor alongside sustainability. AI-ready data centers supporting critical services require investments in redundant systems, edge computing infrastructures, and cybersecurity safeguards to reduce operational vulnerabilities and enhance system readiness. Data shows an increasing reliance on distributed edge computing hubs in disaster-prone regions, reducing data latency by up to 80% and improving the reliability of predictive analytics in applications like real-time flood monitoring and urban evacuation planning. Moreover, the integration of AI in cybersecurity protocols has enabled anomaly detection improvements by up to 95%, safeguarding critical financial and energy systems from escalating cyber threats.

In response to these challenges and opportunities, aligning operational sustainability objectives with financing mechanisms is critical. By linking financial models such as Energy-as-a-Service (EaaS), carbon pricing, and green financing with performance-based outcomes, data center operators can better address capital barriers while meeting their energy, efficiency, and resilience goals. For example, adopting EaaS models has shown a 30%-50% reduction in upfront infrastructure costs for mid-sized data centers while enabling scalable adoption of energy optimization technologies.

Additionally, carbon pricing or emissions trading frameworks such as the European Union's Emissions Trading System (EU ETS) offer incentives for AI-ready data centers to implement energy-efficient solutions, enabling progress toward carbon neutrality within critical sectors. Overall, the findings indicate that sustainable financing strategies are not only indispensable for modernizing AI-ready data centers but also for ensuring their continuity and resilience in supporting critical infrastructure systems. Without such strategic investments, sectors dependent on these facilities will face difficulties in scaling digital transformations necessary for addressing climate change, operational disruptions, and escalating demands in public services.

5.2 Business Implications

Integrating the findings of this thesis into business strategy entails several critical considerations for organizations, stakeholders, and governments operating within or adjacent to critical infrastructure sectors:

- Businesses operating energy-intensive AI data centers have an opportunity to reduce costs while achieving sustainability goals by leveraging green bonds and sustainability-linked financing. In high-stakes sectors such as energy and healthcare, these funding models can directly address environmental mandates while improving operational efficiency.
- Data showing the disproportionate vulnerability of certain regions to climate change and natural disasters highlights opportunities for businesses to design and deploy tailored resilience-focused AI technologies. Public-private partnerships (PPPs) can prove effective in scaling these investments, particularly in bridging infrastructure gaps in emerging markets.

- Businesses with technology offerings in advanced cooling systems or edge computing technologies should prioritize collaboration with operators of AI-ready critical infrastructure. Cooling-as-a-Service and modular edge data hubs represent areas with high growth potential for vendors looking to address the financial and operational demands highlighted in this research.
- With data highlighting AI's effectiveness in improving cybersecurity protocols, businesses must reframe AI-ready data center investments not solely as efficiency measures but as necessities for safeguarding critical infrastructure. Such an approach is particularly vital for finance and defense sectors prone to targeted cyber-attacks.
- Financial institutions can capitalize on high demand for innovative project financing within this intersection of resilience and sustainability. Scaling financing frameworks tied to AI-specific performance outcomes, such as reduced latency or carbon-neutral operations, offers a significant opportunity for differentiation and profit generation.
- Businesses must actively engage in cross-sector partnerships and policy discussions to influence standardized metrics and incentivize financing mechanisms aligned with their operational priorities. These actions can ensure equitable sharing of risks while maximizing the strategic alignment of modernization efforts with global environmental and resilience goals.

5.3 Limitations and Future Research

While the findings of this thesis provide valuable insights into sustainable financing strategies for AI-ready data centers in critical infrastructure sectors, there are certain limitations that may influence the generalizability and completeness of the conclusions:

5.3.1 Reliance on Secondary Data

A significant limitation of this study is its dependence on secondary data sources, including case studies, industry reports, peer-reviewed articles, policy documents, and publicly available data. While extensive efforts were made to source accurate and reliable data, secondary data inherently carries the risk of bias, outdated information, or incomplete context. The lack of primary data collection, such as interviews with industry leaders, hands-on case studies (except the ones mentioned in this thesis), or surveys of financing stakeholders, limits the study's ability to reflect real-time market conditions and perspectives unique to operators and financiers of AI-ready data centers.

