PENINSULA PUBLISHING LLC

SHIFRA

Vol. **(2024)**, 2024, **pp**. 88–96
ISSN: 3078-3186

Research Article

The Role of the Iraqi National Data Center in Advancing Digital Transformation and Data Sovereignty

Israa Ibraheem Al Barazanchi [1,2,*], Dima Haider Rasheed [3]

[1]*College of Computing and Informatics, Universiti Tenaga Nasional (UNITEN), 43000 Kajang, Selangor, Malaysia.*
[2]*College of Engineering, University of Warith Al-Anbiyaa, Karbala, Iraq*
[3]*Department of Cyber Engineering Technologies, Ashur University, Baghdad 10001, Iraq*

ARTICLE INFO

Article History
Received 10 Mar 2024
Revised: 1 May 2024
Accepted 1 Jun 2024
Published 18 Jun 2024

Keywords
Iraqi National Data Center (INDC), digital transformation, data sovereignty, cybersecurity, data centralization,

ABSTRACT

This study examines the key role of the National Data Center in Iraq's digital transformation, focusing on the Iraqi National Data Center (INDC) as a key infrastructure for centralized data management and the digital role You trust to play. Iraq's current digital infrastructure is severely limited, including outdated technologies, cybersecurity weaknesses, regulatory gaps and economic constraints. These obstacles prevent INDC from meeting the increasing demands for data storage, resources and security required for effective government functioning and self-reliance in the digital age f Deliver systems centralized for By implementing this approach, INDC will be able to enhance its data governance and security processes, align with international data authority standards, and forge partnerships that support long-term growth. The findings of this study suggest that targeted reforms in infrastructure, cybersecurity, and regulatory frameworks can significantly increase the efficiency of the INDC government, protect national intelligence from external threats, and help Iraq broader digital transformation objectives And of getting continued investment , emphasizes the importance of skilled labor development and system exchange.

1. INTRODUCTION

Data centers form the backbone of today's digital world, providing a centralized infrastructure where data can be stored, processed and accessed securely. In the digital age where more information is generated per second, data centers play a vital role in supporting everything from government operations and corporate operations to personal data storage They are designed to ensure data availability, security and availability time required, making it necessary for daily activities in modern life. Advanced data centers host cloud computing services, facilitate big data analytics, and support artificial intelligence (AI) applications, all of which contribute to faster innovation and economic growth[1]. These centers also enhance data security, which is important in an era marked by cybersecurity threats, privacy concerns and the need for data sovereignty Essentially, data centers for countries and organization various capabilities to manage the complexity of digital data and support digital transformation in the public and private sectors in Iraq The development of digital infrastructure has seen significant challenges and developments, largely influenced by political, economic and social factors. Despite Iraq's historical challenges such as political instability and economic constraints, the push to digitize has continued in recent years Iraqi government and private organizations have been trying to modernize IT infrastructure it exists today. But the absence of a unified, nationally focused data center meant that data storage, management and security were fragmented and vulnerable to outside influence This posed a threat to Iraqi data sovereignty, because reliance on foreign-owned or outsourced data centers increased the risk of data breaches To prevent, Iraq has established the Iraqi National Data Center (INDC), aimed at to unify the country's digital infrastructure for business. The primary objective of the INDC is to provide a safe, efficient and controlled environment for the collection, processing and processing of internally developed data[2]. This centralized strategy is aimed at enabling Iraq to move forward with the digital transformation process, increase the efficiency of the public sector, and protect the country's data from external threats The establishment of the INDC is a step

*Corresponding author email: israa.albarazanchi2023@gmail.com
DOI: https://doi.org/10.70470/SHIFRA/2024/010

primarily to secure Iraq's digital future and enhance its ability to support innovation, government transparency and economic growth.

1.1 Purpose of the Study:

Focus on the Iraqi National Data Center and its role in digital transformation and data empowerment

The main focus of this study is to examine the role of the Iraqi National Data Center (INDC) in promoting Iraq's digital transformation and protecting its data sovereignty. As Iraq goes digital, INDC is a cornerstone of the country's data management and security. Understanding the importance provides insight into how Iraq can use digital infrastructure to improve governance, improve public services, and protect its data from foreign interference.This paper seeks to analyze how INDC contributes to this goal by analyzing its infrastructure, technological capabilities and policy roles within the broader Iraqi digital landscape. In addition, the paper will examine the role of INDC in fostering digital transformation at the local level and its ability to ensure data sovereignty in an increasingly interconnected global environment[3].

