LUT University

Recommendation on Cybersecurity and Safety in the Hydrogen Economy

Alfasfos Rami, Ullah Mehar, Sillman Jani, Juliano Nardelli Pedro, Soukka Risto

This is a Author's accepted manuscript (AAM) version of a publication

published by IEEE

in 2024 47th MIPRO ICT and Electronics Convention (MIPRO)

DOI: 10.1109/mipro60963.2024.10569632

Copyright of the original publication:

© 2024 IEEE

Please cite the publication as follows:

Alfasfos, R., Ullah, M., Sillman, J., Nardelli, P., & Soukka, R. (2024). Recommendation on Cybersecurity and Safety in the Hydrogen Economy. 2024 47th MIPRO ICT and Electronics Convention (MIPRO), Opatija, Croatia, 2024, pp. 1837-1842. IEEE. https://doi.org/10.1109/mipro60963.2024.10569632

© 2024 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

This is a parallel published version of an original publication. This version can differ from the original published article.

Recommendation on Cybersecurity and Safety in the Hydrogen Economy

Rami Alfasfos*, Mehar Ullah*, Jani Sillman*, Pedro Nardelli*, Risto Soukka*
* LUT University, Lappeenranta, Finland
Rami.Alfasfos@lut.fi

***Abstract*—This study examines the cybersecurity implications of the hydrogen economy, analyzing cyber incidents since 2010. It suggests a cybersecurity framework based on Internet of Things (IoT) and Edge computing to enhance infrastructure resilience against evolving threats. The digital transformation of energy systems, including smart grids and meters, has provided efficiency and clean energy benefits but also heightened cybersecurity risks. The research aims to bridge the cybersecurity gap in the hydrogen economy while acknowledging historical safety concerns related to hydrogen handling. Cyberattacks in the energy sector since 2010 have seen a significant upsurge, particularly peaking between 2020 and 2022. The study categorizes common cybersecurity threats, motivations, types, and consequences, and proposes an IoT model and edge computing framework to enhance cybersecurity defenses. This interdisciplinary approach integrates cybersecurity, IoT, Edge computing, and hydrogen technologies to address pressing challenges. Drawing insights from past incidents, this research equips stakeholders to secure the future of the hydrogen economy, emphasizing the dual role of IoT systems in increasing cyber threats and fortifying cybersecurity in this expanding energy sector.**

Keywords— Hydrogen, Cyber security, big data, edge computing, Internet of Things

I. Introduction

Decarbonizing energy systems and striving for zero net emissions have made Power-to-X (PtX) technologies and the hydrogen economy central to global energy strategies. These technologies offer a promising path to a sustainable future, but their success hinges on securing hydrogen infrastructure.

This article explores the intersection of decarbonization, cybersecurity, and the vital role of hydrogen in the green energy transition. Hydrogen underpins PtX and is essential for converting renewable energy into versatile hydrogen-based products. Ensuring the security of the extensive hydrogen infrastructure is crucial as the demand for hydrogen is growing.

The vast hydrogen infrastructure, including wind farms, transmission lines, energy storage facilities, and distribution systems, underscores the urgency of ensuring its safety and security The power-to-X energy transformation, which encompasses hydrogen, brings with it a unique set of risks and challenges, particularly concerning cybersecurity and data protection. The hydrogen value chain often involves a multitude of stakeholders, with each component operated by different entities. This multifaceted network necessitates digitalization through the incorporation of IoT and ICT systems to harness their potential benefits. Each component generates a continuous stream of data, which must be shared, accessed, and stored. Deciding on the most secure approach for managing this sensitive data presents a complex challenge, with each option carrying distinct advantages and disadvantages. While the number of cyberattacks on hydrogen facilities remains limited or close to zero, the threats and attacks on other energy systems have proliferated. Consequently, gleaning insights from past incidents in energy systems could be invaluable for the rapidly expanding hydrogen industry. These insights can help build resilient and robust cybersecurity measures

In the last decade, the energy sector has witnessed a surge in cyber threats, some of which have resulted in severe consequences. Prominent cybersecurity breaches within the energy industry have prompted governments, businesses, and industry leaders to prioritize cybersecurity measures. This alarming trend is reinforced by the World Economic Forum's Global Risk Report of 2020, which identifies cyberattacks as one of the ten most significant global risks, both in terms of probability and potential impact [1].

