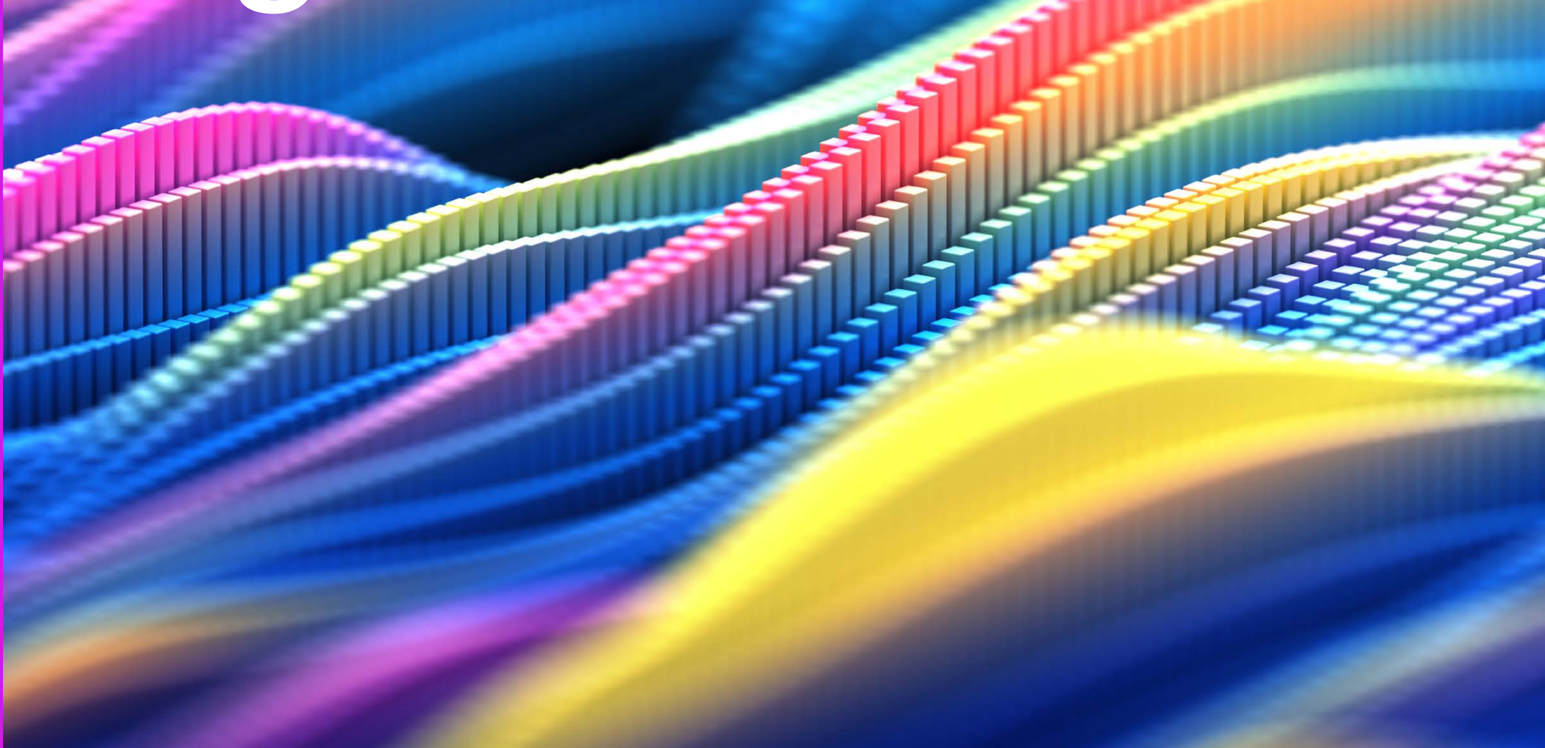
North Sea Energy
offshore system integration

D5.5
WHITE PAPER

North Sea Energy 2023-2025

Unlocking Data Sharing Potential in the North Sea Through Digitalization



North Sea offshore system integration Energy

D5.5 WHITE PAPER

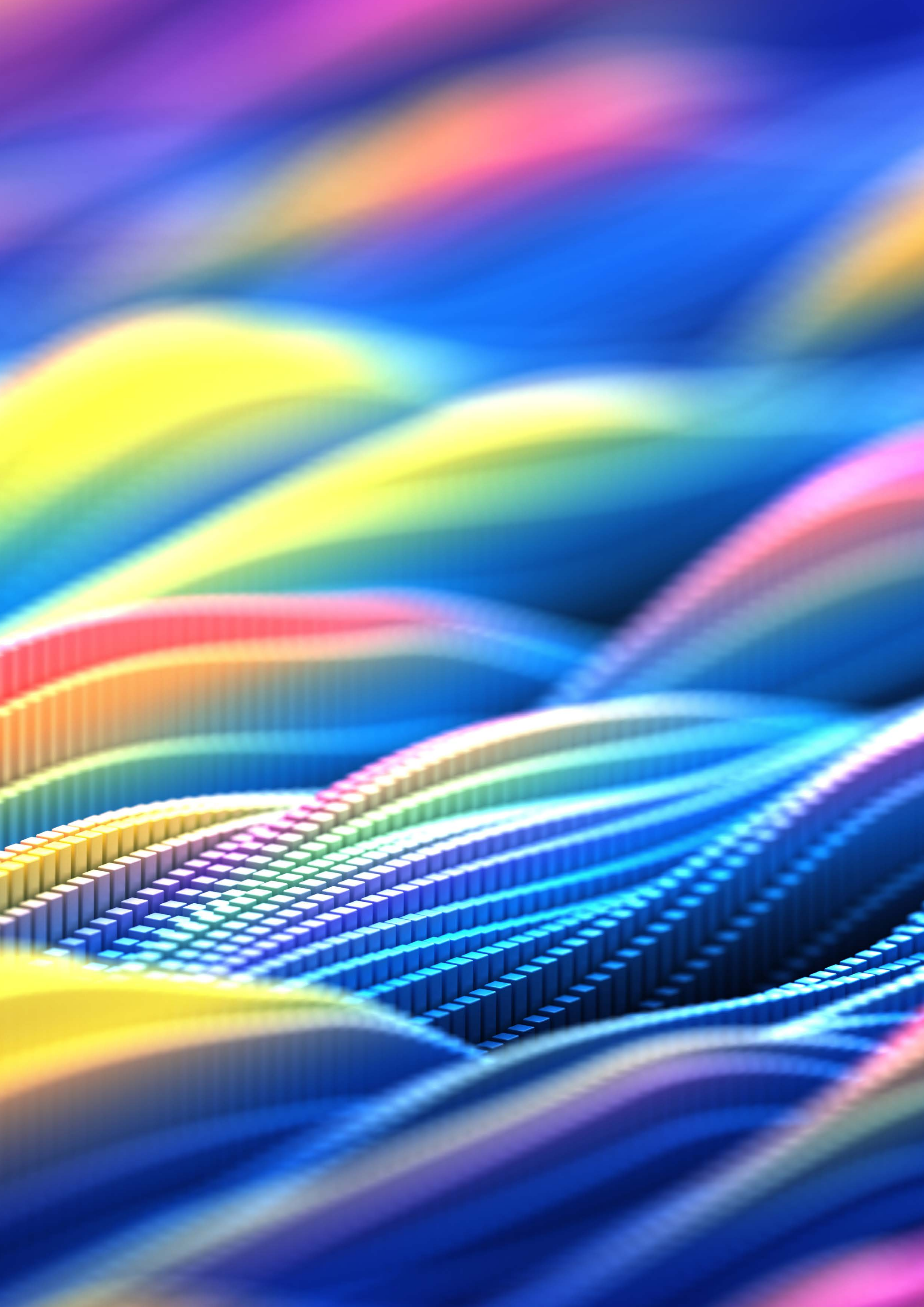
North Sea Energy 2023-2025

Unlocking Data Sharing Potential in the North Sea Through Digitalization

Prepared by:

TNO
Pejman Shoeibi Omrani
Joris Koornneef
Leila Hashemi

The project has been carried out with a subsidy from the Dutch Ministry of Economic Affairs and Climate, National Schemes EZK-subsidies, Top Sector Energy, as taken care of by RVO (Rijksdienst voor Ondernemend Nederland)

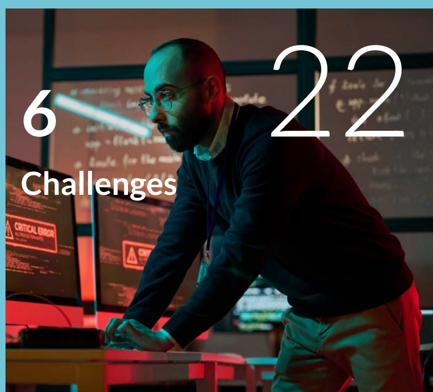


Contents


3
10
Overview of available technologies


4
15
Data sharing in other sectors


5
19
Potential case studies in the North Sea


6
22
Challenges

Executive summary

Introduction

Data sharing across the North Sea holds significant potential for advancing collaboration, innovation, and efficiency in various sectors, including energy, marine research, and infrastructure management. This report aims to investigate both the potential benefits, and the key challenges related to data sharing, supported by relevant case studies.

Problem Statement

This report addresses the challenges and barriers to effective data sharing across the North Sea. Despite its clear benefits, effective data sharing across North Sea industries faces substantial barriers. These include cybersecurity threats, unclear data ownership, complex regulatory landscapes, and varying willingness of stakeholders' to engage in data sharing.

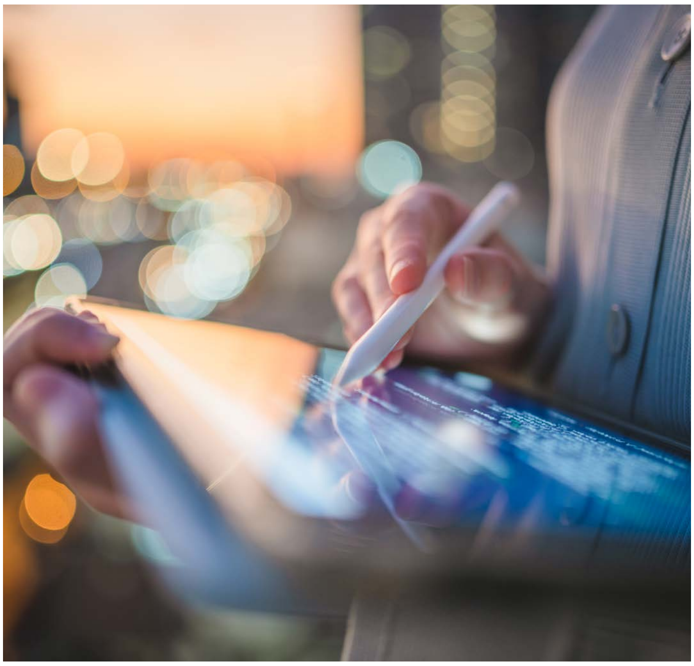
Research question and goal

This white paper explores the possibilities enabled by digital technologies, such as secure multi-party computation and federated learning, which allow for collaborative data utilization without compromising privacy or ownership. It highlights case studies that demonstrate the practical benefits of data sharing. Furthermore, the paper identifies critical challenges that must be addressed to unlock this potential, including cybersecurity risks, data ownership concerns, regulatory compliance, and the willingness of stakeholders to share data.

Approach & scope: The approach includes literature reviews, interviews. The scope covers geographic coverage (North Sea region, including hubs and national entities), technical aspects (e.g., hydrogen production, offshore wind, carbon capture and storage), and thematic areas (technical, economic, and environmental impacts).