1.2 Research Objectives:

Key questions and objectives guide the study
The objectives of this study were to achieve a number of objectives that reflected a deeper understanding of the use and impact of the INDC. Key questions include:
1. What is the current state of INDC's infrastructure and how does it support Iraq's digital transformation?
2. In what ways does INDC contribute to data governance, and what challenges does it face in protecting national data?
3. How has INDC influenced public sector efficiency and service delivery in Iraq?
4. What are the growth possibilities and future directions for INDC in terms of technical development and policy support?

By addressing these questions, this study aims to provide a comprehensive assessment of the INDC, focusing on its contributions, challenges and potential for supporting Iraq's goals for a future of digital security and self-sufficiency on. The findings of this study will contribute to understanding the critical role of the INDC in shaping Iraq's digital landscape and offer recommendations to further strengthen its potential to further advance Iraq's digital data sovereignty[4].

2. RELATED WORK

2.1 Digital Transformation: Definition and Relevance to National Development

Digital transformation refers to the integration of digital technologies into all aspects of society, fundamentally transforming how governments, businesses and individuals work and communicate with each other These processes often require state-of-the-art infrastructure, digital tools and platforms diversity will be implemented, data-driven decisions to increase efficiency, accessibility and transparency. manufacturing and transferring to is global Digital transformation is important for countries aiming to keep pace with growth because it supports economic growth, innovation and effective public services Through digitization, governments can create jobs simplify, reduce bureaucracy and improve public engagement by creating more efficient and responsive services[5]. Digital transformation is particularly important for Iraq because it offers the opportunity to overcome long-standing governance inefficiencies, infrastructure restrictions and improve service delivery f, Digital transformation provides the basis for modern security practices, such as provided data protection has developed its cybersecurity infrastructure, which is needed to protect national interests in an increasingly digital world.

2.2 Data Sovereignty: Importance for Iraq and Its Impact on National Security and Self-Governance

Data sovereignty is the concept that data is subject to the legal and governance framework of the country in which it is collected and stored. It ensures that a nation retains control over its data, especially in the areas of national security, personal privacy, and economic assets.Data sovereignty is essential to preserving national independence in the face of globalization in today's interconnected world in the absence of data governance, a country's sensitive information may be vulnerable to foreign inspection, unauthorized access, or alteration, potentially compromising its security and independence[6]. Data sovereignty is particularly important for Iraq, as the country is still developing its cybersecurity policy and legal framework and transitioning to a digital system Ensuring data sovereignty in Iraq means building a secure digital infrastructure where data is stored store in Iraqi territory, within the country's borders and monitors This protects sensitive government and citizen information from only external threats but also enforces strengthen Iraq's rights over its digital assets, allowing it to establish and implement its own data security measures Data sovereignty enables Iraq to maintain the privacy and security of its citizens, supporting independent decision-making and protect the integrity of domestic information This authority to achieve self-governance Is essential, where data has become central to national governance and national security[7].

2.3 The Role of National Data Centers: Global Examples and Their Contributions to Data Sovereignty and Digital Transformation

National Data Centers (NDCs) are places established by governments to centralize and manage a country's critical data, making them key supporters of data sovereignty and digital transformation Its security is that NDC provides access to

countries businesses need to manage their data in order to create scalable and effective digital services. By capturing government, health, financial and citizen data across national borders, NDCs are pillars of security, transparency and efficiency. Globally, many countries have developed NDCs to support their digital transformation goals and protect their data sovereignty[8]. For example, Estonia, known for its advanced digital infrastructure, relies on national data center networks to support its e-government services, enabling Estonia to access digital identity, online voting and public services a secure Data centers are essential to ensure data protection , which will support the digital trust of citizens, and maintain control over domestic affairs. Similarly, France has invested in its national data center infrastructure to protect sensitive data from foreign scrutiny, particularly in response to data privacy concerns about U.S.-based cloud providers. For Iraq, the establishment of the Iraqi National Data Center (INDC) represents an investment in data sovereignty and digital transformation. INDC provides Iraq with services to manage its digital assets, protect national security, and support the modernization of government services. By modeling successful national databases around the world, Iraq can ensure that its citizens' data remains within local jurisdiction, contributing to a secure, efficient and trustworthy digital landscape and self-control is in line with global trends[9].