The digitalization of energy systems and the Industrial Revolution 4.0 are two interconnected trends that are transforming the way energy is generated, distributed, and managed. The digitalization of energy systems is a key enabler of Industry 4.0, as energy is a fundamental input in industrial processes. Digitalization allows industries to monitor and manage their energy consumption more efficiently, aligning with Industry 4.0's focus on automation and efficiency. In that case, Internet of Things (IoT), edge computing, and big data is playing a major role. IoT is used to collect the data in a secure way using sensors and other devices, edge computing is facilitating the fast and safe collection and transferring the data to the database (internally and to the cloud). Big data is used to store the huge amount of data and transform that data into useful information, that is used for the current and future business decisions [2]. The integration of digital technologies in energy systems facilitates more responsive and flexible energy production and distribution, supporting the demands of modern industries. Together, digitalization of energy systems and Industry 4.0 contribute to a more sustainable and energy-efficient industrial landscape, reducing environmental impacts and promoting economic growth.

The target of this study is to enhance safety measures and provide guidance to stakeholders for preventing and

mitigating future incidents by analyzing major cyber incidents on the energy systems in the last few years. Moreover, the study proposes an Internet of Things (IoT) model and an edge computing framework to fortify cybersecurity defenses. By leveraging these technologies, the hydrogen infrastructure can become more resilient against evolving cyber threats, fostering confidence among stakeholders, and supporting the transition to sustainable energy systems [3].

This article's target audience includes policymakers, energy industry professionals, cybersecurity experts, researchers, and stakeholders in the hydrogen economy. The study's interdisciplinary approach amalgamates cybersecurity, IoT, edge computing, and hydrogen technologies to address pressing challenges in these fields.

In addition to its practical applications, this research contributes to the academic understanding of cybersecurity within energy systems, offering recommendations to establish a roadmap for strengthening cybersecurity and safety in the burgeoning hydrogen economy. By learning from the past, adapting to the present, and preparing for the future, we aim to ensure a safe and secure transition to hydrogen-based energy solutions.

The rest of this paper is organized as follows. In Section II, we describe related studies on cyber security, IoT, edge computing, and digitalization of energy systems and industrial revolution 4.0. In Section III, we explain the cyberattacks in energy sector from 2010 onwards. In section IV contains the information about the 44 major cyberattacks in energy sector. In section V we provide theoretical architecture that contain IoT, edge computing, big data, and machine learning for the safely hydrogen value chain and Finally, Section VI concludes the paper with slight recommendation for future studies.

II. Related Research

In this section, we use systematic literature review structure, similar to [4], to answer the question "what type of technologies can be used to handle the massive amount of data from SG and obtain meaningful information from it, so that it can be used for better business decisions?" The main objectives are to identify technologies that can work together to effectively extract information from big data to fulfil the requirements of SG business and operations.

A. Cybersecurity

Cyber security refers to the practice of protecting computer systems, networks, software, and data from various forms of digital threats and attacks. It encompasses a wide range of measures and strategies aimed at safeguarding information technology (IT) assets against unauthorized access, data breaches, damage, or theft. Cybersecurity is crucial in today's interconnected digital world, where businesses, governments, organizations, and individuals rely on technology for a wide range of activities. Effective cybersecurity practices help safeguard sensitive data, maintain the privacy of individuals, and protect critical infrastructure from cyber threats, including cyberattacks, hacking, data breaches, and other forms of digital attacks.

1) Cybersecurity in the energy sector: Cybersecurity within the energy sector encompasses a myriad of tools, policies, and technologies designed to safeguard digital assets and organizations. It involves a comprehensive set of risk management strategies, proactive measures, ongoing training, adherence to industry standards, and the integration of cutting-edge technologies. The ultimate objective is to guarantee the security, integrity, and confidentiality of sensitive information and critical resources, thereby protecting them against a wide array of cyber threats [5]. Cyberattacks on energy systems have emerged as a substantial and escalating threat since 2010, with a noticeable increase in the number and severity of attacks targeting this sector [6].