Key Findings: The main findings highlight the potential benefits of data sharing, such as improved operational efficiency and cost optimization across sectors like offshore wind, hydrogen and carbon capture. Technologies such as federated learning and secure multi-party computation are mentioned as the promising methods that enables collaborations without compromising data privacy. However, challenges related to data ownership and inconsistent data standards remain. The findings suggest that addressing the identified challenges can unlock the full potential of data sharing that leads to effective and secure collaboration in the North Sea.

Recommendations & actions: This research introduces secure data sharing technologies and relevant case studies. Furthermore, this reports identifies areas that can impact the adoption of these technologies, including enhancing cybersecurity measures, clarifying data ownership, ensuring regulatory compliance and encouraging stakeholder participation. By addressing these, stakeholders can achieve secure, sustainable and efficient collaboration across the North Sea region.



Data sharing across the North Sea boosts collaboration, innovation, and efficiency.

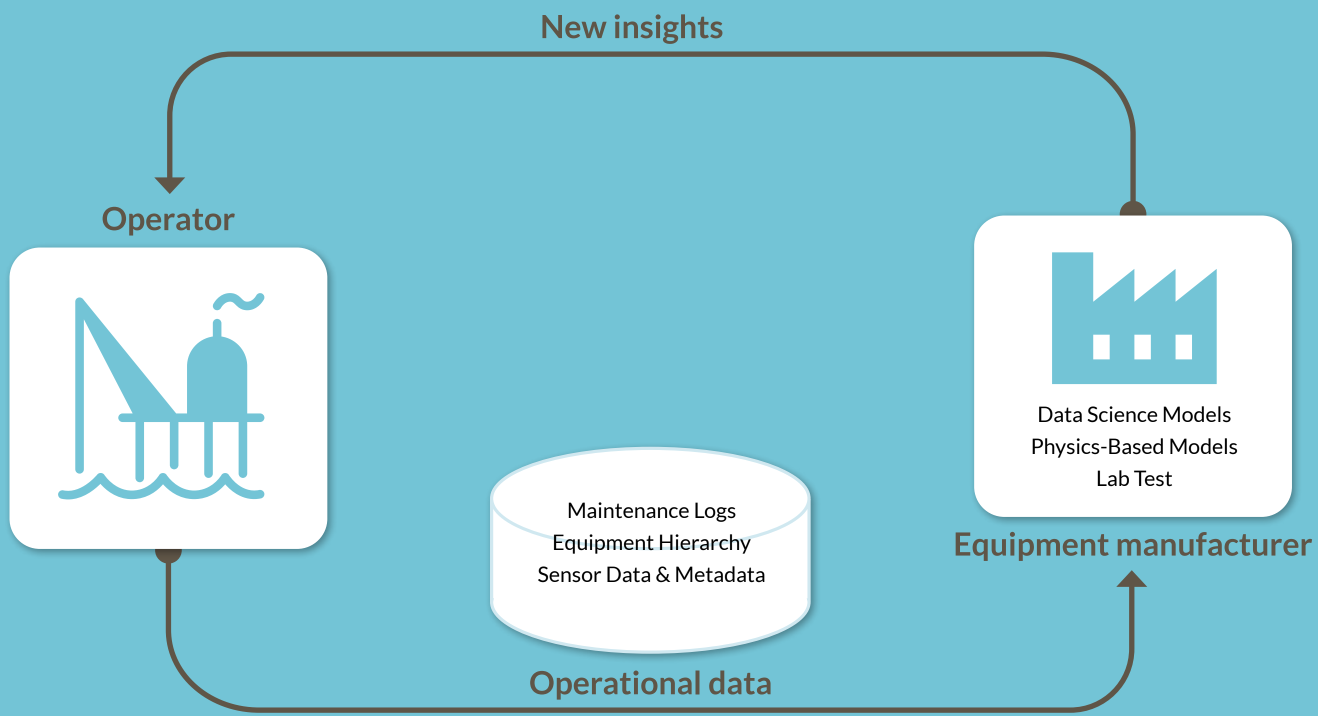
1 Introduction

The North Sea is an essential region for various sectors including renewable energy, offshore oil and gas, maritime logistics, fisheries, and ecological protection. Despite the importance of these industries, effective data sharing remains limited. Many organizations still depend on outdated systems and traditional paper-based methods, causing inefficiencies, higher operational costs, and increased environmental and safety risks (Aadland et al., 2019; Laborie et al., 2019). Effective data sharing across the North Sea industries is challenging due to isolated data hubs. These isolated hubs restrict information flow between organizations, leading to poor collaboration, operational errors, and missed opportunities for improving performance and safety (Elichev & Muñoz, 2018; Caso, 2020).

Recent advancements in digital technologies have demonstrated strong potential to overcome these challenges. Implementing modern data-sharing technologies can improve decision-making, operational efficiency, safety, and environmental sustainability (Bergmann et al., 2021; Lind et al., 2021). One example is the use of digital twins that allows for real-time monitoring and predective analysis. These systems integrate live data streams with simulation and modellings and give more insights to operators and manufacturers to take informed and proactive decisionsand a shared operational context. As shown in Figure 1.1, foundational digital twins can provide a central platform where operators shaare live operational data, while equipment manufacturers can use this data and by simulations or syntetic measurements, send back additional information to the system. This two-way exchange improves decision making, performance and efficientcy for both sides (Laborie et al., 2019). Moreover, digital tools used in offshore operations have improved maintenance planning, reduced inspection times, and provided better access to essential operational data, directly improving safety and efficiency (Aadland et al., 2019).

Additionally, digital tools have supported renewable energy projects by providing better insights into environmental impacts, particularly concerning bird populations around offshore wind farms. Advanced movement modeling and

Figure 1.1. A foundational digital twin provides two-way data exchange between operators and equipment manufacturers. Operational data streams from offshore systems are used by manufacturers and enabled then to feed their own insights or derived information (e.g., synthetic temperature or flow information created by a simulator for equipment where no real sensor exists) back into the foundational digital twin recreated from, (Laborie et al., 2019).



monitoring technologies help planners minimize ecological disturbances, demonstrating clear benefits for environmental conservation (Masden et al., 2009; Masden et al., 2010; Drewitt & Langston, 2006).

Expanding the use of digital solutions for data sharing across the North Sea can lead to innovation, cost reduction, enhanced safety, and improved ecological management. Digitalization and data exchange have been identified as key enablers for a modern adn resilient energy systems (Directorate-General for Energy, 2024)[1]. The Data for Energy (D4E) subgroup, launched in November 2024, aims to enhance access, sharing, and reuse of energy-related data. Its key priorities include energy market flexibility, bi-directional EV charging, and smart building renovations, aligning with the European Green Deal and Digital Decade. Experts are developing high-level use cases, leveraging insights from EU-funded projects and existing policy frameworks. However, achieving these benefits requires addressing significant challenges, such as cybersecurity risks, data ownership, regulatory compliance, and fostering stakeholder willingness to share sensitive information (Dutkiewicz et al., 2022; Varoli & Steinbach, 2025).

Digital technologies, including secure multi-party computation and federated learning, now offer solutions to facilitate data sharing while maintaining data privacy, security, and ownership. These advancements enable stakeholders to unlock valuable insights from shared data without compromising sensitive information (Marwan et al., 2016).

This paper discusses how digital technologies can unlock the full potential of data sharing in the North Sea. It will outline key technologies, review successful examples from different sectors, propose relevant case studies for North Sea operations, and address critical challenges that must be managed to achieve these objectives.

1 https://energy.ec.europa.eu/news/digitalisation-and-data-exchange-are-key-enablers-modern-and-resilient-energy-system-2024-12-02_en

2

Data

Before diving into the complexities of data sharing in North Sea energy systems, it is essential to first understand the different types of data, levels of accessibility, and data ownership structures. These elements form the foundation for an effective data-sharing framework that enables collaboration across stakeholders while ensuring security, transparency, and regulatory compliance.

As illustrated in the *Figure 2.1*, data in North Sea energy systems can be categorized based on three key dimensions: supply chain, data accessibility, and data ownership. The supply chain perspective includes various data types such as production data, transmission data, storage data, and consumption data, each critical for operational decision-making. In terms of accessibility, data can be private, restricted/shared, or open/public, reflecting different levels of control and availability. Finally, data ownership is distributed among several stakeholders ranging from energy producers, grid and infrastructure operators, market operators, regulators, technology providers, to logistics companies and ecological institutions, each contributing valuable information to the system.

The nature of the data itself can vary significantly. Some data are structured, such as sensor readings, market prices, and asset maintenance logs, which are stored in databases and easily processed. Other data are unstructured, including satellite imagery, maintenance reports, and environmental impact assessments, requiring advanced analytics and processing techniques. Recognizing these distinctions is crucial for designing a robust data-sharing ecosystem that balances accessibility with security and efficiency.

The other distinction in the data that needs to be made is whether the data is historical or real-time. Real-time data often generated through sensor readings and monitoring systems which are primarily used for operational decision-making. Historical data, such as reports and logs are useful information for mid- to long-term planning, forecasting, and modifications in the systems.

One of the key considerations for data when it comes to data-sharing is ensuring data interoperability across diverse stakeholders. Each entity collects and stores data using different formats, protocols, and proprietary systems, creating barriers to efficient data exchange and integration. The lack of common standards can hinder cross-sector collaboration and slow down the development of integrated energy systems. To address this, the adoption of standardized data exchange frameworks, such as Open Energy Data standards, IEC standards for grid data, and international offshore energy protocols, is essential. Furthermore, interoperability initiatives driven by EU-funded projects, European Data Spaces (The energy data space, 2025) [2], and Open Energy Data Platforms (Open Energy Platform, 2025)[3] aim to harmonize data-sharing mechanisms across multiple energy sectors.

2 Enershare | The Energy Data Space for Europe, https://enershare.eu/
3 OEP, https://openenergyplatform.org/

Figure 2.1. Classification of data in the North Sea energy systems

Data Accessibility	Data Owner	Supply Chain, Type of Data
Private/corporate data	Operators (energy producers, grids, vessel)	Operation data (production, transmission, storage, consumption)
Public/ Public data	Energy consumers	Logistics data
Restricted/Shared data	Service companies	Service and maintenance data
	Logistic companies	Market data
	Original equipment manufacturers (OEMs)	Ecological and environmental data
	Regulators	Meteorological and oceanographic data
	Meteorological agencies	Geospatial data
	Ecological institutions	
	NGOs	

3

Overview of available technologies

The top technologies for data sharing, particularly in energy systems and sectors like the North Sea energy ecosystem, include the following.

3.1 Federated Learning

Federated learning (FL) is also known as collaborative learning and originally created by Google. It allows multiple parties to collaboratively train machine learning models without sharing raw data, thus maintaining data privacy. Instead, only model updates (e.g., weights) are exchanged, ensuring data privacy (Xu et al., 2021). The first version of the model is sent to the parties, so they can train it locally using their own data. After that, they send the updated model information such as wights or gradient back to the main server, *Figure 3.1*. The server collects the updates from all parties, average them and creates a new improved version of the model. These updates are then shared with the parties again. These steps are repeated until the model becomes more accurate (Nadian-ghomsheh, 2021).

There are two main types of FL: Horizontal and Vertical. In horizontal (sample-based) FL different parties share the data with the same features, which provides the extended dataset for training one model. This combining data from different sources allows to reduce the bias and have more accurate and reliable model. On the other hand, in vertical (featured-based) FL the data from different parties has different features for the same samples. For example, an eCommerce company and a credit card company can train a model together with different data features to provide a fraud detection model (Nadian-ghomsheh, 2021).

Application: Useful for energy systems to build predictive models (e.g., equipment health monitoring, demand forecasting) across distributed datasets from different stakeholders.