2.4 Current Requirements of an Efficient National Data Center

1. High-Level Security and Data Protection:
   Security is the number one priority in any high-performance National Data Center (NDC), as it handles the most sensitive government, private and financial data. NDCs with multiple layers of firewalls, intrusion prevention systems and secure access methods are more likely to be targeted by cyberattacks, so advanced encryption standards a deployment, routine security assessments and real-time threat monitoring are essential to protect against breaches in addition to securing physical There are restrictions on access presence, monitoring and emergency planning. Data protection policies should also be well defined, ensuring compliance with national and international laws on data privacy and confidentiality. Together, these initiatives ensure that the NDC remains a trusted and reliable custodian of national information[10].
2. Scalability and Flexibility:
   A state-of-the-art national data center must be scalable and flexible enough to meet increasing data demands as government and its services expand. This means that the data center must be able to handle increasing volumes of data, users and applications without compromising performance. Scalability can be achieved through a modular infrastructure, where additional servers, storage units and network components can be added as needed. The flexibility of data center infrastructure allows it to adapt to new technologies, applications, or needs. For example, virtualized infrastructure, containerization, and cloud-based models help ensure that the data center can adapt to changing business needs, delivering future-proof solutions that support continuous improvement and technological advancement[11].
3. Energy Efficiency and Sustainability:
   National databases consume a lot of energy to power servers and cooling systems. Due to rising energy costs and environmental concerns, energy efficiency is important. The use of energy-efficient technologies such as more efficient servers, less power and advanced cooling systems can help reduce energy consumption. Many modern NDCs use water-cooled or air-cooled solutions to reduce reliance on traditional high-energy cooling systems. In addition, green data centers typically reduce their carbon footprint by incorporating renewable energy such as solar or wind power into their power supply and prioritize energy efficiency and sustainability , national data centers not only reduce operating costs but also support government goals for environmental protection and sustainability[12].
4. Redundancy and High Availability:
   To ensure easy access to critical data services, national data centers should be equipped with new high-availability systems. This means backup servers, power supplies and network connectivity to avoid single points of failure. Redundancy also includes implementing failover mechanisms so that if one component fails, another takes over immediately to maintain increased continuity of service availability essential for disasters availability and business continuity management, as data centers often hold sensitive government and public data. Having multiple geographically distributed data centers or remote storage locations can further enhance reliability, ensuring that data remains secure and accessible even in the event of a disaster or major technical failure[13].
5. Advanced Data Management and Analytics:
   Effective data governance practices are necessary to enhance storage, availability, and resource efficiency in a national database. This includes data classification, indexing, and implementation of systems to ensure rapid and accurate data retrieval. Advanced analytics capabilities also support government decision-making, enabling real-time data insights into infrastructure health, operating systems, and potential security threats Combining artificial intelligence (AI) and machine learning (ML) tools in the data center, enabling predictive analytics to predict equipment failures, energy efficiency, and detect anomalies in real-time s can be done, which contributes to more agile and effective data center management[14].
6. Compliance with National and International Standards:

It is important to adhere to established national and international standards to ensure proper and secure operation of the data center. These standards typically include guidance on data protection, security measures, energy efficiency and business continuity. Certifications such as ISO/IEC 27001 for information security management and ISO/IEC 20000 for IT service services are widely recognized and often required in government-run data centers Compliance with these standards for consumers the role assures that the data center follows best practices and is ready to comply with any compliance regulatory, security, or operational obligations various types. Compliance is also important to build trust among citizens and organizations, as it demonstrates the government's commitment to maintaining high standards in data processing and security[15].

7. Skilled Workforce and Continuous Training:
   An efficient national database needs highly skilled personnel trained in data center management, cybersecurity, network management, data analytics, etc. Given the complexity and sensitivity of the industry, it is imperative that finding employees who can manage, manage and refine processes and professional development is equally important, especially in a rapidly evolving industry where new threats and technologies are constantly emerging. Employees will receive regular training on the latest security measures, software updates, and compliance practices. Additionally, having a robust system for cross-border knowledge sharing and training can ensure that the data center remains fully operational even when critical personnel are unavailable[16].

Table I provides a comparative analysis of national databases in ten countries, focusing on key criteria such as scalability, energy efficiency, data security, redundancy, standards compliance, operational costs and what etc. This reveals that although many countries face advanced data centers with high levels of security and redundancies Some areas with challenges related to high operating costs and energy efficiency about, like India's NIC and Japan's Government Cloud Center, struggle with scalability and security improvements. Overall, the table highlights the importance of infrastructure efficiency, increased energy efficiency and robust data security measures to meet increasing demand and ensure reliability and emphasis on sustainability[17].