5.3.2 Geographical Variability

The study draws heavily from data and policy examples originating in mature regions, such as North America, Europe, and parts of Asia-Pacific, where the financing ecosystem for sustainability and critical infrastructure modernization is more developed. Consequently, the findings may be less representative of emerging markets or regions with less structured regulatory and financial systems. For example, challenges faced in Sub-Saharan Africa or rural parts of South Asia may require unique financing approaches not fully explored in this research.

5.3.3. Dynamic Nature of AI and Energy Technologies

AI-driven data centers and their supporting technologies, such as liquid cooling systems, edge computing, and renewable integrations, are rapidly evolving. These technologies introduce uncertainties in terms of their long-term costs, energy consumption patterns, and adoption rates. Relying on existing technological and environmental benchmarks may limit the study's relevance to future scenarios, especially as innovations accelerate.

5.3.4. Limited Empirical Validation of Financing Models

While the thesis highlights the potential of financing mechanisms such as green bonds, Energy-as-a-Service (EaaS), and public-private partnerships (PPPs), these models rely on past successful examples or theoretical frameworks. The lack of large-scale empirical testing or real-world validation tailored to AI-ready data centers in critical infrastructure sectors introduces uncertainties regarding their scalability, feasibility, and adaptability to various market conditions.

5.3.5. Sectoral and Contextual Specificity

Critical infrastructure sectors such as healthcare, energy, transportation, and telecommunications have diverse operational demands and financing challenges. Although the research attempts to provide sector-specific insights, the complexity and interdependence of these sectors mean that certain nuances may not have been fully captured. For example, the unique regulatory and operational requirements of healthcare data centers differ significantly from those of energy grid management systems, suggesting that a one-size-fits-all financing strategy may oversimplify sectoral needs.

5.3.6. Absence of Real-Time Resilience Data

The study emphasizes resilience as a cornerstone of AI-ready data center design for critical infrastructure but largely infers resilience metrics from existing literature and use cases. The absence of real-time resilience performance data, such as disaster recovery efficiency or cybersecurity breach simulations, limits the depth of analysis on how well financing strategies directly support resilience-building objectives in practice.

5.3.7. Regulatory Differences Across Regions

The research is partially constrained by the complexity of harmonizing regulatory frameworks across various regions. Differences in emissions policies, sustainability mandates, and energy market dynamics often influence financing models in region-specific ways. The study's reliance on generalized regulatory trends may overlook localized constraints or requirements critical to effective implementation in certain contexts.

5.3.8. Limited Integration of Social Equity Considerations

While environmental sustainability and operational resilience were the central focuses of the study, the research does not extensively investigate social equity concerns tied to AI-driven data centers and their financing. For example, issues such as the accessibility of critical infrastructure resources in underserved communities or the ethical implications of AI deployment are underexplored, leaving space for further interdisciplinary investigation.

Future research addressing these limitations could include the collection of primary data through stakeholder interviews or surveys to better capture real-time market perspectives and localized challenges. Additionally, conducting longitudinal studies or empirical tests of financing models in diverse regions and sectors would validate their scalability and adaptability. Incorporating real-time data on resilience outcomes during disasters or cybersecurity events, as well as deeper exploration of emerging markets and their regulatory frameworks, would significantly enhance the robustness and global applicability of the study's findings. Expanding the analysis to integrate social equity considerations would also ensure a more comprehensive understanding of the societal impact of AI-ready data centers and their financing mechanisms.

REFERENCES

Abbasi, T. Holz, E. Zambon, S. Etalle, “ECFI: Asynchronous control flow integrity for programmable logic controllers”, Proceedings of the 33rd Annual Computer Security Applications Conference, 2017, pp. 437–448.