3.2 Secure Multi-Party Computation (SMPC)

SMPC enables multiple parties to jointly compute a function over their private inputs while keeping those inputs confidential (Abbe et al., 2012; Bogdanov et al., 2012; Doğuç, 2022). In 1982, Yao introduced a method that allows two parties, who do not trust each other, to perform secure transactions. He showed that both parties can work together and get a correct result without sharing their private data using

Figure 3.1. Privacy-preserving machine learning and multi-party computation technique, federated learning, recreated from (Nadian-ghomsheh, 2021).

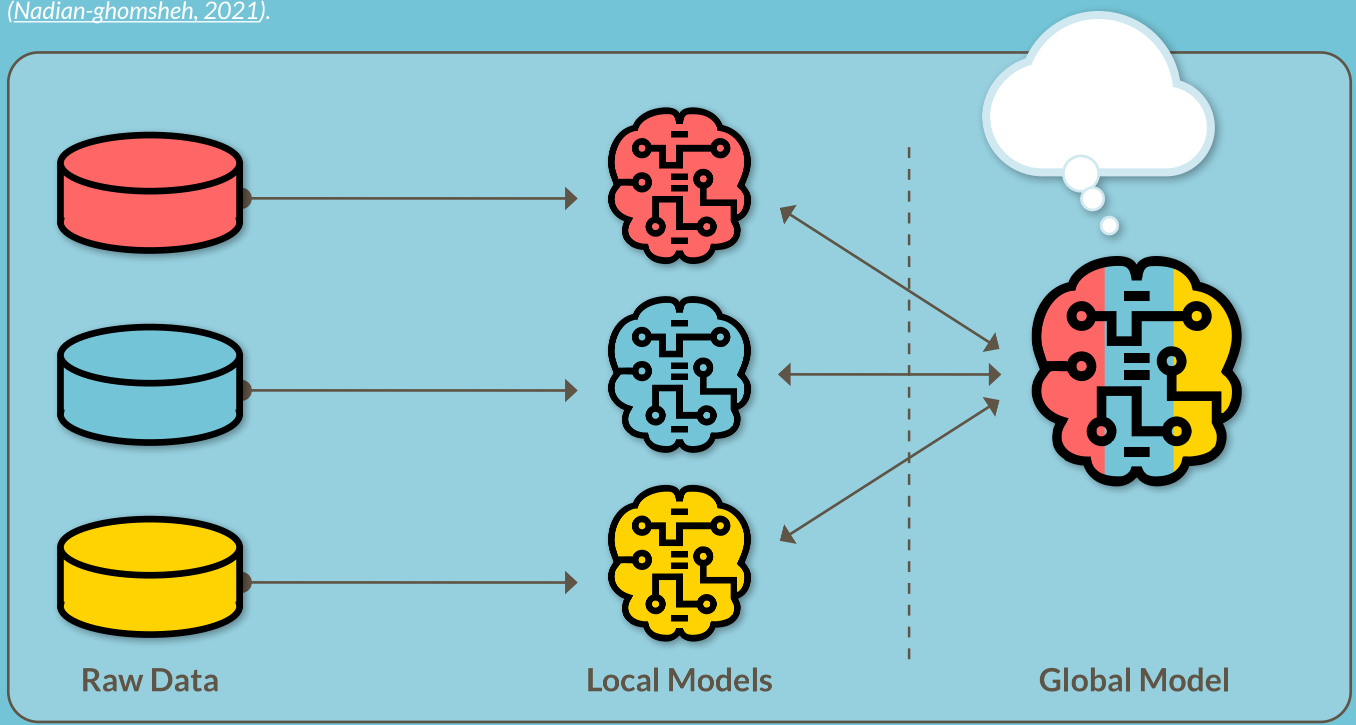


Figure 3.2 Secure multi-party computation. In security sharing, security values (blue and yellow pie) are split into any number of shares that are distributed among the computing nodes. During the computation, no computation node is able to recover the original value nor learn anything about the output (green pie). Any nodes can combine their shares to reconstruct the original value, recreated from (Xu et al., 2021)

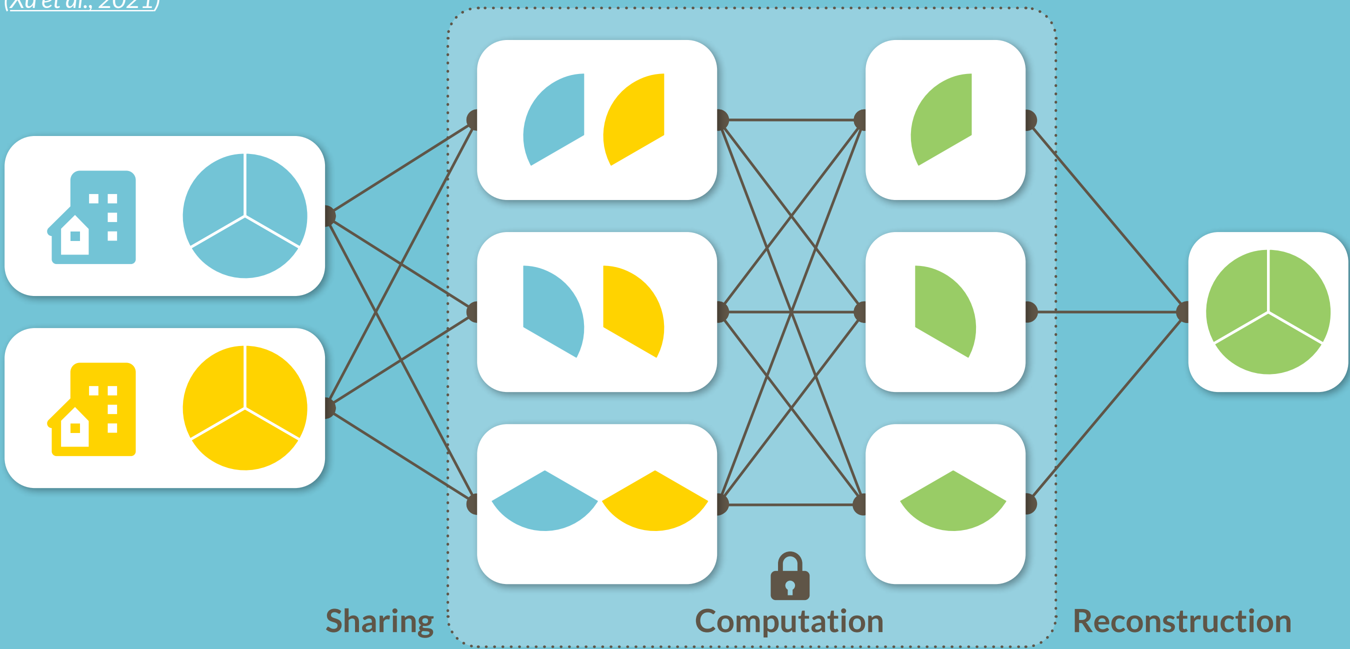
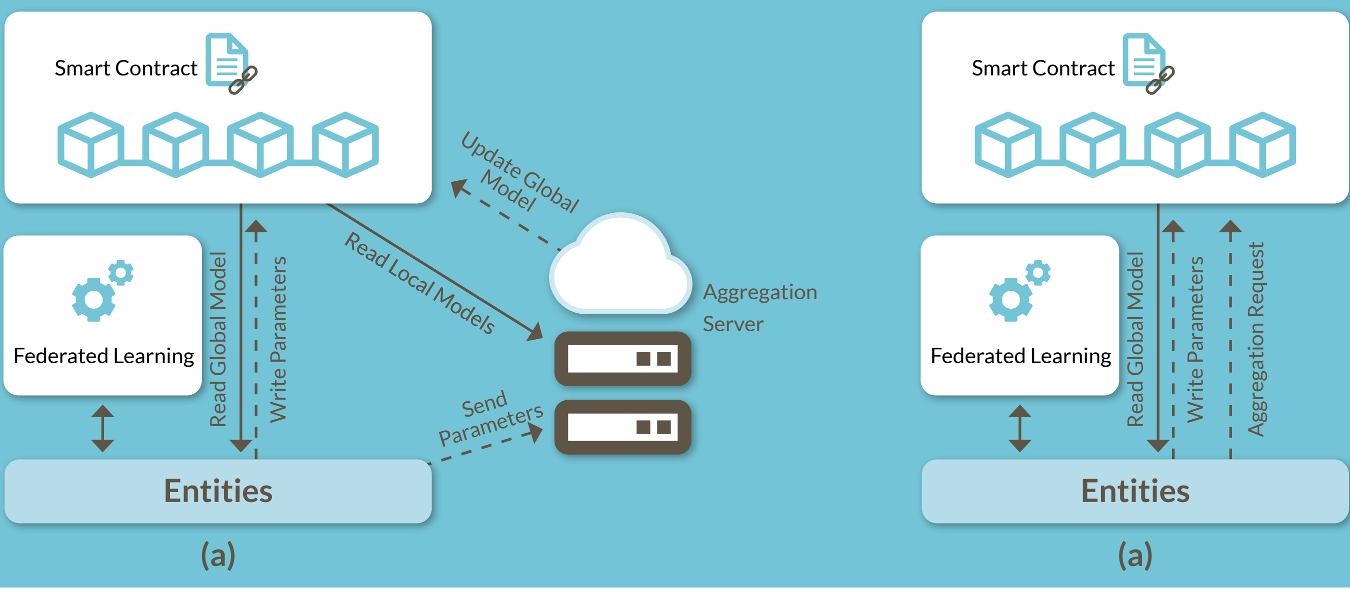


Figure 3.3. Flat Blockchain and Federated Learning-Based Models on the Internet of Energy: (a) Federated Learning and Flat Blockchain-based Systems with Centralized Aggregation, (b) Federated Learning and Flat Blockchain-based Systems with Decentralized Aggregation. In (a), the entities either send local models to the server for aggregation or they write them to the blockchain where the server can access them. In (b), entities might request for aggregating the model, or the aggregation will be done automatically by the smart contract, recreated from (Zekiye & Özkasap, 2023).



Boolean circuits. Over time, this idea was extended to work with more than two parties (Yao, 1982). Each party splits its data into secret (shares) and distributes these shares to other parties, *Figure 3.2*. Then, using mathematical operations on these shares, the compute the desired function together. Since no party has the full data, privacy is secured during the process (Doğuç, 2022).

Application: Ideal for energy collaborations where participants need aggregated insights (e.g., joint asset performance analysis) without revealing proprietary or sensitive data.

3.2.1 Blockchain Technology

Blockchain provides a decentralized, secure, and transparent way to manage data transactions and ensure trust between parties, *Figure 3.3*. It supports immutable records and smart contracts for automating data access agreements (Zekiye & Özkasap, 2023)

Application: Data provenance, secure transactions, and energy system traceability (e.g., carbon credits, energy trading).

3.3 Homomorphic Encryption

Homomorphic encryption allows computations to be performed on encrypted data without decrypting it, *Figure 3.4*. This ensures data privacy while still enabling analysis (Cheng et al., 2023; Marwan et al., 2018).