There has been a growing concern about energy infrastructure cybersecurity, a competent workforce, government-private sector collaboration, and resilient information sharing are required. There are recommendations to protect important energy infrastructure in cyberspace [7]. Adding to that despite that fact the global database reveals a significant recent increase in incidents, particularly in the electricity sector. There is still a gap in measuring and tracking cybersecurity risks and impacts pose challenges due to insufficient public data, unreported incidents, undetected attacks, and varying definitions of incidents and attacks [8]. Cyberattacks on energy facilities can result in catastrophic damage, with far-reaching consequences. These attacks have the potential to plunge entire cities into darkness during the coldest months, cause hardware damage to critical infrastructure, and disrupt energy production on a massive scale. To give an example a study estimated that a six-hour winter black-out in France could potentially result in damages totaling over €1.5 billion ($.1.7 billion) [9]. While the cyber threat is palpable, the integration of cybersecurity measures into energy systems remains inadequate. Many organizations are endeavoring to establish policies and frameworks that mandate cybersecurity as a core consideration in energy transition planning. However, these efforts remain a work in progress.

There have been numerous studies and articles on learning from cyber security accidents, however the adaptation of the outcome of these studies has been limited. Though these studies in general provide guidance and recommendations for companies and organizations to prevent or mitigate cyber threats Cyberattacks use these listed methods in their attacks. This is due to different factors, one of which is the no evaluation of whether the actions taken reduce future security incidents in addition the studies recommendations might be not in the right level to the real threats of cyber-attacks [10].

Moreover, this threat has led to different cybersecurity strategies and programs include the European Program for Critical Infrastructure Protection (EPCIP, 2006), the Cybersecurity Strategy of the European Union (2013), and the European Agenda on Security (2015). These initia-

tives emphasize cooperation, information sharing, and the establishment of a common approach to address cyber threats, with specific proposals for EU-wide cybersecurity agencies and certification schemes. [11].

B. Internet of Things

The term "Internet of Things", or "IoT", was introduced by the British technology entrepreneur Kevin Ashton in 1999 as the title of a presentation at Procter and Gamble. IoT and can be defined as small and complex systems that allow businesses, governments, and citizens to adopt and interconnect physical objects and virtual objects based on existing and evolving interoperable information and communication technologies [12]. IoT is a new technology paradigm that has emerged as a global network of machines and devices capable of interacting with each other and with the platform for collecting, analyzing, storing and visualizing data generated from the devices and machines using sensors, actuators, communications, and analytical tools. [13].

C. Edge computing

Edge computing refers to the enabling technologies that allow computations to be performed at the edge of the network; from the cloud viewpoint, edge data is downstream data, and from the IoT services viewpoint, it is upstream data. In such a scenario, edge can be defined as any computing and networking resource that is between the data source and cloud. Smart phone is a simple example of an edge device, because it lies between the human user and the cloud. The aim of edge computing is to ensure that computations are performed at the proximity of data sources [14], [15].

The nodes at the network edge are performing many tasks such as data processing, caching, device management, and privacy protection to reduce the traffic from the devices to the cloud. In order to perform all these tasks in the network, the edge should be well designed to effectively meet the security, reliability and privacy protection requirements [16].

D. Digitalization of energy systems and Industrial revolution 4.0

The digitalization of energy systems has ushered in a new era with numerous advantages, including the ability to connect an array of devices and energy sources. This digital transformation offers the potential for enhanced energy efficiency, streamlined operation and control, reduced operational costs, and accelerated adoption of clean energy solutions [17]. The integration of Information Communication Technologies (ICT) dates to the era of the Cold War and the invention of the internet. It has evolved further with the advent of the Internet of Things (IoT), a network of interconnected devices that has been extensively deployed within diverse energy infrastructures.

ICT and IoT technologies offer unprecedented benefits, including seamless connections between various networks, facilitated data access and storage in the cloud, simplified device control, and the potential for automation and enhanced security through data collection, analysis, and informed decision-making [18]. However, with these benefits come significant risks. Highly digitalized and automated systems are inherently more susceptible to cyberattacks [17]. The increasing utilization of smart systems such as smart grids and smart meters, particularly in developed nations like Finland and Sweden, renders electricity systems more vulnerable to cyber threats [19].

III. Methods and Materials

To address challenges at hand, this study explores methodologies and materials used to offer cybersecurity and safety recommendations within the hydrogen economy. The primary focus is on cyber incidents in the energy sector from 2010 onward, with an emphasis on hydrogen infrastructure-related events. Categorizing common cybersecurity threats in both energy and hydrogen industries involves an in-depth analysis of their origins, characteristics, and repercussions. The investigation examines motives behind these threats, types of attacks, and their impacts. Incident motives are categorized based on original sources or assumed by the author. The study scrutinizes geographical attack sources and attacker motives, enriched with references from online news and published reports.