Achiam, S. Adler, S. Agarwal, L. Ahmad, I. Akkaya, F. L. Aleman, D. Almeida, J. Altenschmidt, S. Altman, S. Anadkat et al., “GPT-4 technical report,” arXiv preprint arXiv:2303.08774, 2023.

Aljbour, J., Wilson, T., Patel, P. “Powering intelligence: Analyzing artificial intelligence and data center energy consumption,” EPRI White Paper no. 3002028905, 2024.

Allianz, “Cyber attacks on critical infrastructure,” 2016. Available at: <https://commercial.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html>

Altaieb, H. & Rajnai, Z., “Malware Attacks on SCADA Systems: Assessing Risks and Strengthening Cybersecurity Measures,” IEEE, pp. 625-630, 2023.

Amazon Web Services, “What is Amazon simple storage service (Amazon S3)?” 2024, Available: <https://docs.aws.amazon.com/AmazonS3/latest/dev/Welcome.html>

Ampratwum, V.W. Tam, R. Osei-Kyei, “Critical analysis of risks factors in using public-private partnership in building critical infrastructure resilience: a systematic review”, Constr. Innov. 23 (2) (2023) 360–382.

Apruzzese, G., Laskov, P., Montes de Oca, E., Mallouli, W., Brdalo R.L., Grammatopoulos, A.V., Di Franco, F. “The role of machine learning in cybersecurity”, Dig. Threats Res. Pract. 4 (1) (2023) 1–38.

APT Power Technology, “How AI compute loads are transforming datacenter infrastructure,” June 2025. Available at: <https://apt4power.com/how-ai-compute-loads-are-transforming-datacenter-infrastructure>

Avelar, P. Donovan, P. Lin, W. Torell, and M. A. T. Arango, “The AI disruption: Challenges and guidance for data center design,” *Artificial Intelligence in Medicine*, vol. 138, 2023.

Azarifar, Arik, M., Chang, J.-Y. “Liquid cooling of data centers: A necessity facing challenges,” *Applied Thermal Engineering*, vol. 247, p. 123112, Jun. 2024.

Baezner, M. Robin, P., “Stuxnet,” Technical Report, ETH Zurich, 2017.

Bederna, Z., Rajnai, Z. & Szadeczky, T., “Attacks against energy, water and other critical infrastructure in the EU,” 2020 IEEE 3rd International Conference and Workshop in Óbuda on Electrical and Power Engineering (CANDO-EPE), pp. 125-130, 2020.

Beerman, J., Berent, D., Falter, Z. & Bhunia, S., “A Review of Colonial Pipeline Ransomware Attack,” 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW), pp. 8-15, 2023.

Bhamare, Zolanvari, M., Erbad, A., Jain, R., Khan, K., Meskin, N. “Cybersecurity for industrial control systems: A survey,” *Comput. Secur.* 89 (2020) 101677.

Bloomberg News. AI needs so much power, it’s making yours worse. December 2024. Available at: <https://www.bloomberg.com/graphics/2024-ai-power-home-appliances/?embedded-checkout=true>

Bout, Loscri, V., Gallais, A. “How machine learning changes the nature of cyberattacks on IoT networks: A survey,” *IEEE Commun. Surv. Tutor.* 24 (1) (2021) 248–279.

Budžys, A., Kurasova, O. & Medvedev, V., “Behavioral Biometrics Authentication in Critical Infrastructure Using Siamese Neural Networks,” *HCI for Cybersecurity, Privacy and Trust*, Springer Nature Switzerland, pp. 309–322, 2023.

Carrier, T., Victor, P., Tekeoglu, A. & Lashkari, A. H., “Detecting Obfuscated Malware using Memory Feature Engineering,” *2023 IEEE Colombian Conference on Applications of Computational Intelligence (ColCACI)*, pp. 177–188, 2022.

Catak, F. O. & Yazı, A. F., “A Benchmark API Call Dataset for Windows PE Malware Classification,” *arXiv*, 2021.