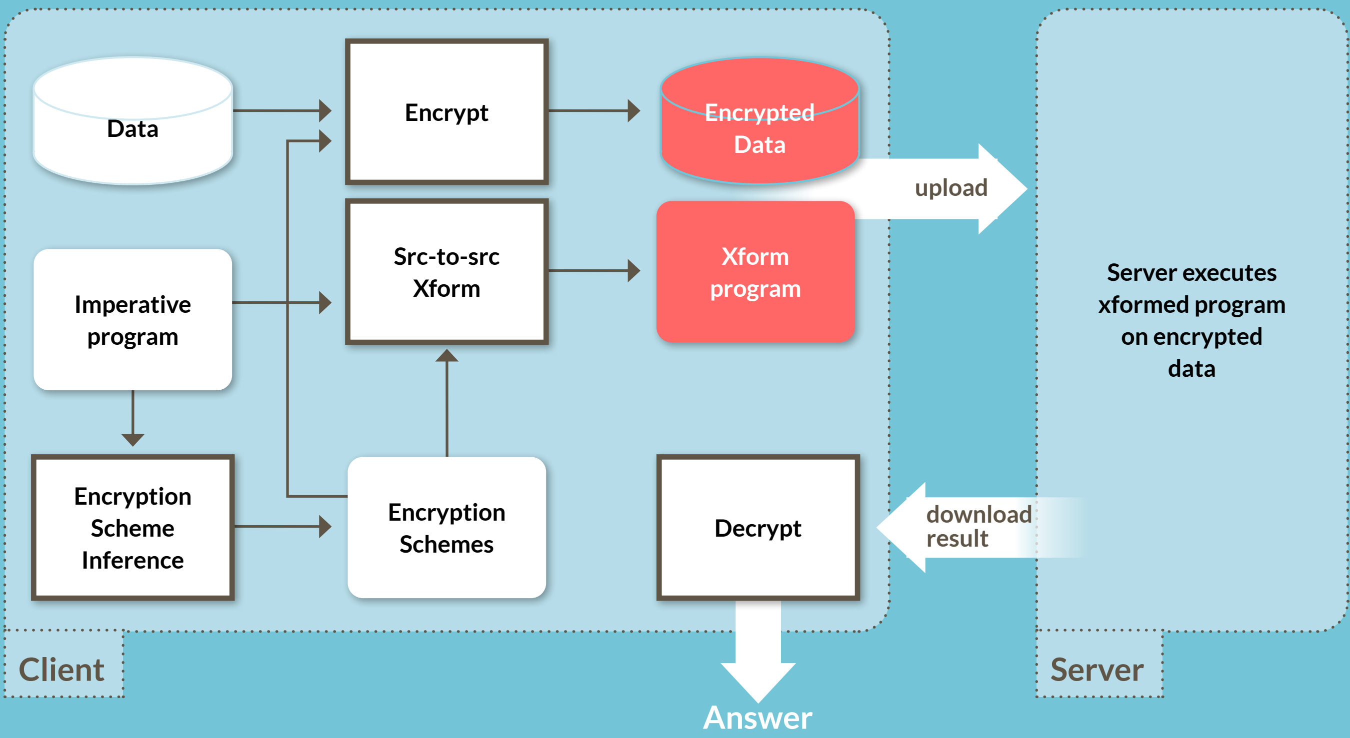
Application: Facilitates secure third-party analysis or cloud-based computations in shared energy datasets.

3.3.1 Cloud-Based Platforms with Data Governance

Modern cloud platforms (e.g., AWS, Azure, Google Cloud) provide robust infrastructure for data sharing while enabling access control, security, and compliance tools, *Figure 3.5* (Marwan et al., 2018).

Application: Centralized platforms for cross-organizational energy data sharing with advanced governance policies.

Figure 3.4. MrCrypt architecture uses homomorphic encryption to ensure data confidentiality by automatically transforming the programs, recreated from (Papisetty, 2017).



3.4 Data Spaces and Trusted Data Intermediaries

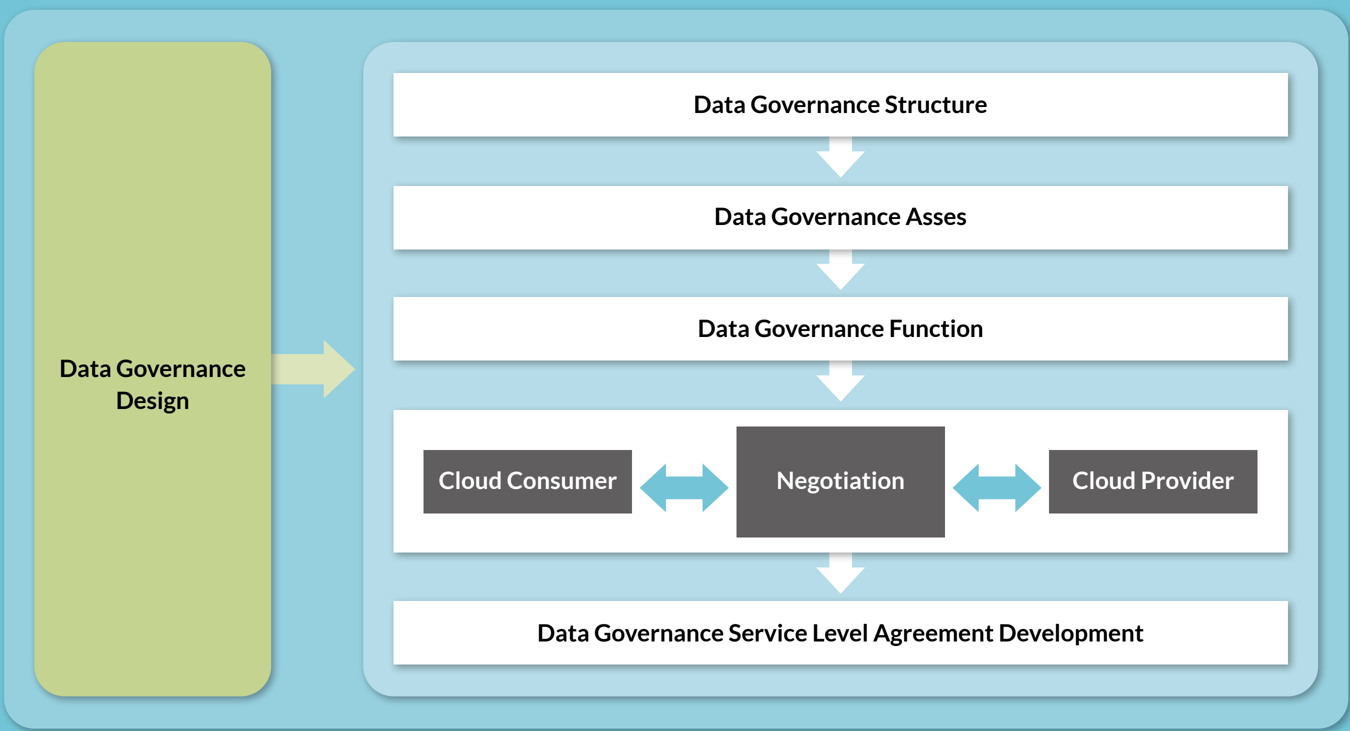
Data spaces (e.g., GAIA-X in Europe) act as decentralized ecosystems where participants share data under agreed-upon rules. Trusted intermediaries facilitate secure and fair data exchanges through advanced cryptographic methods, *Figure 3.6* (Fabianek et al., 2024).

Application: Energy system operators share data for grid management, renewables forecasting, and predictive maintenance.

Recent research explores advanced technologies for secure and privacy-preserving data sharing in energy systems and other sectors. Homomorphic Encryption, Secure Multi-Party Computation (SMPC), Differential Privacy, and Federated Learning are highlighted as promising tools to address privacy challenges in the energy domain (Cali, Umit, Aghaei, Mohammadreza, Moazami, Amin, Lobaccaro, 2024). Blockchain and smart contracts, integrated with Federated Learning, offer opportunities for decentralized Energy Internet services, particularly in energy trading, smart microgrids, and electric vehicle management (Zekiye & Özkasap, 2023). The concept of trustless data intermediaries utilizing SMPC and Fully Homomorphic Encryption (FHE) is proposed for secure data spaces, addressing challenges in identity management, policy enforcement, and access control (Fabianek et al., 2024). These privacy-preserving techniques can enhance trust in data sharing transactions, aligning with EU regulations like the Data Governance Act and GDPR (Dutkiewicz et al., 2022). However, challenges remain in widespread application and performance optimization of these technologies.
These technologies collectively enable secure, efficient, and scalable data sharing while addressing concerns like privacy, cybersecurity, and regulatory compliance.

Federated learning and secure multi-party computation are both privacy-preserving techniques that allow collaborative data analysis without sharing raw data. However, they are different in structure and applications. FL lets multiple parties train a shared machine learning model locally and only exchange model updates to keep the data secure (Xu et al., 2021). That is more suitable for distributed and environments with large databases like energy grids. On the other hand, SMPC allows parties to jointly compute a function by splitting data into encrypted parts and performing secure computation

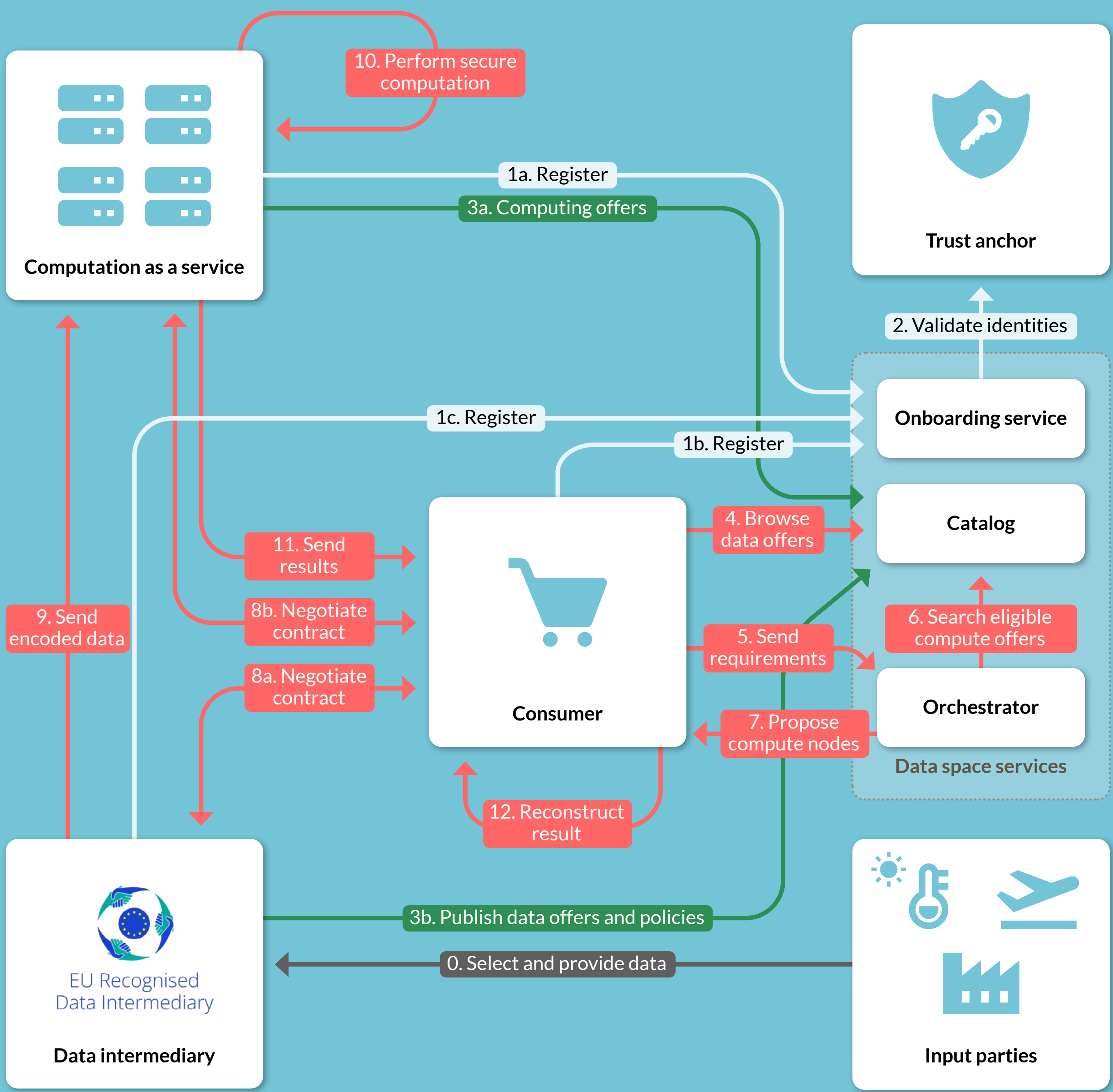
Figure 3.5. Conceptual Framework for Design Data Governance for Cloud Computing Services, recreated from (Al-Ruithe et al., 2016).



and making sure no party sees the raw data from each other (Yao, 1982). That is specifically effective for secure and sensitive analytics where trust is minimal. While FL offers scalability and efficiency for continuous learning and predicting tasks, SMPC provides strong cryptographic guarantees but can be more computationally expensive. Therefore these technologies can be complementary, FL for collaborative model development and SMPC for secure specific computations.