TABLE I. COMPARISON OF KEY PERFORMANCE PARAMETERS AND LIMITATIONS ACROSS NATIONAL DATA CENTERS

National Data Center	Scalability	Energy Efficiency	Data Security	Redundancy	Compliance with Standards	Operational Cost	Limitations and Problems
Estonian National Data Center	High	High	High	Advanced	Full (ISO/IEC 27001)	Moderate	High operational costs due to advanced security; increasing energy usage despite energy-saving practices.
France's National Data Center (Groupe La Poste)	Moderate	High	Advanced	High	Full (GDPR, ISO standards)	High	Complexity with GDPR compliance; relatively high energy consumption.
India's National Data Center (NIC)	Moderate	Moderate	Moderate	Limited	Partial	Moderate	Scalability issues with rising data demands; limited redundancy and moderate security measures.
Singapore Government Data Hub	High	High	High	Advanced	Full	High	High setup and maintenance costs; strict compliance adds operational complexity.
UAE Federal Data Center	High	High	Advanced	Advanced	Full	High	High operational and energy costs; reliance on imported technologies for some components.
United States (National Center for Critical Infrastructure)	High	Moderate	Advanced	Advanced	Full (NIST, ISO standards)	High	High operational expenses; varying energy efficiency levels depending on facility.
Australia (National Computational Infrastructure)	Moderate	High	High	Moderate	Full	High	Limited scalability due to budget constraints; high energy costs despite green initiatives.
Japan Government Cloud Center	Moderate	Moderate	Advanced	High	Full (ISO standards)	Moderate	Scalability limited by resource allocation; energy efficiency needs improvement.
Canada's Federal Data Center	High	High	High	Advanced	Full	Moderate	High maintenance and energy costs; requires advanced redundancy to prevent outages.
Germany's Federal IT Center (BWI)	High	Moderate	High	Advanced	Full (GDPR, ISO standards)	High	Elevated operational costs and stringent GDPR compliance; faces scalability issues.
South Korea Government Integrated Data Center	High	High	Advanced	Advanced	Full	High	High initial infrastructure cost; strict compliance and operational expenses.

This study particularly contributes a lot to understanding National Data Centers (NDCs) and their role in supporting national digital transformation and data sovereignty. First, the study provides comparative insights by examining the performance indicators of NDCs in ten different countries. This comparison highlights common challenges faced by these environments, including scalability issues, high operating costs, energy inefficiencies, and the need for data security improved policies By examining these global examples, the study identifies critical areas of ineffectiveness of multiple NDCs and sets out policies for improvement. Another important contribution of the study is to identify the key challenges affecting the performance of the National Data Center[18]. Issues such as limited scalability, insufficient redundancy, and inefficient energy management are common in many countries. These findings underscore the importance of investing in technology upgrades and infrastructure improvements to ensure robust, efficient and secure data center operations. In addition, the study highlights the importance of aligning NDCs with international standards on data protection and privacy, which can help improve compliance and security The study also provides a framework for future reforms that can inform government and organizational approach to enhance NDC implementation. This strategy identifies specific areas of focus, such as adding advanced security measures, scaling up infrastructure to meet increasing data demands, and providing solutions energy efficiency measures and Aligning them, ensuring that NDCs pursue data sovereignty and security The survey contributes to the broader conversation about digital transformation by providing insights into how national data centers can be key drivers of economic growth, national security and effective governance. By emphasizing the critical role of NDCs in ensuring efficient and secure data management, this study contributes to shaping a digital policy vision while contributing to long-term national development[19].

The findings from this study can be used in a variety of ways to improve the development and operation of national databases. Policy makers and government officials can use the survey findings for policy and infrastructure development. Understanding the challenges faced by existing NDCs enables governments to make informed decisions about how to allocate resources and develop strategic priorities to upgrade or build more efficient, secure and scalable data centres in this energy efficiency, data security, measurement and target specific improvements Economic measures can be added. Another key use case is investment in technology. Countries can use the findings of the study to direct investments towards the adoption of new technologies that can address the limitations identified[20]. This includes investments in cloud computing, virtualization technologies and green technologies to increase energy efficiency and scalability and reduce operating costs These investments can help overcome the current challenges of high power consumption and the ability to process the limited data. The study also highlights the importance of harmonization with international standards to ensure compliance with global best practices. Countries can implement this recommendation by aligning their national databases with internationally recognized standards such as ISO/IEC 27001 on data protection and GDPR on privacy, not as a standard compliance with these types will not only enhance data security but improve the facility's ability to safely and reliably handle sensitive data . Additionally, the study encourages governments to use the findings to strengthen national security and data sovereignty. By improving data protection measures and ensuring compliance with local laws and regulations, NDCs can safeguard sensitive information and ensure that sensitive data remains under state control, ensuring security and their own rule has been successful. The insights provided can inform efforts to strengthen data sovereignty policies and protect national digital infrastructure. To address scalability and redundancy issues, the study suggested future proofing techniques. This may include scaling up data center systems to accommodate increasing amounts of data and better redundancy protocols to ensure continuity of services during peak periods or failures In this way beyond this, national data centers can evolve to meet the growing demands for data management in the digital age[21].