Ćelić, J., Bronzin, T., Horvat, M., Jović, A., Stipić, A., Prole, B., Maričević, M., Pavlović, I., Pap, K., Mikota, M. & Jelača, N., “Generative AI in E-maintenance: Myth or Reality?” *2024 47th MIPRO ICT and Electronics Convention (MIPRO)*, 2024.

Chalise, A. Golshani, S. R. Awasthi, S. Ma, B. R. Shrestha, L. Bajracharya, W. Sun, and R. Tonkoski, “Data center energy systems: Current technology and future direction,” in *IEEE Power & Energy Society General Meeting*. IEEE, 2015, pp. 1–5.

Charles, V., Emrouznejad, A. & Gherman, T. “A critical analysis of the integration of blockchain and artificial intelligence for supply chain,” *Annals of Operations Research*, Vol. 327, pp. 7–47, 2023.

Chen, X., Ding, M., Wang, X., Xin, Y., Mo, S., Wang, Y., Han, S., Luo, P., Zeng, G. & Wang, J., “Context autoencoder for self-supervised representation learning,” *International Journal of Computer Vision*, Vol. 132, pp. 208–223, 2024.

Chen, Y.H. Peng, Y., Wang, I. “Thermodynamic analysis of hybrid cooling system integrated with waste heat reusing and peak load shifting for data center,” *Energy Conversion and Management*, vol. 183, pp. 427–439, 2019.

Choquette, J., Gandhi, W., Giroux, O., Stam, N., Krashinsky, R. “NVIDIA A100 tensor core GPU: Performance and innovation,” IEEE Micro, vol. 41, no. 2, pp. 29–35, 2021.

Choukse, E., Warriar, B., Heath, S., Belmont, L., Zhao, A., Khan, H.K., Harry, B., Kappel, M., Hewett, R.J., Datta, K., et al., “Power stabilization for AI training datacenters,” arXiv preprint arXiv:2508.14318, 2025.

Chowdhury, Gkioulos, V. “Cyber security training for critical infrastructure protection: A literature review,” Comp. Sci. Rev. 40 (2021) 100361.

Ciancamerla, E., Minichino, M., Palmieri, S. “Modeling cyber attacks on a critical infrastructure scenario,” IISA 2013, IEEE, 2013, pp. 1–6.

Cohen, “AI is pushing the world toward an energy crisis,” Forbes, May 2024. Available at: <https://www.forbes.com/sites/arielcohen/2024/05/23/ai-is-pushing-the-world-towards-an-energy-crisis>

Crusoe, “Crusoe and tallgrass announce AI data center in wyoming,” July 2025. Available at: <https://www.crusoe.ai/resources/newsroom/crusoe-and-tallgrass-announce-ai-data-center-in-wyoming>

Das, S. Munikoti, B. Natarajan, B. Srinivasan, “Measuring smart grid resilience: Methods, challenges and opportunities,” Renew. Sustain. Energy Rev. 130 (2020) 109918.

Das, T.K., Adepu, S., Zhou, J. “Anomaly detection in industrial control systems using logical analysis of data,” Comput. Secur. 96 (2020) 101935.

Davenport, B. Singer, N. Mehta, B. Lee, J. Mackay, A. Modak, B. Corbett, J. Miller, T. Hari, J. Ritchie et al., “Generational growth: AI, data centers and the coming US power demand surge,” Goldman Sachs, vol. 28, April 2024.

Di Pietro, R., Raponi, S., Caprolu, M. & Cresci, S., “Critical Infrastructure, New Dimensions of Information Warfare,” Springer International Publishing, pp. 157–196, 2021.

Do, J., Ferreira, V. C., Bobarshad, H., Torabzadehkashi, M., Rezaei, S., Heydarigorji, A., Souza, D., Goldstein, B. F., Santiago, L., Kim, M.S. et al., “Cost-effective, energy-efficient, and scalable storage computing for large-scale AI applications,” *ACM Transactions on Storage (TOS)*, vol. 16, no. 4, pp. 1–37, 2020.