Figure 3.6. Components of a data space-based deployment, recreated from (Fabianek et al., 2024).

Onboarding phase — Setup phase — Transaction phase



4

Data sharing in other sectors

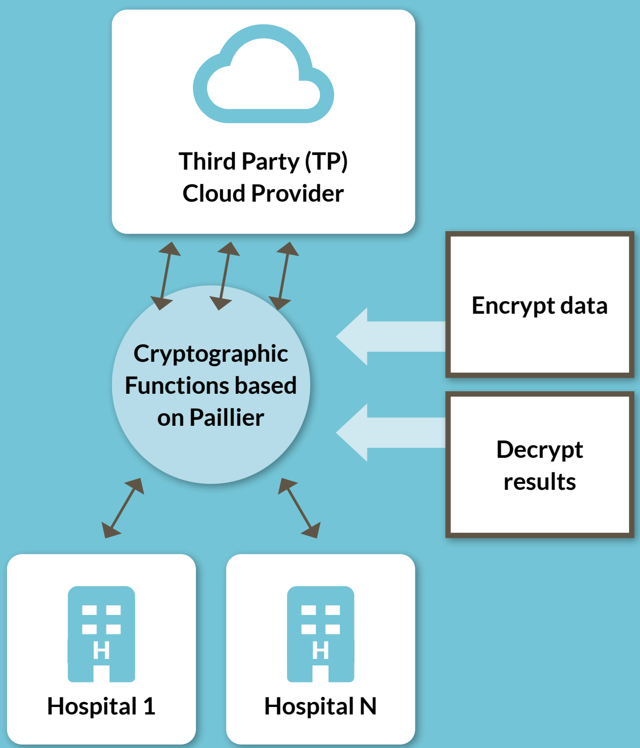
List of examples in which data sharing is applied in different sectors.

4.1 Health

Secure Multi-Party Computation (SMC) is emerging as a promising approach for privacy-preserving data sharing in healthcare. SMC enables collaborative analysis of sensitive medical data without revealing individual inputs, aligning with regulations like HIPAA and GDPR (Md Fahim Ahammed & Md Rasheduzzaman Labu, 2024). It facilitates secure collaboration between healthcare organizations, improving service quality while protecting patient privacy, *Figure 4.1* (Marwan et al., 2016). SMC can be implemented using homomorphic encryption techniques, such as the Paillier scheme, which allows computations on encrypted data (Marwan et al., 2018). This approach enables healthcare institutions to perform analytics on combined datasets without sharing the underlying sensitive information (Veeningen et al., 2018). While SMC shows great potential for transforming healthcare data management and enhancing patient outcomes, challenges remain in areas such as scalability and usability (Md Fahim Ahammed & Md Rasheduzzaman Labu, 2024). Nonetheless, SMC represents a significant step towards balancing the need for data-driven decision-making with stringent privacy requirements in healthcare.

Veeningen et al. (2018) showed how SMC can be used to improve data analytics in hospitals, ensuring compliance with privacy laws like GDPR. Their work focused on using SMC to optimize hospital workflows, reduce costs, and improve the quality of care. Marwan et al. (2018) developed a cloud-based framework that uses SMC and homomorphic encryption, based on the Paillier scheme, to allow secure data sharing

Figure 4.1 The proposed architecture for securing healthcare collaboration. Each hospital starts sending its private data after being successfully encrypted for computations. Then, a third party (TP) as a cloud provider compute encrypted data and sends the result to all parties. Next, each participating hospital decrypts the encrypted data to get the final result using their private key, recreated from (Marwan et al., 2016).



SMC lessons transfer from healthcare to energy for secure data sharing.

between healthcare institutions. This system can perform calculations on encrypted data without needing access to the original information, making it safe to use even in public cloud environments.

Real-world examples also highlight the value of SMC. Van Egmond et al. (2021) (Egmond et al., 2024) used SMC to combine data from a hospital and a health insurance company to train a predictive model that identifies lifestyle factors linked to heart failure. Other studies show SMC's use in genomic data sharing (MIT), secure aggregation in health monitoring systems (Stanford University), and protecting electronic health records with differential privacy (Harvard Medical School). These examples demonstrate how SMC allows organizations to work together securely, providing better insights without risking sensitive information.

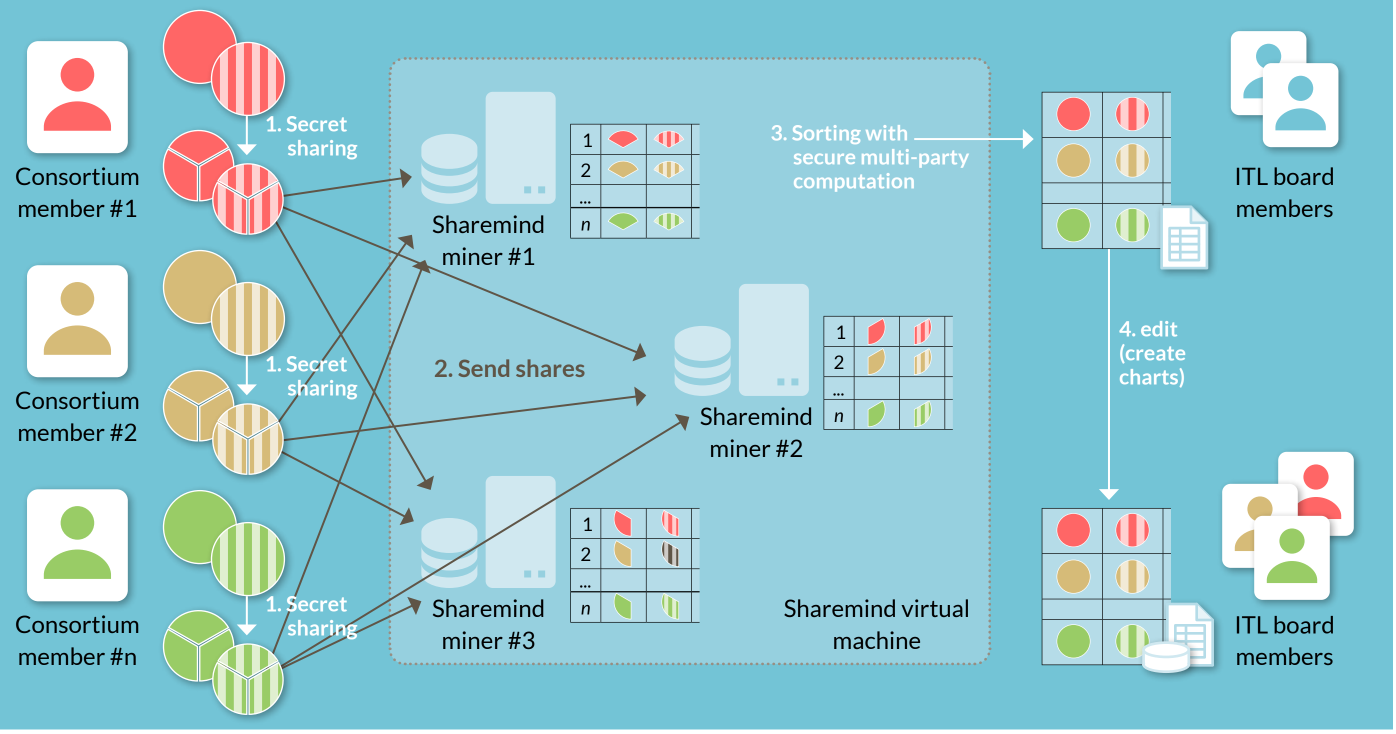
Research by Ahammed and Labu (2024) also highlights how SMC aligns with important privacy laws like HIPAA and GDPR, making it a reliable choice for protecting patient data. While there are still challenges, such as high computational costs and building trust among organizations, SMC offers solutions that make secure collaboration, data sharing, and decision-making possible. By protecting sensitive information and enabling advanced analytics, SMC is shaping the future of privacy in healthcare.

4.2 Finance

Digital collaboration is becoming an important way for industrial clusters to grow sustainability and reduce carbon emission. Industrial clusters are groups of business and institutions located close to each other that work together. By using digital tools like real-time data sharing and digital twins, these clusters can improve how they use energy, cut costs, and innovative. For example, the Net-Zero energy efficiently, saving money and supporting climate goals. Similarly, the Zero Carbon Humber cluster in the UK uses digital twin technology to plan for hydrogen-based energy systems and involve local stakeholders. However, challenges like cybersecurity, data sharing, and building trust between businesses need to be addressed. Initiatives like the World Economic Forum's Transitioning Industrial Clusters framework are helping clusters overcome these challenges and successfully adopt digital technologies (Varoli & Steinbach, 2025).

These papers explore privacy-preserving methods for sharing and analyzing sensitive financial data using secure multi-party computation (MPC) techniques. Abbe et al. (2011) (Abbe

Figure 4.2 Data flow and visibility in the improved solution using the Sharemind framework. Sharemind is a distributed virtual machine that uses secure multi-party computation to securely process data, recreated from (Bogdanov et al., 2012).



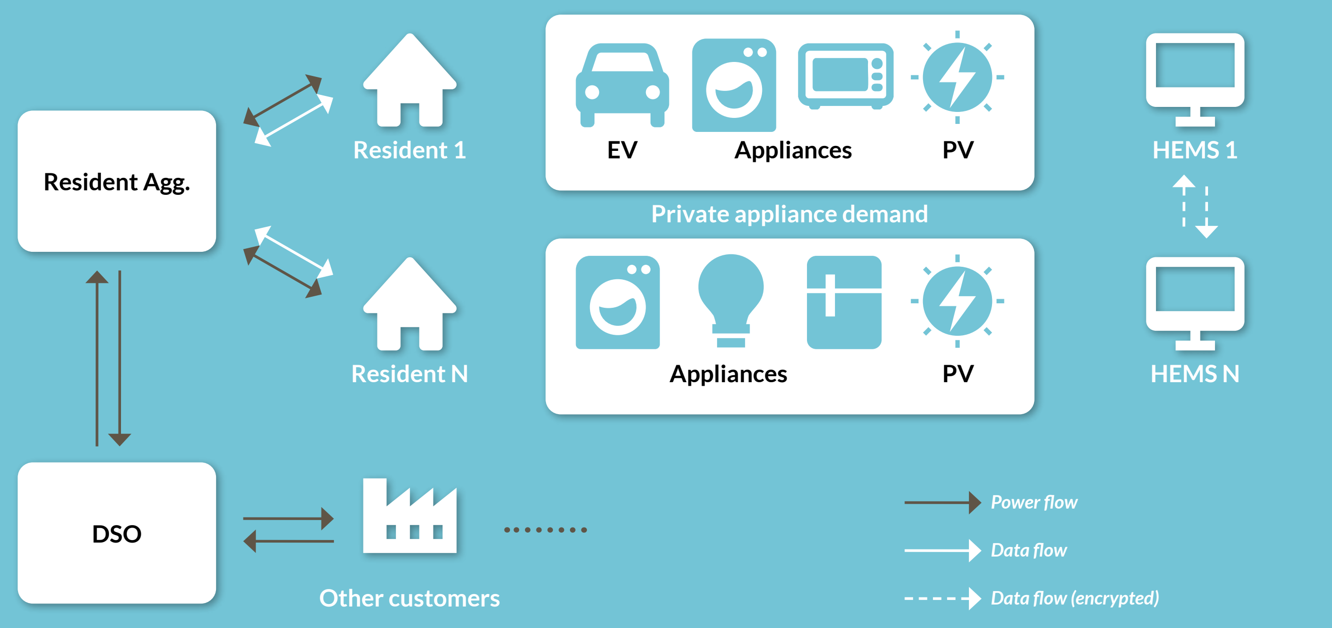
et al., 2012) propose protocols for computing risk exposure statistics without revealing individual inputs, applicable to creating real-time bank indexes and monitoring investments. Bogdanov et al. 2012 (Bogdanov et al., 2012) describe the first implementation of MPC for financial data analysis over the internet with geographically distributed nodes, demonstrating its feasibility and user acceptance. Doğuç (2022) (Doğuç, 2022) presents PPDM protocols for banking applications, focusing on homomorphic cryptosystems and MPC for tasks like clustering and Bayesian networks. These studies highlight the potential of MPC in enabling privacy-preserving data sharing and analysis in the finance sector, addressing concerns about trade secrecy (Abbe et al., 2011) and data privacy. The research indicates that MPC techniques provide sufficient assurance for participants to share sensitive information for collaborative analysis (Bogdanov et al., 2012; Do▯uç, 2022).