To achieve this, specialized online databases were meticulously reviewed for major cyber-attacks and energy system cyberattacks. The study evaluates cyber incidents disclosed by targeted facilities. It identifies 44 significant cyber-attacks since 2010, rigorously analyzed and categorized. References from the CSIS Significant Cyber Incidents database support the findings [20].

The research extensively reviews literature and organizational materials to establish a resilient cybersecurity framework. Analysis of these 44 cyber-attacks yields comprehensive graphical representations, tables, and figures, outlining attack nature and evolving trends since 2010.

Furthermore, this study has developed an illustrative model of the green hydrogen production value chain. This model delineates the various stages and processes involved in hydrogen production, while simultaneously addressing the incorporation of IoT (Internet of Things) and edge computing systems. The model extends to elucidate how IoT, and edge computing systems are employed for data collection from each component of the hydrogen production value chain and where this data is stored. The model also outlines the interconnections among the data collected from each component. Moreover, it examines the flexibility afforded to stakeholders of each component in deciding which data should be stored locally and which should be transmitted to the cloud system. The study discusses how edge computing systems facilitate these data storage and sharing mechanisms, ultimately proposing a solution for enhancing the efficiency and security of cyber systems within the hydrogen production value chain.

IV. Results and Discussion

The year 2010 marked a pivotal moment in the threat landscape of cyberattacks against the energy sector. It served as a stark warning of the potential consequences

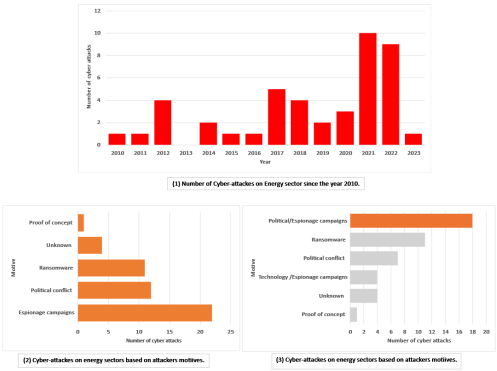

Fig. 1. Analysis of 44 major cyberattacks on energy sector since the year 2010, numbers and motives.

such attacks could have on the industry, emphasizing the urgent need for proactive measures to ensure a secure transition. During this year, cybercriminals demonstrated their capability not only to access or conceal sensitive data but also to inflict physical damage on energy facilities. An example of this was the deployment of the Stuxnet worm in a cyberattack on a nuclear facility in Iran, representing a significant milestone in such attacks. While the full extent of the consequences remains undisclosed, reports indicated that it resulted in the destruction of numerous centrifuges at Iran's Natanz uranium enrichment facility. Despite the assumed political motives behind the attack, it left a profound impact on energy sector security concerns. Subsequently, extensive efforts have been initiated to establish more resilient cybersecurity systems to safeguard the future of the energy sector's transition. Table 1 illustrates selected major cyberattacks examples from the analyzed 44 events on the energy. The examples illustrate the sever of consequences of these attacks. The table also shares the known technologies that were used for these attacks and what energy sector they have also targeted the announced motives behind these attacks.

The analysis of these 44 occurrences, like other reports, led to a consistent result, emphasizing a large growth in cyberattacks, with the peak happening in 2021 and 2022, as shown in Figure 1. This same statistic demonstrated that the predominant motivation for these examined attacks was political and espionage efforts. However, various other motivations were revealed, such as ransomware assaults, technology and espionage efforts, and proof of concept. In certain cases, the motivation for specific attacks was unknown or not disclosed to the public. These findings highlight the frightening potential of cyberattacks as lethal weapons in political confrontations and wars.

The analysis of these 44 occurrences, like other reports, led to a consistent result, emphasizing a large growth in cyberattacks, with the peak happening in 2021 and 2022, as shown in Figure 1. This same statistic demonstrated that the predominant motivation for these examined attacks was political and espionage efforts. However, various other motivations were revealed, such as ransomware assaults, technology and espionage efforts, and proof of concept. In certain cases, the motivation for specific attacks was

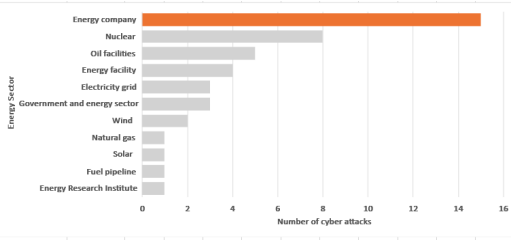

Fig. 2. Cyberattacks by energy sectors since the year 2010.