Duman, O., Ghafouri, M., Kassouf, M., Atallah, R., Wang, L. Debbabi, M., “Modeling Supply Chain Attacks in IEC 61850 Substations,” 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), pp. 1-6, 2019.

Eggers, S., “A novel approach for analyzing the nuclear supply chain cyber-attack surface,” *Nuclear Engineering and Technology*, Vol. 53, pp. 879-887, 2021.

El Hussein, F., Noura, H., Salman, O. & Chehab, A., “Advanced Machine Learning Approaches for Zero-Day Attack Detection: A Review,” 2024 8th Cyber Security in Networking Conference (CSNet), pp. 297-304, 2024.

Esmaili, B., Azmoodeh, A., Dehghantanha, A., Srivastava, G., Karimipour, H. Chun-Wei Lin, J., “A GNN-Based Adversarial Internet of Things Malware Detection Framework for Critical Infrastructure: Studying Gafgyt, Mirai, and Tsunami Campaigns,” *IEEE Internet of Things Journal*, Vol. 11, pp. 26826-26836, 2024.

Fovino, I.N., Carcano, A., Masera, M., Trombetta, A. “An experimental investigation of malware attacks on SCADA systems,” *Int. J. Crit. Infrastruct. Prot.* 2 (4) (2009) 139–145.

Gaidarski, I. & Minchev, Z., “Insider Threats to IT Security of Critical Infrastructures,” in: T. Krassimir, K. Vyacheslav, K. J. T. Todor & Atanassov, eds.,

Digital Transformation, Cyber Security and Resilience of Modern Societies, Springer International Publishing, pp. 381-394, 2021.

George, A. Dilger, M. J. Brim, R. Mohr, A. Shehata, J. Y. Choi, A. M. Karimi, J. Hanley, J. Simmons, D. Manno et al., “Lustre unveiled: Evolution, design, advancements, and current trends,” ACM Transactions on Storage, vol. 21, no. 3, pp. 1–109, 2025.

Gooding, M. “Microsoft and caterpillar power data center for 48 hours using hydrogen fuel cells,” January 2024. Available at: <https://www.datacenterdynamics.com/en/news/microsoft-caterpillar-hydrogen-fuel-cell-data-center/>

Google, “Google data center pue performance,” Available at: <https://datacenters.google/efficiency/>

Google’s Green Data Centers: Network POP Case Study. Available at: <https://sustainability.google/reports/dc-best-practices-google/>

Haghshenas, B. Setz, Y. Bloesch, and M. Aiello, “Enough hot air: The role of immersion cooling,” Energy Informatics, vol. 6, no. 1, p. 14, Aug. 2023.

Heydari, A. R. Gharaibeh, M. Tradat, Y. Manaserh, V. Radmard, B. Eslami, J. Rodriguez, B. Sammakia et al., “Experimental evaluation of direct-to-chip cold plate liquid cooling for high-heat-density data centers,” Applied Thermal Engineering, vol. 239, p. 122122, 2024.

Hossain, S., Senouci, S.-M., Brik, B. & Boualouache, A., “A privacy-preserving Self-Supervised Learning-based intrusion detection system for 5G-V2X networks,” Ad Hoc Networks, Vol. 166, pp. 103674, 2025.

Husnoo, M.A., Anwar, A., Chakraborty, R.K., Doss, R., Ryan, M.J. “Differential privacy for IoT-enabled critical infrastructure: A comprehensive survey,” IEEE Access 9 (2021) 153276–153304.

Hussain, Q. Du, B. Sun, Z. Han, “Deep learning-based DDoS-attack detection for cyber-physical system over 5G network,” IEEE Trans. Ind. Inform. 17 (2) (2020) 860–870.

InfiniBand Trade Association, “InfiniBand – high-performance interconnect technology,” 2025. Available at: <https://www.infinibandta.org/>

International Energy Agency, “Energy and AI,” International Energy Agency, Tech. Rep., September 2024. Available at: <https://www.iea.org/reports/energy-and-ai>

Jegham, N., Abdelatti, M., Elmoubarki, L., Hendawi, A. “How hungry is AI? benchmarking energy, water, and carbon footprint of LLM inference,” arXiv preprint arXiv:2505.09598, 2025.