Abbe et al. (2011) presented a framework that uses SMC to share and aggregate financial risk exposures while protecting the privacy of all parties involved and eliminating the need for a trusted third party. This approach enables secure calculations of financial statistics, such as concentration indexes and pairwise correlations. Potential applications include privacy-preserving real-time indexes of bank capital and leverage ratios, monitoring delegated portfolio investments, conducting financial audits, and developing proprietary trading strategy indexes.

In the banking sector, privacy-preserving data mining (PPDM) has also been used to perform tasks like clustering and association rule mining securely and efficiently. Doğuç (2022) combined homomorphic encryption and SMC protocols to demonstrate how common data mining techniques can be applied to sensitive banking data while maintaining customer privacy. This builds on foundational work by Yao, who introduced protocols for securely sharing data between parties with differing security concerns. Tools like the Fairplay system, which allows two parties to construct and evaluate Boolean circuits securely, have made practical implementation of these ideas more accessible.

Bogdanov et al. further explored the use of SMC in financial data analysis by deploying Sharemind, a distributed virtual machine based on secret sharing techniques, *Figure 4.2*. Their study was the first to implement SMC on real-world financial data over the internet, with geographically distributed computing nodes. This development highlights the scalability of SMC and its potential for secure data processing in complex financial systems.

Figure 4.3 Secure multi-party household load scheduling framework. During load scheduling, the sensitive appliance load demands are the private data of residents, which can be encrypted and then shared using their home energy management systems (HEMSs). The encryption technology prevents privacy leakage, recreated from (Cheng et al., 2023).



These studies collectively show how SMC can address critical privacy challenges in the finance sector, enabling secure data sharing, analytics, and collaboration. By protecting sensitive financial information, SMC opens new possibilities for innovation in risk assessment, auditing, and data-driven decision-making. However, challenges like computational complexity and integration into existing systems remain, requiring further research and development.

4.3 Energy

Recent research has explored secure multiparty computation (SMPC) and data sharing in the energy sector to address privacy concerns while optimizing energy systems. Cheng et al. (2023) (Cheng et al., 2023) proposed a framework using homomorphic encryption for secure data sharing between home energy management systems, improving demand-side management without compromising user privacy. Similarly, Si et al. (2023) (Si et al., 2023) introduced SMPC to distributed optimization of integrated energy systems, achieving better convergence than differential privacy methods. Li et al. (2023) developed a distributed privacy-preserving data sharing scheme for energy storage using additive secret sharing, demonstrating lower computational costs and improved scalability compared to traditional methods. These approaches enable efficient coordination of distributed energy resources while protecting sensitive information. Pujić et al. (2020) (Pujić et al., 2020) highlighted the suitability of big data technologies in the energy domain, emphasizing the need for modernization in processing, storing, and interpreting vast amounts of data to improve overall energy efficiency.

Cheng et al. (2023) proposed a decentralized framework for real-time demand-side management (DSM) in households, *Figure 4.3*. Their model integrates home energy management systems (HEMS) with homomorphic encryption (HE) to enable secure data sharing while maintaining user privacy. A reinforcement learning method, boosting tree-based deep Q-network, was used to optimize load scheduling. This approach reduced peak loads without increasing electricity costs for users, showing that privacy-preserving frameworks can achieve similar results to traditional methods without compromising sensitive information.

Similarly, Si et al. (2023) applied SMC to distributed optimization in Integrated Energy Systems (IES). By coordinating multiregional energy resources and networks through IoT technologies, IESs improve overall energy efficiency. However, the need for sharing sensitive information, such as energy demand and operational data, raises privacy concerns. To address this, Si et al. introduced a privacy-preserving distributed optimization algorithm combining the Paillier cryptosystem with the Alternating Direction Multiplier Method (ADMM). Their study demonstrated that this method ensured convergence without revealing plaintext data and outperformed differential privacy-based approaches in accuracy and performance.

Pujić et al. (2020) explored the broader challenges of big data in the energy domain, emphasizing the need for secure and efficient data handling to address the increasing complexity of energy systems. Privacy-preserving methods like SMC provide a foundation for tackling these challenges by enabling secure collaboration and optimization across stakeholders.
In addition to computational frameworks, the ecological impact of renewable energy projects, such as wind farms, highlights the importance of data-driven planning. While wind farms contribute to renewable energy goals, they can affect bird populations by altering migration paths and increasing energy expenditure ((Drewitt & Langston, 2006);(Masden et al., 2009)) . Movement models based on bird avoidance behavior inform better planning and mitigation strategies, such as habitat restoration, to reduce these impacts (Masden et al., 2012). These studies collectively illustrate the potential of SMC and privacy-preserving technologies to optimize energy systems, address privacy concerns, and guide environmentally responsible decision-making in the energy sector.

Wind farms, while contributing to renewable energy goals, can negatively impact bird populations through collision, displacement, barrier effects, and habitat loss (Drewitt & Langston, 2006). Studies have shown that birds, particularly migratory species like common eiders, adjust their flight paths to avoid wind farms, resulting in increased energy expenditure (Masden et al., 2009). However, the additional distance travelled due to a single wind farm is relatively minor compared to the total migration distance (Masden et al., 2009). Nonetheless, cumulative effects of multiple wind farms along migration routes could significantly impact bird populations (Masden et al., 2009; (Masden et al., 2010)). To assess and mitigate these impacts, researchers have developed movement models based on observed avoidance behaviors, which can inform wind farm planning and configuration (Masden et al., 2012). Additionally, considering species-specific ecology during the planning process and implementing mitigation measures, such as habitat restoration, may help reduce negative effects on bird populations (Masden, 2010).

5

Potential case studies in the North Sea

This section provides the potential case studies in the North Sea based on literature and expert interviews. The list of case studies are only a fraction of possibilities for data sharing in the North Sea but they mainly illustrate how strategic data sharing can solve critical challenges in the North Sea energy systems.

5.1 Data sharing for logistics: Routine maintenance planning

Maintenance planning in the energy sector involves several stakeholders, including operators, service providers, and logistics companies, each managing various aspects of the process. Operators plan maintenance based on platform schedules and internal priorities, service providers handle the availability of skilled personnel and equipment, logistics companies coordinate vessel schedules and cargo handling. Currently these stakeholders operate independently, and information is only shared as needed without prior planning. For example, vessel trip details and cargo schedules are often communicated just 2-3 days in advance, which leads to inefficiencies like higher operational costs, last minute adjustments, inefficiently used vessels.

However, sharing data between these parties can address these challenges and improve coordination. Operators can provide maintenance schedules scope and frequency to allow service providers and logistics companies to align their plans, in turn, service provides could share data on resource availability such as equipment and skilled staff, while logistics companies could share vessel activity details, trip frequencies and cargo volumes. This collaboration would enable stakeholders to align their operations and optimize maintenance tasks across platforms. This will ensure timely maintenance, and lower costs while improving the reliability of operations.

5.2 Maintenance: Predicting (non-) critical component failures

The prediction of equipment failures, for both critical and non-critical components, is often handled independently by operators, where each maintains its own failure logs and operational records. This lack of shared data creates challenges for logistics companies and other stakeholders. They cannot anticipate maintenance needs and prepare vessels, spare equipment, or personnel in advance, which causes higher costs and resource inefficiencies. If operators share failure data such as frequency of failures for the equipment, aggregated operational data to provide inputs on the history of the equipment and other relevant metrics, it could provide significant benefits to all stakeholders. This data, combined from multiple sources, would help identify patterns and predict maintenance needs more accurately. Logistics companies could use this information to plan vessel schedules, allocate spare equipment and ensure the availability of skilled personnel in advance. Operators would benefit from improved operational stability, as maintenance could be planned proactively for a longer term, reducing the chances of delays or costly downtime.

Furthermore, operators and original equipment manufacturers (OEMs) can collaborate more effectively by using vertical federated learning. This approach allows operators to share data with OEMs to improve the design and operation of the equipment. Federated learning ensures that sensitive data remains decentralized, maintaining privacy while developing more robust predictive models.

5.3 Offshore grid flexibility trading

As the North Sea evolves into a hybrid energy hub, integrating offshore wind, hydrogen production, and cross-border energy interconnectors, grid congestion, and transmission bottlenecks are becoming increasingly problematic. This reduces efficiency and raises costs for energy production and distribution. Transmission system operators (TSOs), energy producers, market operators, and traders often work in silos, leading to inefficiencies in balancing energy flows between different energy sectors. A solution to this problem could lie in the development of data sharing architecture for the entire offshore energy grid and optimizes energy flows across the

system in real-time. By sharing data on generation forecasts, storage capacities, grid congestion levels, and energy market prices, stakeholders could work collaboratively to simulate different energy scenarios and avoid renewable energy curtailment. For example, the system could identify moments of grid congestion and suggest flexible energy trading between electricity producers and hydrogen producers to alleviate bottlenecks. The collaborative and federated digital twin could also allow for the predictive management of energy flows and the optimization of short-term flexibility trading to ensure the grid is always balanced, reducing the need for curtailment and increasing the overall efficiency of offshore energy infrastructure. This would contribute to a more flexible, resilient, and cost-effective offshore energy system, improving integration across renewable energy sources and hydrogen production in the North Sea.

5.4 Infrastructure Optimization

In the evolving offshore energy landscape, repurposing existing oil and gas infrastructures—such as platforms and pipelines—for new applications like hydrogen transport requires informed decision-making. Effective data sharing among key stakeholders enables optimized infrastructure utilization while ensuring safety and compliance. Pipeline operators contribute real-time monitoring data and pipeline configuration insights, while oil and gas operators provide information on platform integrity and operational status. Original Equipment Manufacturers (OEMs) share asset and component details, and regulatory bodies ensure integrity compliance through access to structural and environmental data. By integrating these data streams into a collaborative digital platform, stakeholders can assess feasibility, mitigate risks, and support a smoother transition to hydrogen transport, ultimately extending asset lifespans and enhancing offshore energy sustainability.

5.5 Ecology: Predicting bird migration to optimize offshore wind farm operations

The intersection of offshore wind farms and bird migration highlights the critical need for data sharing among ecologists, wind farm operators, regulatory bodies, and research institutes. Birds migrate across the North Sea, an area where offshore wind farms are rapidly developing. However, without collective data, it is not possible to predict migration patterns accurately and understand the impact of wind turbine operations on birds.