3. OVERVIEW OF THE IRAQI NATIONAL DATA CENTER (INDC)

3.1 Establishment and Development

The Iraq National Data Center (INDC) was established as part of a broader strategy to modernize Iraq's digital infrastructure and provide improved national data management across sectors This increased digital activity, which has increased the amount of data that the dramatic increase in production has highlighted the need for a robust system for controlling and protecting vital national data. Initially, the launch of INDC was an important step in addressing the challenges faced by Iraq's fragmented data infrastructure[22]. Prior to the creation of the INDC, data was often stored in decentralized systems, making it difficult to monitor, analyze and protect sensitive information. As part of Iraq's digital transformation strategy, INDC was created to focus on data storage and services to address these challenges. Since its inception, the center has grown through various technological developments, with government investment in state-of-the-art infrastructure, cloud solutions and advanced data management tools This growth reflects Iraq's commitment to that is to be able to exhibit resilience that can help the country's growth and stability in the digital age It can be a digital ecosystem[23].

3.2 Infrastructure and Technology

Iraq's National Data Center infrastructure is designed as an efficient, reliable and secure facility that can meet the country's growing data demands It includes an integrated physical and virtualized infrastructure, with cloud computing , including

data backup, disaster recovery and data analytics. Multidisciplinary Support To ensure efficient and secure data management across government departments and agencies, INDC is equipped with state-of-the-art servers, efficient storage facilities and advanced networking solutions in. Cloud computing is central to the center's technology, allowing for on-demand delivery of IT resources, improving efficiency and reducing costs for government businesses[24]. In addition, INDC uses virtualization techniques to optimize server and storage operations, which contributes to more efficient and flexible resource utilization by scaling up or down based on requirements Security is a major concern for INDC, since it handles sensitive national data, including personal information, government records , and financial information. The center uses state-of-the-art security measures including encryption protocols, multi-channel security and multifactor authentication to protect data from unauthorized access and cyber threat Security audits regularity and adherence to international standards ensures the center's resilience to potential breaches. In addition to these technical safeguards, INDC is supported by a team of cybersecurity experts who continuously review and improve security measures to protect against evolving threats[25].

3.3 Mission and Objectives

The main mission of the Iraqi National Data Center (INDC) is to establish a centralized location for viewing, storing and processing data to support the country's digital transformation INDC aims to streamline government service delivery, for decision a through data has been improved, and improved efficiency in public sector operations Allows integration, facilitates management of national affairs and views as data will move seamlessly between government agencies INDC's primary objective is to support data sovereignty by ensuring that Iraqi data remains under federal control. This is especially important to maintain the confidentiality and security of sensitive national information. By locally monitoring data storage and operations, INDC helps protect against external data breaches, foreign jurisdiction over sensitive data and thus strengthens national security, promoting self-governance encourage, and reduce reliance on foreign cloud providers. Another important objective of INDC is to improve efficiency and service delivery across the public sector. By adopting modern technologies such as cloud computing and data analytics, INDC aims to provide faster, more cost-effective systems for government applications This enables more efficient use of resources, faster response times and effective public services. For example, by digitizing government records and providing secure cloud services, INDC facilitates better communication between government agencies, streamlines business processes, reduces the time and resources required to consume them address and manage issues in addition to supporting Iraq's digital financial development INDC plays an important role in promoting economic growth by doing so. It enables you to create a more conducive environment for businesses and startups, providing secure cloud-based services, data storage solutions and analytics tools that can be used for innovation INDC aims to make data-driven decisions so -is to foster a culture of productivity, which is essential for Iraqi economic development, public policy and governance in an increasingly digital world.

4. INDC'S ROLE IN DIGITAL TRANSFORMATION

4.1 Data Centralization and Accessibility

The Iraqi National Data Center (INDC) plays a key role in centralizing national data, greatly improving its accessibility and management in government agencies Before the establishment of INDC, data was often distributed in Iraq, storing it in isolated systems and the challenges would be in a centralized center By collecting data, INDC ensures that government agencies can access relevant information quickly and efficiently. This concept reduces data silos, improves accuracy and consistency of information, enables easy sharing of data across departments, improves communication and decision-making INDC's architecture can store, manage and retrieve data efficiently, enhancing productivity facilitates public sector agencies and improves overall governance.