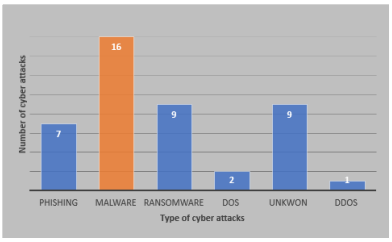

Fig. 3. Types of cyber attacks

unknown or not disclosed to the public. These findings highlight the frightening potential of cyberattacks as lethal weapons in political confrontations and wars.

The studies indicate that major energy companies, particularly in the electricity and oil sectors, have been the primary targets of cyberattacks, as shown in Figure 2. Examples include the significant attack on Aramco, one of the world's largest oil companies, which resulted in the wiping out of tens of thousands of data in their computers. Nuclear facilities have also been subjected to attacks, often associated with political conflicts or technology espionage. Notably, there has been a substantial increase in attacks on the electricity grid and wind energy systems, with the potential to cause severe economic damage, widespread fear, and impact the lives of many. For instance, the 2015 attack in Ukraine, which used the BlackEnergy Malware, resulted in a power outage affecting over 220,000 people in the capital area, underscoring the perilous implications of cyberattacks on people's well-being in the energy sector, especially during critical times like winter.

Various technologies were employed in the attacks analyzed, and their choice often relates to the attack type and motive. Additionally, the targeted energy sector facilities and their cybersecurity systems influence the selection of these technologies. As depicted in Figure 3, Malware emerged as the most used technology in cyberattacks, with ransomware, typically associated with ransom attacks, following closely. It's noteworthy that an equal number of ransom attacks were linked to "known" technologies, which could be attributed to limited reporting, new technologies, or company policies.

V. The Role of IoT and Edge Computing in Hydrogen Value Chain

In this context, the Internet of Things (IoT) is enabling companies to make more informed decisions and operate more efficiently by providing a data network of physical objects that are connected to one another through dedicated applications. The industrial IoT has emerged

TABLE I
LIST OF RECENT CYBER ATTACKS

Year	Location	Energy sector	Cyber attacked technology	Motive	Consequences
2010	Iran	Nuclear	Stuxnet worm	Political conflict	Destroyed numerous centrifuges in Iran's Natanz uranium enrichment facility
2012	Saudia Arabia	Oil field	Shamoom malware	Political conflict	Wiping out the hard drives of tens of thousands of computers
2015	Ukrain	Electricity grid	Black energy malware	Political conflict	Cut lights to 225,000 people
2017	USA	Wind turbines	Malware	proof of concept	Affected every networked turbine in the field
2021	Poland	Govt. energy sector	Unknown	Political conflict	Spread false information about a non-extent radioactive threat
2021	Norway	Energy company	Ryuk ransomware	Ransomware attack	Shutdown water and its treatment facilities in 200 municipalities, affecting about 85% of the Norwegian population.
2022	USA	Fuel pipline	Darkside malware	Ransomware attack	About 4.4 million dollars ransom payment it had to shut down 90 % of its internal control. Wiped 25 years of colonial pipeline historical data.
2022	Ukrain	Wind Turbines	AcidRain wiper malware	Political conflict	Tens of thousands of modems dropped off the network. Collateral damage from this attack also deactivated the remote monitoring or control of 5800 Enercon wind turbines in Germany.

as a key component of Industry 4.0, as it enables the collection of vast amounts of industrial data that can be used to optimize processes and improve decision-making. Data platforms have been developed to build and run different IoT applications, i.e., to process the huge amount of data generated by the IoT devices that are as diverse as the different industrial sectors. Handling such a massive amount of data is a challenge, leading to an approach usually called big data [2].

To spur growth in businesses, effective business decisions are very important, and they are often made possible by getting information from collected data. IoT is a major source of data; by some estimates, there are currently more than ten billion devices connected to IoT networks, generating around trillions GB of data. These devices gather, analyze, share, and transmit data in real time. To handle such massive amounts of data, IoT needs edge computing and big data, making them the key to improve decision making [21].