Currently, migration data is scattered and incomplete, collected through bird ringing, local radars, turbine-mounted cameras, and manual ecologists observations. This data is not centralized and bird migration routes are unknown.

Existing data points are limited to two observation locations where birds are ringed and their numbers are recorded when captured elsewhere. Each partner holds different types of data, ecologists have bird ringing data and manual observations, wind farm operators collect data from turbine-mounted cameras (locally monitoring the bird movements) and operational data, regulatory bodies manage local radar data, and research institutes develop prediction models.

Therefore, sharing data improves understanding and predicting bird migration patterns, benefiting all the involved stakeholders. Ecologists can access to real-time movement data from radars and cameras, models so that they can validate their observations and make better conservation strategies. Wind farm operators can use predictive models to adjust turbine operations during peak migration periods and minimizing bird collisions while maintaining energy efficiency. Regulatory bodies benefit from comprehensive datasets that lead to better policy decisions, environmental monitoring. Research institutes can refine their predictive models with more accurate data sources which leads to improved migration forecasting and sustainable wind farm design. Centralizing data from various sources and stakeholders can lead to improved prediction models, operational adjustments to minimize the impact on birds during peak migration periods and optimize wind farm design.

5.6 Marine wildlife protection using offshore infrastructure data

Offshore energy installations such as wind farms and platforms can impact marine biodiversity through factors like noise pollution, habitat disruption, and changes to ocean currents. However, traditional ecological monitoring methods are

limited in scope, as they rely on periodic surveys that miss real-time changes and long-term impacts on ecosystems. By integrating data from offshore wind operators, oil & gas, H2 and CCS platform operators, and marine research institutes, it is possible to create ecosystem monitoring platforms. Data such as underwater noise levels, seabed impact assessments, and marine species migration patterns could be combined with real-time video feeds and environmental sensor readings to detect marine species in real-time. For example, the system could detect and classify species such as whales, dolphins, and fish populations, while also predicting habitat changes based on energy infrastructure operations. The data shared by stakeholders could also enable regulatory agencies to make more informed decisions regarding offshore activities, ensuring that policies and operations minimize negative environmental impacts. Models derived from such a data sharing ecosystem would enable stakeholders to adapt offshore energy operations in real-time to better protect marine life, improve biodiversity outcomes, and meet sustainability targets while allowing for the continued development of offshore energy infrastructure.

5.7 Shipping and fuel traceability

As the shipping industry moves towards low-carbon fuels, particularly hydrogen-based ammonia and methanol, ensuring that these fuels are truly sustainable and meet regulatory standards becomes increasingly critical. However, verifying the origin and carbon footprint of fuels used in shipping has been a challenge, particularly with the international nature of the industry. A blockchain-based fuel traceability system could provide a solution by enabling the sharing of data between stakeholders such as hydrogen and biofuel producers, shipping companies, port authorities, and regulatory bodies. Hydrogen producers could share data about the fuel's carbon intensity and production methods, while shipping companies could provide fuel consumption data and emissions monitoring. Port authorities would contribute refueling logs, and regulatory agencies could supply compliance data. By utilizing blockchain technology, all parties involved would have access to verifiable and immutable records regarding the origin of the fuel, its carbon footprint, and whether it complies with sustainability targets. The real-time tracking of fuel data would allow shipping companies to optimize their routes based on fuel availability and carbon pricing. This would ensure compliance with environmental regulations such as the International Maritime Organization (IMO) standards, helping to accelerate the transition to greener shipping practices.

5.8 License and green certificate

Ensuring transparency and credibility in sustainability claims, e.g. for hydrogen, is crucial. There are several companies and organizations for issuing Guarantees of Origin (GoO) and Certificates of Origin (CoO) for sustainable energy carriers, and the data sharing plays a key role in certifying hydrogen's provenance. Effective data sharing between hydrogen producers, grid operators, energy traders, and regulatory bodies enables accurate tracking of hydrogen's lifecycle—from production to end-use. Producers share real-time production data, while grid operators provide transport and distribution insights. Traders rely on this verified information to facilitate GoO and CoO transactions, ensuring market trust. By integrating these data streams into a secure and interoperable digital platform, stakeholders can enhance the credibility of hydrogen markets, support regulatory compliance, and enable a transparent, tradeable certification system that accelerates the transition to a low-carbon economy.

5.9 Decommissioning optimization

As the North Sea's offshore energy infrastructure, particularly oil and gas platforms, approaches the end of its operational life, decommissioning presents a significant challenge in terms of cost, environmental impact, and waste generation. However, many of these aging platforms, turbines, and other offshore structures have considerable potential for reuse in alternative sectors such as aquaculture, floating solar, or even as artificial reefs. Currently, there is no centralized system for sharing the critical data required to match decommissioned assets with potential reusers. By creating a data sharing platforms, can also be referred to as Decommissioning-as-a-Service (DaaS) platform, data from platform operators, offshore wind developers, and environmental agencies could be shared to facilitate the repurposing of offshore infrastructure. Data such as structural integrity assessments and material compositions would allow companies in the marine construction, aquaculture, and circular economy sectors to evaluate the feasibility of reusing platforms or turbine foundations and equipment for new purposes. Furthermore, environmental agencies could provide data on the ecological impact of repurposing these structures, ensuring that the environmental benefits of reusing offshore infrastructure outweigh the potential risks. This data-sharing initiative would allow stakeholders to lower decommissioning costs, extend the lifespan of offshore assets, and contribute to a circular offshore economy. It could also prevent the wasteful scrapping of platforms and turbines and ensure that these valuable resources are used effectively in new, innovative applications, supporting both economic and environmental goals in the North Sea.

6
Challenges

Several challenges must be addressed to achieve successful data sharing in the North Sea. These challenges include cybersecurity risks, issues regarding data ownership, regulatory and compliance complexities, and stakeholders' willingness to share data. Successfully addressing these issues requires integrating advanced technological solutions, clear and supportive regulatory frameworks, and fostering a culture of trust and collaboration among stakeholders. By effectively managing these challenges, substantial efficiency, sustainability, and innovation can be achieved across the North Sea energy sectors (Md Fahim Ahammed & Md Rasheduzzaman Labu, 2024).

6.1 Cyber security

Data sharing inherently exposes stakeholders to risks associated with cyberattacks, data breaches, and unauthorized access. Sensitive operational data related to energy production, maintenance schedules, and infrastructure performance could become targets for cyberattacks, potentially leading to disruptions, operational losses. Shared platforms, APIs, and networks introduce multiple points of vulnerability, especially if robust encryption and access controls are not in place.

Advanced threats such as ransomware, phishing, and persistent attacks (APT) particularly threaten critical infrastructure (Cheng et al., 2023; Dutkiewicz et al., 2022).

To mitigate these cybersecurity risks, the implementation of secure multi-party computation (SMPC) and robust encryption methods is crucial. Regular security audits and the adoption of secure-by-design digital platforms featuring multi-factor authentication (MFA) and zero-trust architectures are

also necessary strategies to protect sensitive information effectively (Fabianek et al., 2024).

6.2 Ownership

Ownership concerns revolve around determining who "owns" the data generated by collaborative efforts and shared systems. In multi-stakeholder ecosystems like the North Sea energy networks, data often originates from multiple parties, complicating ownership rights.

Determining clear data ownership within collaborative multi-stakeholder environments like the North Sea presents significant challenges. Ambiguity around who owns the data, whether operators, technology providers, or infrastructure managers, often leads to conflicts regarding data usage rights and intellectual property protection. Furthermore, stakeholders may fear losing competitive advantages if valuable operational data is shared openly, raising additional concerns about monetization and strategic disadvantages. Clearly distinguishing between shared and proprietary data is often difficult but essential (Caso, 2020; Varoli & Steinbach, 2025).

Transparent data-sharing agreements explicitly defining ownership, access rights, and usage policies are essential. Technologies such as blockchain and smart contracts can provide transparency and enforce agreed-upon rules effectively, thereby addressing ownership disputes and enhancing trust among stakeholders (Zekiye & Özkasap, 2023).

6.3 Regulatory and compliance

Data sharing in energy systems must comply with a complex landscape of regulations and standards, which vary across regions and jurisdictions. Non-compliance can lead to legal, financial, and reputational risks.

Compliance with various international, regional, and industry-specific regulations complicates data-sharing initiatives. Regulations like the EU's General Data Protection Regulation (GDPR) impose strict requirements on data handling, significantly complicating cross-border and cross-sector data exchanges. Additionally, operational data often includes sensitive information related to critical infrastructure, necessitating compliance with specific cybersecurity laws and sector regulations. Navigating these complex legal requirements adds considerable administrative burdens and legal risks for stakeholders (Dutkiewicz et al., 2022).

Addressing these regulatory challenges involves developing comprehensive governance frameworks aligned with regional and international standards. Using trusted data intermediaries or compliance-focused digital platforms can simplify these processes. Techniques such as data anonymization and federated learning also enable stakeholders to comply with privacy regulations while still sharing valuable insights (Xu et al., 2021).

6.4 Willingness to share data

The success of data-sharing initiatives hinges on stakeholders' willingness to collaborate and share data, which can be hindered by cultural, operational, and business-related concerns. The effectiveness of data-sharing initiatives greatly depends on stakeholders' willingness to collaborate openly. Factors such as lack of trust in data security and usage, competitive concerns about losing business advantages, and entrenched cultural barriers often reduce the motivation to share data. Stakeholders may also perceive that the costs and risks of sharing outweigh potential long-term benefits, further hindering collaborative efforts (Aadland et al., 2019; Varoli & Steinbach, 2025).

To increase willingness among stakeholders, it is critical to establish transparent governance frameworks and demonstrate tangible, immediate benefits such as operational efficiencies, cost savings, and innovation. Encouraging public-private partnerships and leveraging secure data-sharing technologies like federated learning and SMPC can help stakeholders feel confident that sensitive data will remain protected while enabling valuable collaboration and insights (Md Fahim Ahammed & Md Rasheduzzaman Labu, 2024).

Cyber security, ownership, compliance, and willingness to share are key challenges in data sharing.

7
Conclusions and next steps

Transparency in data shared by energy companies is crucial for building and maintaining trust among stakeholders such as investors, regulators, and the general public. By promoting transparency, energy companies can enhance their credibility, ensure regulatory compliance, and support meaningful engagement and informed decision-making among stakeholders. This openness is a fundamental driver for progress and innovation within the North Sea energy sectors.

Facilitating **data sharing** for research and innovation is equally crucial. Making data accessible to researchers and technology developers can significantly speed up the creation of innovative solutions and technologies. These advancements can increase operational efficiency, reduce costs, and minimize environmental impacts, benefiting the entire industry. Collaborative efforts in data sharing can lead to significant breakthroughs that benefit the entire industry.