Jouppi, N., Kurian, G., Li, S., Ma, P., Nagarajan, P., Nai, L., Patil, N., Subramanian, S., Swing, A., Towles, B. et al., “TPU v4: An optically reconfigurable supercomputer for machine learning with hardware support for embeddings,” in Proceedings of the 50th annual international symposium on computer architecture, 2023, pp. 1–14.

Kaloudi, N., Li, J. “The AI-based cyber threat landscape: A survey,” ACM Comput. Surv. 53 (1) (2020) 1–34.

Kambhampati, A., van den, D., Schild, J., “Moving beyond diesel generators: Exploring renewable backup alternatives for data centers,” in Journal of Physics: Conference Series, vol. 2929, no. 1. IOP Publishing, 2024, p. 012008.

Kayan, H., Nunes, M., Rana, O., Burnap, P., Perera, C., “Cybersecurity of industrial cyber-physical systems: a review,” ACM Comput. Surv. 54 (11s) (2022) 1–35.

Koay, A.M., Ko, R.K.L., Hettema, H., Radke, K. “Machine learning in industrial control system (ICS) security: current landscape, opportunities and challenges,” *J. Intell. Inf. Syst.* 60 (2) (2023) 377–405.

Kuncoro, W., Pambudi, N., Biddinika, M.K., Widiastuti, I., Hijriawan, M., Wibowo, H. “Immersion cooling as the next technology for data center cooling: A review,” in *Journal of Physics: Conference Series*, vol. 1402, no. 4. IOP Publishing, 2019, p. 044057.

Lehto, M. “Cyber-attacks against critical infrastructure,” in: *Cyber Security: Critical Infrastructure Protection*, Springer, 2022, pp. 3–42.

Li and J. Li, “AI load dynamics – a power electronics perspective,” arXiv preprint arXiv:2502.01647, 2025, Available at: <https://arxiv.org/html/2502.01647v2>

Li, Mughees, M., Chen, Y., Li, Y.R. “The unseen AI disruptions for power grids: LLM-induced transients,” arXiv, Sep. 2024.

Li, Y., Liu, Q. “A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments,” *Energy Rep.* 7 (2021) 8176–8186.

Lin, L., Wijayawardana, R., Rao, V., Nguyen, H., Gnibga, E.W., Chien, A.A. “Exploding AI power use: an opportunity to rethink grid planning and management,” in *Proceedings of the 15th ACM International Conference on Future and Sustainable Energy Systems*, 2024, pp. 434–441.

Liu, C. Qian, W.G. Hatcher, H. Xu, W. Liao, W. Yu, “Secure Internet of Things (IoT)-based smart-world critical infrastructures: Survey, case study and research opportunities,” *IEEE Access* 7 (2019) 79523–79544.

Liu, V. Hagenmeyer, H.B. Keller, “A review of rule learning-based intrusion detection systems and their prospects in smart grids,” *IEEE Access* 9 (2021) 57542–57564.

Maglaras, L., Ferrag, M., Derhab, A., Mukherjee, M., Janicke, H., Rallis, S. “Threats, countermeasures and attribution of cyber attacks on critical infrastructures,” EAI Endorsed Trans. Secur. Saf. 5 (16) (2018)

Makrakis, G.M., Kolias, C., Kambourakis, G., Rieger, C., Benjamin, J. “Industrial and critical infrastructure security: Technical analysis of real-life security incidents,” IEEE Access 9 (2021) 165295–165325.

McKinsey & Company, “How data centers and the energy sector can sate AI’s hunger for power,” Available at: <https://www.mckinsey.com/industries/private-capital/our-insights/how-data-centers-and-the-energy-sector-can-sate-ais-hunger-for-power>

Mughees, M., Li, Y., Chen, Y., Li, Y. R. “Short-term load forecasting for AI-data centers,” arXiv preprint arXiv:2503.07756, 2025.