4.2 Support for Government Services

INDC has been instrumental in enabling the digitization of government services, transforming the way Iraqi public agencies interact with the public. One key way to support those government services is to provide a centralized e-government infrastructure. These services range from online tax return systems, digital health records and electronic voting platforms to business licenses and licenses Hosted in the national data center, INDC ensures that these services are securely stored, accessible and scalable in to meet the growing demands of the public INDC also facilitates the integration of services, in order to Create a more flexible public experience. Citizens, for example, can now access multiple government services through a single online portal, reducing waiting times, increasing convenience and reducing bureaucratic delays.

4.3 Enhancing Public Sector Efficiency

INDC increases the efficiency of the public sector by modernizing the way government services are run and streamlining business processes. By centralizing data, government agencies are better equipped to handle big data analytics that can guide informed decision-making and policy implementation INDC gives government employees the tools they need to manage resources effectively, has responded more rapidly to public needs, and distributed public funds in a more efficient manner. Additionally, with cloud-based solutions, INDC reduces the need for expensive physical infrastructure and reduces

downtime, resulting in productivity and productivity in greater efficiency comes in. The Center also supports the digitization of key sectors such as payroll, social security and public procurement, contributing to faster and more transparent processes.

4.4 Innovation and Development

INDC plays a key role in driving innovation in Iraq's IT and digital sectors. Offering state-of-the-art infrastructure and data warehousing capabilities, INDC is the basis for innovation in areas such as cloud computing, big data analytics and artificial intelligence (AI). or to support. In addition, INDC acts as a catalyst for the IT industry by providing a secure and scalable platform where startups can develop and test new applications and functionality. This support helps develop a vibrant digital ecosystem, vital to Iraq's economic growth and establishing the country as a regional leader in technology and digital services INDC leads efforts to ensure for Iraq data protection and privacy through robust security measures. The center adheres to the highest security standards, using advanced encryption techniques and multiple access methods that protect sensitive national data from unauthorized access This security measure is designed to to reduce the risk of data breaches and cyberattacks that are increasingly common in the digital ageIn addition, INDC ensures compliance with national data privacy laws aimed at protecting the personal information of Iraqi citizens and organizations By implementing strict data privacy policies and security measures, INDC conditions a secure environment for data storage and processing, ensuring that sensitive data is protected from external and internal threats Ability to maintain control over your data if influence or dislike and . INDC manages its own infrastructure rather than relying on foreign cloud providers to ensure that Iraqi data remains within national control This control enables Iraq to protect sensitive data, especially in areas such as security, governance and healthcare, where national security and privacy are paramount. By centralizing data storage and processing within its borders, Iraq can protect itself from the risk of foreign governments or companies obtaining sensitive data INDC acts as a shield, and it enables Iraq to maintain its sovereignty over digital resources and avoid the possibility of its data being used or manipulated by outside entities They are consistent with national policies, aimed at protecting the country's digital assets and ensuring that will be handled ethically of citizen data Iraq has established a legal framework for data management and retention, ensuring that these laws meet international standards for data protection and privacy INDC closely follows these policies to ensure that Data collected by government agencies is properly stored, handled responsibly and used lawfully. Furthermore, Iraq's policy on data sovereignty emphasizes the importance of self-reliance in the management of digital services, reducing the country's reliance on foreign actors INDC governing this policy help strengthen Iraq's commitment to data protection, privacy, and national security. Despite significant progress in developing the INDC, Iraq continues to face technical and infrastructural challenges that hinder its full potential. The initial set-up required significant investment in state-of-the-art equipment and technology, but challenges persist, including outdated infrastructure, limited technical resources and labour lack of expertise in advanced areas such as cloud computing and data analytics. These limitations can delay development, reduce the center's ability to scale as data demand increases, and hinder the adoption of new technologies. To ensure that INDC continues to produce ground-breaking digital projects, continued investment in hardware, software and human capital will be required. Cyber security is one of the most important challenges facing INDC, as the center is a major target of cyber-attacks because of the sensitivity of the data it manages that hackers and cybercriminals can attempt to breach the center's security systems to steal sensitive data or damage government services. Although indc fixation, enlisting, accidents, etc., and the implication of growth in society size as active-in-law requires the centers to face the possibility of attack. Keep employees accountable Training is important.