In this work, we have designed an architecture for getting Hydrogen (H2) production data using IoT and edge nodes as shown in Figure. The life-cycle of hydrogen production data starting from data generation to data analytics. The data is generated from numerous sectors (renewable generation, electrolysis, H2 compression to storage and transportation and end user) is captured using sensors, and digital devices with a specific time scale. Data, such as weather, humidity, temperature, and pressure data, can also be collected from the environment. Some usable data, e.g., information about external events, can be collected from social media. The generated data are transmitted to the IoT network using IoT devices such as sensors and actuators through the network technologies 3G/4G/5G, ZigBee, wi-fi, Bluetooth, and wired communication.

The important data that needs to be processed quickly (requiring low latency) is processed by the edge nodes. The edge nodes are close to the data collection points, and therefore, require very low latency [3]. However, there are some cases in which the benefits may not be achieved, since the latency not only depends on the distance between the data collection point and edge processing server, but also on the edge server's processing power, tasks' computational complexity, and edge traffic [4]. To achieve the latency requirements efficiently, the edge network should be designed by keeping in mind factors such as task complexity, processing power of the servers, and the network topology used. Regarding the bandwidth, edge computing reduces the data traffic by distributing the data among different edge servers for computational workload, and thus, lower amount of data is required to be shifted to the cloud.

The cooperation between cloud and edge computing provides high bandwidth as the bits are transmitted to the cloud server when the sum of the tasks exceeds the combined computational capacity of the edge servers. The huge amount of data generated by these devices is stored in a low-cost storage at the cloud. In the second phase of data acquisition, the generated big data based on the volume, velocity, and variety is stored in a shared distributed fault tolerant database. The collected data is then transferred into the master node(s) in the Hadoop cluster. As the data is collected from multiple heterogeneous devices, it may have different data formats and information, and therefore, data preprocessing will be required. The last phase is the data analytics; the tools used in Hadoop for data analytics is Scalable Advanced Massive Online Analysis (SAMOA), a distributed streaming ML framework consisting of programming abstraction for distributed streaming algorithms for data mining and ML tasks. Data visualization (graphs, reports, etc.) is done using Tableau, a common tool for interactive data visualization and sharing of information and dashboards.

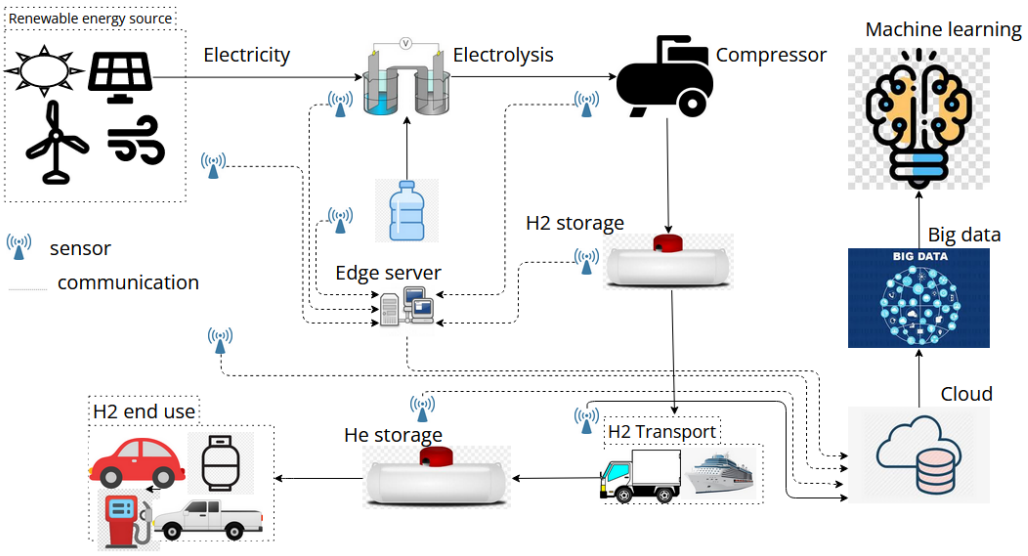

Fig. 4. Hydrogen process from generation, storage, transportation to end use, using the renewable energy sources

VI. Conclusions

Cyberattacks on energy facilities can result in catastrophic damage, with far-reaching consequences. These attacks have the potential to plunge entire cities into darkness during the coldest months, cause hardware damage to critical infrastructure, and disrupt energy production on a massive scale. While the cyber threat is palpable, the integration of cybersecurity measures into energy systems remains inadequate. Many organizations are endeavoring to establish policies and frameworks that mandate cybersecurity as a core consideration in energy transition planning. However, these efforts remain a work in progress.