Muhammad, A. Kalwar, and K. Mekhilef, “Review: uninterruptible power supply (UPS) system,” Renewable and Sustainable Energy Reviews, vol. 58, pp. 1395–1410, 2016.

Nazir, S. Patel, D. Patel, “Assessing and augmenting SCADA cyber security: A survey of techniques,” Comput. Secur. 70 (2017) 436–454.

Ni, J., Bai, X. “A review of air conditioning energy performance in data centers,” Renewable and sustainable energy reviews, vol. 67, pp. 625–640, 2017.

Nlyte Software, “Data center rack power costs: A condensed analysis,” 2024 Available at: <https://www.nlyte.com/blog/data-center-rack-power-costs-a-condensed-analysis/>

NVIDIA Corporation, “NVIDIA NVLink high-speed GPU interconnect,” 2025. Available at: <https://www.nvidia.com/en-us/products/workstations/nvlink-bridges/>

Patel, D., Chu, W., Tseng, C., Xie, M., Ontiveros, J.E., Nishball, D. “GB200 hardware architecture-component supply chain & bom,” 2024. Available at: <https://semianalysis.com/2024/07/17/gb200-hardware-architecture-and-component/#>

Patel, D., Ontiveros, J.E., Nishball, D. “Datacenter anatomy part 1: Electrical systems,” 2024, Available at: <https://semianalysis.com/2024/10/14/datacenter-anatomy-part-1-electrical/>

Patterson, D., Gonzalez, J., Le, Q., Liang, C., Munguia, L.M., Rothchild, D., So, D., Texier, M., Dean, J. “Carbon emissions and large neural network training,” arXiv preprint arXiv:2104.10350, 2021.

Pilz, K., Mahmood, Y., Heim, L. “AI’s power requirements under exponential growth: Extrapolating AI data center power demand and assessing its potential impact on U.S. competitiveness,” RAND Corporation, January 2025. Available at: https://www.rand.org/pubs/research_reports/RRA3572-1.html

Potamos, G., Theodoulou, S., Stavrou, E., Stavrou, S. Building maritime cybersecurity capacity against ransomware attacks, in: Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media: Cyber Science 2022, 20–21 June Wales, Springer, 2023, pp. 87–101.

Resul, D., Gündüz, M.Z. Analysis of cyber-attacks in IoT-based critical infrastructures, *Int. J. Inform. Secur. Sci.* 8 (4) (2020) 122–133.

Sakhnini J., Karimipour H., Dehghantanha A., Parizi R.M. AI and security of critical infrastructure *Handb. Big Data Priv.* (2020), pp. 7-36

Semba, K., “Artificial intelligence, real consequences: Confronting AI’s growing energy appetite,” August 2024. Available at: <https://www.extremenetworks.com/resources/blogs/confronting-ai-growing-energy-appetite-part-1?>

Sousa, M. Arieiro, V. Pereira, J. Correia, N. Lourenço, T. Cruz, Elegant: “Security of critical infrastructures with digital twins,” IEEE Access 9 (2021) 107574–107588.

Spenneberg, M., Brüggemann, H., Schwartke, H. “Plc-blasters: A worm living solely in the plc,” Black Hat Asia 16 (2016) 1–16.

Stellios, P., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., Lopez, J. “A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services,” IEEE Commun. Surv. Tutor. 20 (4) (2018) 3453–3495.

Sun, J., Wang, S., Wang, J., Tolbert, L.M. “Dynamic model and converter-based emulator of a data center power distribution system,” IEEE Transactions on Power Electronics, vol. 37, no. 7, pp. 8420–8432, 2022.

Sunarti S., Fadzlul Rahman F., Naufal M., Risky M., Febriyanto K., Masnina R. “Artificial intelligence in healthcare: opportunities and risk for future Gaceta Sanit.,” 35 (2021), pp. S67-S70

Teague, S. S. Refaat, M. Farrag, and A. Karki, “A comparative study of UPS batteries for data center applications,” in 2025 IEEE 19th International Conference on Compatibility, Power Electronics and Power Engineering (CPE-POWERENG). IEEE, 2025, pp. 1–6.