Although Iraq has made progress in developing a legal framework for data sovereignty, there are still gaps in the legal and regulatory environment affecting the implementation of INDC for example, vague or inconsistent legislation on data protection, privacy and computing so safety can pose challenges to ensure full compliance with national and international standard Furthermore, as technology advances, regulatory systems can struggle to keep up with new developments in areas live that as cloud computing, artificial intelligence, and big data. INDC faces ongoing challenges related to funding and investment, which are essential for its growth and development. Designing and maintaining a state-of-the-art data center infrastructure requires significant financial resources, especially limited government budgets in areas such as technology upgrades, security upgrades and personnel. international cooperation and investment in technology companies, to ensure the continued expansion and modernization of the center.

5. FUTURE PROSPECTS AND RECOMMENDATIONS

Cybersecurity is one of INDC's greatest concerns, as it handles the nation's most sensitive information, including government records, personal information, and national security information. Hackers, cybercriminals, and state-sponsored employees also attempt to steal sensitive data, compromise government services, compromise national security or breach Center defenses Cybersecurity threats such as malware, phishing attacks, denial-of-service (DoS) attacks, and ransomware poses significant risks He remains vigilant In response to these threats, INDC has has implemented a number of cybersecurity measures to protect its data and services. These initiatives include advanced encryption protocols, multifactor authentication, firewalls, intrusion detection systems (IDS), and robust access controls to prevent unauthorized access INDC also works closely with global cybersecurity experts to ensure its systems are up to date with the latest threat intelligence security measures given its nature, must INDC cybersecurity programs remains flexible and flexible. Regular security audits, ongoing

assessments, and employee training on the latest cybersecurity practices are essential to ensure the site can effectively defend against emerging threats. Furthermore, improving cybersecurity skills within the broader public sector is essential, as government employees may inadvertently contribute to security breaches if they do not learn best practices for effectively handling sensitive information that.

6. CONCLUSION

In summary, this study highlights the important role of the Iraqi National Data Center (INDC) as a central repository and enabler of accessible, secure, and efficient digital services INDC laid the foundation for government improved infrastructure, innovation in IT and promotion of data sovereignty—Iraq's national self-governance in the digital age is essential for s Causes: Despite these advances, the INDC has limitations that it is essential. Technological constraints, antiquated infrastructure and lack of specialist knowledge are hindering its ability to meet the high standards of today's database. Furthermore, cybersecurity threats that pose a threat to vital national information require constant vigilance and a well-prepared response plan. Regulatory gaps, often accompanied by rapid technological change, create a challenging environment to align INDC operations with international standards, while financial constraints limit the potential for industry growth and development long-term sustainability , including strategic investments, program updates, and collaboration with international partners The implementation of this strategy will enable INDC to strengthen its role as a secure, resilient and advanced national data center, ensuring Iraq's place in the global digital economy and supporting sustainable national development aspirations.

Conflicts Of Interest

The authors declare no conflicts of interest regarding the publication of this research.

Funding

This research received no external funding.

Acknowledgment

The authors thank all the individuals and institutions that supported this research, including our relevant academic institutions and colleagues who provided valuable input. We appreciate the tools and platforms for data analysis, and the reviewers for their helpful suggestions.

References

[1] A. M. Ali, M. A. Ngadi, R. Sham, and I. I. Al_Barazanchi, "Enhanced QoS Routing Protocol for an Unmanned Ground Vehicle, Based on the ACO Approach," *Sensors*, vol. 23, no. 3, p. 2023, 2023, doi: 10.3390/s23031431.

[2] A. M. Ali, M. A. Ngadi, I. I. Al Barazanchi, and P. S. JosephNg, "Intelligent Traffic Model for Unmanned Ground Vehicles Based on DSDV-AODV Protocol," *Sensors (Basel).*, vol. 23, no. 14, pp. 1–13, 2023, doi: 10.3390/s23146426.

[3] A. M. Ali, M. A. Ngadi, R. Sham, and I. I. Al Barazanchi, "Enhanced QoS Routing Protocol for an Unmanned Ground Vehicle, Based on the ACO Approach," *Sensors (Basel).*, vol. 23, no. 3, 2023, doi: 10.3390/s23031431.

[4] A. A. K. Ammar, "Data Governance and Decentralization: A Blockchain Approach," *Journal of Information Technology*, vol. 45, no. 3, pp. 12–28, 2021.

[5] S. A. H. Ahmed, "The role of cloud storage in rebuilding governmental data after conflict: A case study of Sudan," 2023.