Acknowledgements

The authors gratefully acknowledge the public financing of Business Finland for the 'HYGCEL' project.

References

[1] E. G. Franco, M. Kuritzky, R. Lukacs, S. Zahidi *et al.*, "The global risks report 2020," in *World Economic Forum*, 2020.

[2] M. Ullah, "Framework for digitalizing different industrial sectors via the internet of things," 2023.

[3] M. Ullah, D. Gutierrez-Rojas, E. Inkeri, T. Tynjälä, and P. H. Nardelli, "Operation of power-to-x-related processes based on advanced data-driven methods: A comprehensive review," *Energies*, vol. 15, no. 21, p. 8118, 2022.

[4] C. Okoli and K. Schabram, "A guide to conducting a systematic literature review of information systems research," 2010.

[5] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *computers & security*, vol. 38, pp. 97–102, 2013.

[6] G. Desarnaud, "Cyber attacks and energy infrastructures: Anticipating risks," 2017.

[7] P. Sanders, C. Bronk, and M. D. Bazilian, "Critical energy infrastructure and the evolution of cybersecurity," *The Electricity Journal*, vol. 35, no. 10, p. 107224, 2022.

[8] L. Meegahapola, P. Mancarella, D. Flynn, and R. Moreno, "Power system stability in the transition to a low carbon grid: A techno-economic perspective on challenges and opportunities," *Wiley Interdisciplinary Reviews: Energy and Environment*, vol. 10, no. 5, p. e399, 2021.

[9] E. Martel, R. Kariger, and P. Graf, "Cyber resilience in the electricity ecosystem: Principles and guidance for boards," *Center for Cybersecurity and Electricity Industry Community*, 2019.

[10] C. M. Patterson, J. R. Nurse, and V. N. Franqueira, "Learning from cyber security incidents: A systematic review and future research agenda," *Computers & Security*, p. 103309, 2023.

[11] L. Fischer, M. Uslar, D. Morrill, M. Döring, and E. Haesen, "Study on the evaluation of risks of cyber-incidents and on costs of preventing cyber-incidents in the energy sector," *European Commission: Berlin, Germany*, vol. 6, p. 41, 2018.

[12] M. Ullah and K. Smolander, "Highlighting the Key Factors of an IoT Platform," *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 901–906, 2019.

[13] M. Ullah, P. H. Nardelli, A. Wolff, and K. Smolander, "Twenty-one key factors to choose an iot platform: Theoretical framework and its applications," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10 111–10 119, 2020.

[14] A. A. Munshi and Y. A. Mohamed, "Cloud-based visual analytics for smart grids big data," in *2016 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2016, pp. 1–5.

[15] W. Shi and S. Dustdar, "The promise of edge computing," *Computer*, vol. 49, no. 5, pp. 78–81, 2016.

[16] J. Zhang, H.-W. Lee, and E. Modiano, "On the robustness of distributed computing networks," in *2019 15th International Conference on the Design of Reliable Communication Networks (DRCN)*. IEEE, 2019, pp. 122–129.

[17] J. Hou, C. Hu, S. Lei, and Y. Hou, "Cyber resilience of power electronics-enabled power systems: A review," *Renewable and Sustainable Energy Reviews*, vol. 189, p. 114036, 2024.

[18] C. Li, J. Wang, S. Wang, and Y. Zhang, "A review of iot applications in healthcare," *Neurocomputing*, p. 127017, 2023.

[19] N. Ferris and S. Van Renssen, "Cybersecurity threats escalate in the energy sector," *URL: https://www. energy-monitor. ai/tech/digitalisation/cybersecurity-threatsescalate-in-the-energy-sector.(accessed: 15.05. 2022)*, 2021.

[20] H.Andrew Schwartz, "Significant Cyber Events List," 2024. [Online]. Available: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[21] M. Ullah, A. Narayanan, A. Wolff, and P. Nardelli, "Smart grid information processes using iot and big data with cloud and edge computing," in *2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO)*. IEEE, 2021, pp. 956–961.