Team, G., Anil, R., Borgeaud, S., Alayrac, J.B., Yu, J., Soricut, R., Schalkwyk, J., Dai, A. M., Hauth, A., Millican, K. et al., “Gemini: a family of highly capable multimodal models,” arXiv preprint arXiv:2312.11805, 2023.

Ten, C.W., Manimaran, G., Liu, C.C. “Cybersecurity for critical infrastructures: Attack and defense modeling,” IEEE Trans. Syst. Man Cybern. A 40 (4) (2010) 853–865.

Touvron, H., Lavril, T., Izacard, G., Martinet, X., Lachaux, M.A., Lacroix, T., Rozière, B., Goyal, N., Hambro, E., Azhar F., et al., “LLaMA: Open and efficient foundation language models,” arXiv preprint arXiv:2302.13971, 2023.

Wells, E.M., Boden, M., Tseytlin, I., Linkov, I., “Modeling critical infrastructure resilience under compounding threats: a systematic literature review,” *Prog. Disaster Sci.* (2022) 100244.

Wilke, J. J., Kenny, J.P. “Opportunities and limitations of quality-of-service in message passing applications on adaptively routed dragonfly and fat tree networks,” in 2020 IEEE International Conference on Cluster Computing (CLUSTER). IEEE, 2020, pp. 109–118.

Yadav, G., Paul, K. “Architecture and security of SCADA systems: A review,” *Int. J. Crit. Infrastruct. Prot.* 34 (2021) 100433.

Yang, Y., Tatano, H., Huang, Q., Liu, H., Yoshizawa, G., Wang, K. “Evaluating the societal impact of disaster-driven infrastructure disruptions: A water analysis perspective,” *Int. J. Disaster Risk Reduct.* 52 (2021) 101988.

Zhang, Z. Meng, X. Hong, Y. Zhan, J. Liu, J. Dong, T. Bai, J. Niu, and M. J. Deen, “A survey on data center cooling systems: Technology, power consumption modeling and control strategy optimization,” *Journal of Systems Architecture*, vol. 119, p. 102253, 2021.

Zhao, W. X., Zhou, K., Li, J., Tang, T., Wang, X., Hou, Y., Min, Y., Zhang, B., Zhang, J., Dong, Z. et al., “A survey of large language models,” arXiv preprint arXiv:2303.18223, vol. 1, no. 2, 2023.

Zhou, C. Shen, G. Ma, X. Yan, “Power usage effectiveness analysis of a liquid-pump-driven hybrid cooling system for data centers in subclimate zones,” *Sustainable Energy Technologies and Assessments*, vol. 52, p. 102277, Aug. 2022.

APPENDIX A: Criteria Definitions and Selection Process

Sectoral Alignment: Assesses how well the financing mechanism aligns with the sector's operational, regulatory, and technological characteristics. Higher scores were given if the mechanism strongly supported the sector's needs, such as scalability, cybersecurity, and AI integration.

Scalability and Funds Availability: Measures whether the financing mechanism can support large-scale deployments across the sector and accommodate future expansion. Accessibility of funds to stakeholders (e.g., private companies or public institutions) was also considered.

Government and Regulatory Backing: Evaluates the level of regulatory and policy support available for the financing mechanism. Mechanisms reinforced by existing policies, grants, or federal programs scored higher.

Investor and Public Sentiment: Considers the attractiveness of the financing mechanism to investors and its alignment with societal or market perceptions (e.g., sustainability, ESG initiatives). Mechanisms associated with public demand for environmental and infrastructure investments received higher scores.

Execution and Risk Tolerance: Examines the ease of implementation, legal complexity, potential risks, and the mechanism's overall practicality in achieving sector objectives. Financing mechanisms with lower execution risks and higher adoption rates scored favorably.