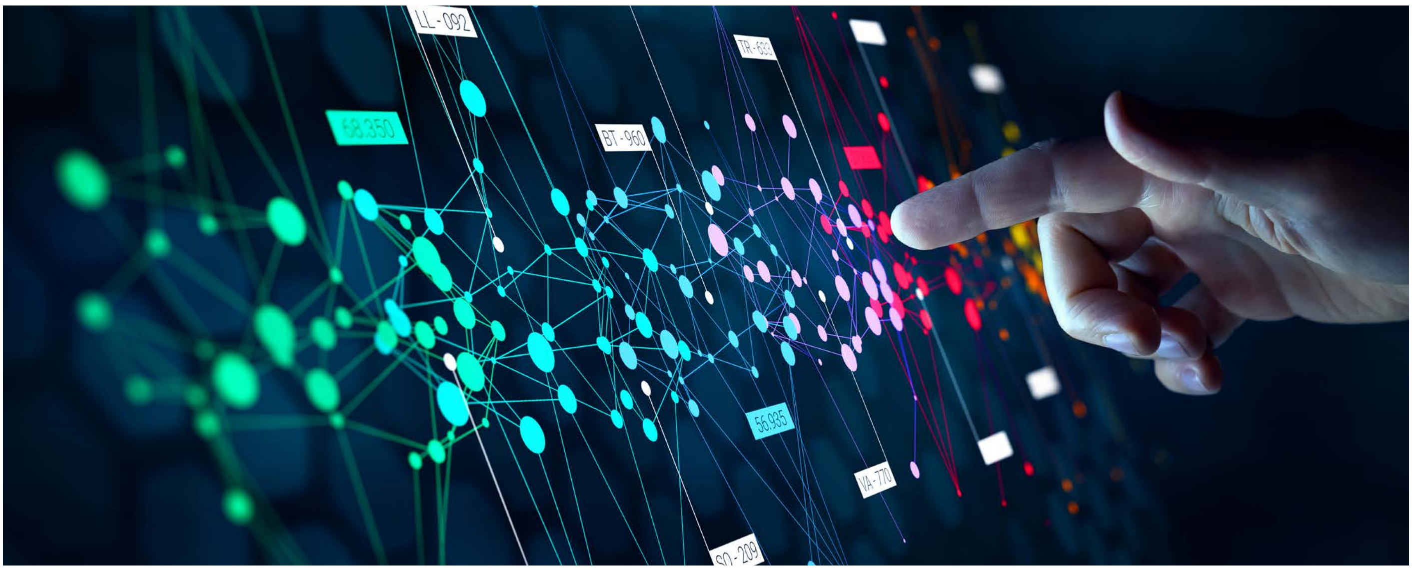
Successful data sharing and innovation rely heavily on the **cooperation of diverse stakeholders** including industry leaders, research institutions, policymakers, and the public. Creating collaborative platforms and forums can play an essential role in addressing the complex challenges facing the North Sea energy sector. Such platforms allow stakeholders to exchange insights, align their objectives, and develop coordinated strategies.

These technologies are already demonstrated in other applications but for the North Sea energy systems, their application is novel. Demonstration and pilot cases in research programs to show the added value and practical requirements of such a data sharing platform is a crucial step. NSE program offers a great opportunity to serve as a **platform** for these collaborative initiatives. Through its established networks and resources, NSE can effectively facilitate transparent data sharing, strengthen stakeholder collaboration, and accelerate innovation. A dedicated initiative such as the NSE Offshore Data Hub (NODE) could serve as a central repository, enhancing the accessibility and usability of shared offshore energy data.

Next steps

To effectively harness the benefits of data sharing in the North Sea the following actions are recommended:

- Enhance data transparency: Develop and implement clear policies and guidelines ensuring data from energy companies is transparent, accessible, and useful for all stakeholders.
- Promote data sharing: Establish formal frameworks, standardized agreements, and secure platforms to enable seamless data sharing specifically for driving research and innovation.
- Pilot projects: demonstrate the added value of data sharing through case studies and pilot projects and to provide insights on technical and regulatory requirements.
- Engage stakeholders: Organize regular forums, workshops, and collaborative events that bring together stakeholders from various sectors to foster trust, collaboration, and shared understanding.
- Develop the NSE Offshore Data Hub: Invest in developing NODE as a dedicated, central repository for offshore energy data, ensuring it supports secure, efficient, and effective data sharing.



References

Aadland, A., Straumsheim, C. F., & Giset, A. (2019). Digital worker: Empowering offshore operators with easily accessible data to improve efficiency and safety. Society of Petroleum Engineers - SPE Offshore Europe Conference and Exhibition 2019, OE 2019. https://doi.org/10.2118/195749-MS

Abbe, E. A., Khandani, A. E., & Lo, A. W. (2012). Privacy-preserving methods for sharing financial risk exposures. American Economic Review, 102(3), 65–70. https://doi.org/10.1257/aer.102.3.65

Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2016). A Conceptual Framework for Designing Data Governance for Cloud Computing. Procedia Computer Science, 94(MobiSPC), 160–167. https://doi.org/10.1016/j.procs.2016.08.025

Bergmann, M., and Primor, O., & and Chrysostomou, A. (2021). Digital Data Sharing for Enhanced Decision-Making. In Maritime Informatics (pp. 155--165). Springer International Publishing. https://doi.org/10.1007/978-3-030-50892-0_10

Bogdanov, D., Talviste, R., & Willemson, J. (2012). LNCS 7397 - Deploying Secure Multi-Party Computation for Financial Data Analysis. http://www.cra.org/statistics

Cali, Umit, Aghaei, Mohammadreza, Moazami, Amin, Lobaccaro, G. (2024). Digital Twin Technology for the Energy Sector. Elsevier.

Caso, C. (2020). Gaining a Competitive Edge by Digitalizing Subsurface Operations. J Pet Technol, 72(40–41). https://doi.org/https://doi.org/10.2118/0820-0040-JPT

Cheng, L., Zang, H., Wei, Z., & Sun, G. (2023). Secure Multi-Party Household Load Scheduling Framework for Real-Time Demand-Side Management. IEEE Transactions on Sustainable Energy, 14(1), 602–612. https://doi.org/10.1109/TSTE.2022.3221081

Directorate-General for Energy. (2024). Digitalisation and data exchange are key enablers for a modern and resilient energy system.

Doğuç, Ö. (2022). Data Mining Applications in Banking Sector While Preserving Customer Privacy. Emerging Science Journal, 6(6), 1444–1454. https://doi.org/10.28991/ESJ-2022-06-06-014

Drewitt, A. L., & Langston, R. H. W. (2006). Assessing the impacts of wind farms on birds. Ibis, 148(SUPPL. 1), 29–42. https://doi.org/10.1111/j.1474-919X.2006.00516.x

Dutkiewicz, L., Miadzvetskaya, Y., Ofe, H., Barnett, A., Helminger, L., Lindstaedt, S., & Trügler, A. (2022). Privacy-Preserving Techniques for Trustworthy Data Sharing: Opportunities and Challenges for Future Research. Data Spaces, 319–335. https://doi.org/10.1007/978-3-030-98636-0_15

Egmond, M. B. Van, Dunning, V., Berg, S. Van Den, Sangers, A., Poppe, T., & Veldsink, J. (2024). Privacy-preserving Anti-Money Laundering using Secure Multi-Party Computation. Cryptology EPrint Archive, 1–19.

Elichev, V., & Muñoz, E. (2018). Case study of digital oilfield implementation in the southern North Sea. Society of Petroleum Engineers - SPE Russian Petroleum Technology Conference 2018, RPTC 2018, October, 15–17. https://doi.org/10.2118/191596-18rptc-ms

Fabianek, C., Krenn, S., Loruenser, T., & Siska, V. (2024). Secure Computation and Trustless Data Intermediaries in Data Spaces. October. https://doi.org/10.48550/arXiv.2410.16442

Laborie, F., Røed, O. C., Engdahl, G., & Camp, A. (2019). Extracting value from data using an industrial data platform to provide a foundational digital twin. Proceedings of the Annual Offshore Technology Conference, 2019-May. https://doi.org/10.4043/29576-ms

Lind, M., and Ward, R., and Jensen, H. H., and Chua, C. P., and Simha, A., and Karlsson, J., and Gothberg, L., and Penttinen, T., & and Theodosiou, D. P. (2021). The Future of Shipping: Collaboration Through Digital Data Sharing. In Maritime Informatics (pp. 137--149). Springer International Publishing. https://doi.org/10.1007/978-3-030-50892-0_9

Marwan, M., Kartit, A., & Ouahmane, H. (2016). Applying secure multi-party computation to improve collaboration in healthcare cloud. Proceedings - 2016 3rd International Conference on Systems of Collaboration, SysCo 2016, 1–6. https://doi.org/10.1109/SYSCO.2016.7831325

Marwan, M., Kartit, A., & Ouahmane, H. (2018). A cloud based solution for collaborative and secure sharing of medical data. International Journal of Enterprise Information Systems, 14(3), 128–145. https://doi.org/10.4018/IJEIS.2018070107

Masden, E. A., Haydon, D. T., Fox, A. D., & Furness, R. W. (2010). Barriers to movement: Modelling energetic costs of avoiding marine wind farms amongst breeding seabirds. Marine Pollution Bulletin, 60(7), 1085–1091. https://doi.org/10.1016/j.marpolbul.2010.01.016

Masden, E. A., Haydon, D. T., Fox, A. D., Furness, R. W., Bullman, R., & Desholm, M. (2009). Barriers to movement: Impacts of wind farms on migrating birds. ICES Journal of Marine Science, 66(4), 746–753. https://doi.org/10.1093/icesjms/fsp031

Masden, E. A., Reeve, R., Desholm, M., Fox, A. D., Furness, R. W., & Haydon, D. T. (2012). Assessing the impact of marine wind farms on birds through movement modelling. Journal of the Royal Society Interface, 9(74), 2120–2130. https://doi.org/10.1098/rsif.2012.0121

Md Fahim Ahammed, & Md Rasheduzzaman Labu. (2024). Privacy-Preserving Data Sharing in Healthcare: Advances in Secure Multiparty Computation. Journal of Medical and Health Studies, 5(2), 37–47. https://doi.org/10.32996/jmhs.2024.5.2.4

Nadian-ghomsheh, A. (2021). A hierarchical privacy-preserving IoT architecture for vision-based hand rehabilitation assessment Content courtesy of Springer Nature , terms of use apply . Rights reserved . Content courtesy of Springer Nature , terms of use apply . Rights reserved . 31357–31380.

Open Energy Platform. (2025). Open Energy Platform. https://openenergyplatform.org/

Papisetty, S. D. (2017). Homomorphic Encryption: Working and Analytical Assessment : DGHV, HElib, Paillier, FHEW and HE in cloud security. February. www.bth.se

Pujić, D., Jelić, M., Tomašević, N., & Batić, M. (2020). Case study from the energy domain. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 12072 LNCS (pp. 165–180). Springer. https://doi.org/10.1007/978-3-030-53199-7_10

Si, F., Zhang, N., Wang, Y., Kong, P. Y., & Qiao, W. (2023). Distributed Optimization for Integrated Energy Systems With Secure Multiparty Computation. IEEE Internet of Things Journal, 10(9), 7655–7666. https://doi.org/10.1109/JIOT.2022.3209017

The energy data space. (2025). The energy data space. https://enershare.eu/

Varoli, I., & Steinbach, P. (2025). Digital Collaboration Is Transforming Industrial Clusters. https://www.weforum.org/stories/2025/01/digital-collaboration-industrial-clusters/

Veeningen, M., Chatterjea, S., Horváth, A. Z., Spindler, G., Boersma, E., Van Der Spek, P., Van Der GaliËn, O., Gutteling, J., Kraaij, W., & Veugen, T. (2018). Enabling analytics on sensitive medical data with secure multi-party computation. Studies in Health Technology and Informatics, 247, 76–80. https://doi.org/10.3233/978-1-61499-852-5-76

Xu, J., Glicksberg, B. S., Su, C., Walker, P., Bian, J., & Wang, F. (2021). Federated Learning for Healthcare Informatics. Journal of Healthcare Informatics Research, 5(1), 1–19. https://doi.org/10.1007/s41666-020-00082-4

Yao, A. C. (1982). Protocols for Secure Computations. Annual Symposium on Foundations of Computer Science - Proceedings, 160–164. https://doi.org/10.1109/sfcs.1982.38

Zekiye, A., & Özkasap, Ö. (2023). Blockchain-based Federated Learning for Decentralized Energy Management Systems. 2023 5th International Conference on Blockchain Computing and Applications, BCCA 2023, 186–193. https://doi.org/10.1109/BCCA58897.2023.10338852

North Sea Energy
offshore system integration

North Sea Energy

offshore system integration