[6] B. Hassib and J. Shires, "Cybersecurity in the GCC: From economic development to geopolitical controversy," *Middle East Policy*, vol. 29, no. 1, pp. 90–103, 2022.

[7] M. Zayani and J. F. Khalil, *The Digital Double Bind: Change and Stasis in the Middle East*. Oxford University Press, 2024.

[8] S. A. AbdulAmeer, W. R. Saleh, R. Hussam, H. Al-Hareeri, T. Alghazali, Y. S. Mezaal, and I. N. Saeed, "Cyber security readiness in Iraq: Role of the human rights activists," *International Journal of Cyber Criminology*, vol. 16, no. 2, pp. 1–14, 2022.

[9] M. H. Ali, A. Ibrahim, H. Wahbah, and I. Al_Barazanchi, "Survey on encode biometric data for transmission in wireless communication networks," *Period. Eng. Nat. Sci.*, vol. 9, no. 4, pp. 1038–1055, 2021, doi: 10.21533/pen.v9i4.2570.

[10] A. Al-Rawi, "Cloud-Fog Computing Models for Smart City Deployment," *Computers in Urban Studies*, vol. 32, no. 2, pp. 155–170, 2020.

[11] Z. Liu and T. H. Zhang, "Digital Silk Road: Risks and Governance Framework," *Asian Policy Journal*, vol. 15, no. 4, pp. 457–479, 2021.

[12] P. Neirotti *et al.*, "Current Trends in Smart City Initiatives," *Cities*, vol. 38, no. 1, pp. 25–36, 2014.

[13] A. Cammett *et al.*, "Social Contracts in the Arab World," *Middle Eastern Studies*, vol. 47, no. 6, pp. 923–942, 2018.

[14] A. Calderaro and S. Blumfelde, "Artificial intelligence and EU security: The false promise of digital sovereignty," *European Security*, vol. 31, no. 3, pp. 415–434, 2022.

[15] K. Taylor, "Digital Decolonization and Sovereignty Challenges," *International Digital Ethics Review*, vol. 8, no. 2, pp. 112–130, 2021.

[16] M. Leese, S. Noori, and S. Scheel, "Data matters: The politics and practices of digital border and migration management," *Geopolitics*, vol. 27, no. 1, pp. 5–25, 2022.

[17] M. Musoni, P. Karkare, C. Teevan, and E. Domingo, "Global approaches to digital sovereignty: Competing definitions and contrasting policy," 2023.

[18] R. Sioshansi, "Energy Policy Adaptations in Emerging Economies," *Renewable Energy Policy*, vol. 14, pp. 80–102, 2019.

[19] S. C. West, "Cyberwarfare and Digital Tools in Modern Conflict," *Journal of Conflict Studies*, vol. 45, no. 1, pp. 35–53, 2020.

[20] S. R. Ersoy and J. Terrapon-Pfaff, "Sustainable transformation of Iraq's energy system: Development of a phase model," 2022.

[21] J. Arquilla and D. Ronfeldt, *Networks and Netwars: The Future of Warfare*. RAND Corporation, 2001.

[22] M. A. Hashem, H. Fakhari, and E. A. Naftchli, "The effect of IT governance on the relationship between corporate social responsibility and performance in Iraqi banks," *International Journal of Professional Business Review*, vol. 8, no. 5, p. 49, 2023.

[23] D. Petcu, "Multi-Cloud: Challenges and Opportunities," *Computer Science Review*, vol. 15, pp. 55–65, 2015.

[24] S. S. Dali and A. Asmar, "Study and analysis of models from the sovereign wealth fund for selected countries with a reference to the possibility of developing a proposed model suitable for the Iraqi economy," *Al-Qadisiyah Journal for Administrative and Economic Sciences*, vol. 25, no. 4, 2023.

[25] H. Černy, "How the Iraqi Kurdistan independence debate came to die: Western IR scholars as co-protagonists of the nationalist conflicts they set out to describe," in *Variations on Sovereignty*, Routledge, pp. 108–130, 2023.

[26] S. A. Shawkat and I. Al-Barazanchi, "A proposed model for text and image encryption using different techniques," *TELKOMNIKA (Telecommunication Comput. Electron. Control)*, vol. 20, no. 4, p. 858, Aug. 2022, doi: 10.12928/telkomnika.v20i4.23367.

[27] H. R. Abdulshaheed, H. H. Abbas, E. Q. Ahmed, and I. Al-Barazanchi, "Big Data Analytics for Large Scale Wireless Body Area Networks; Challenges, and Applications," 2022, pp. 423–434.