MA-Proposal-Danesh

Navid Rahimidanesh

March 2023

1 Abstract

2 Introduction

2.1 Motivation

2.2 Thesis Goal

Towards a data sharing platform for "Cyber Threat Intelligence" information focused in the Smart Grid use case, that supports privacy and sovereignty of data to increase the security of smart electricity infrastructure.

2.3 Outline

3 Background and Related Work

3.1 Background

Smart Grid Security

A smart grid is an advanced electrical grid that uses advanced technologies to efficiently manage the generation, distribution, and consumption of electricity. Smart grid security involves protecting the system from cybersecurity threats that can disrupt or damage the grid's operations. It could be divided into three layers: physical security, network security, and data security. Physical security includes measures to protect the physical infrastructure of the grid, such as substations, transformers, and power lines. This can include fencing, security cameras, and access controls. Network security involves protecting the communication networks used by the smart grid. This can include implementing firewalls, intrusion detection systems, and encryption to prevent unauthorized access or attacks. Data security involves protecting the data generated and used by the smart grid, including customer data, operational data, and control data. This can include implementing access controls, data encryption, and backup and recovery systems to ensure the availability and integrity of the data.

Smart grids face a range of severe cyber threats, including data injection attacks on state estimation [5,6], distributed denial of service (DDoS) and denial of service (DoS) attacks [7], targeted attacks, coordinated attacks, hybrid attacks, and advanced persistent threats [8,9]. Moreover, in recent years, ransomware campaigns have emerged as a significant risk to the sector [10-12].

Threat intelligence Sharing

Cyber threat intelligence (CTI) is the process of collecting, analyzing, and disseminating information about potential or current cyber threats. CTI relies on gathering data from diverse sources, including security tools, threat feeds, honeypots, forums, social media platforms, and other relevant online and offline sources. This data can include indicators of compromise (IOCs), malware samples, network traffic logs, vulnerability information, and more. The goal is to provide organizations with a comprehensive understanding of potential cyber threats to make informed decisions. It helps identify the tactics, techniques, and procedures (TTPs) used by threat actors and vulnerabilities in an organization's security infrastructure. It is an important component of a comprehensive cybersecurity strategy to reduce the risk of a cyber attack. Sharing cyber threat intelligence allows organizations to enhance their situational awareness, proactively defend against potential threats, and improve incident response capabilities. Through collaboration and information exchange between organizations, it leads to a more robust cybersecurity posture for the entire community.

There are several approaches and frameworks for sharing CTI, including commercial and non-commercial platforms. It could include government initiatives as well as open-source communities. Commercial platforms are typically managed by cybersecurity vendors that provide CTI feeds to their customers. Non-commercial platforms include collaborative initiatives among organizations, such as Information Sharing and Analysis Organizations (ISAOs) and Information Sharing and Analysis Centers (ISACs).

Despite the benefits of CTI sharing, there are also gaps and limitations that need to be addressed. These include concerns around privacy, legal and regulatory barriers, lack of trust among participants, and difficulties in sharing information in real-time. In addition, the lack of a standardized format for CTI sharing can make it challenging for organizations to share and use CTI effectively. As such, efforts to standardize CTI sharing formats and improve trust among participants are critical for improving the effectiveness of CTI sharing initiatives.

Data Spaces

The term data spaces term was first coined by Franklin et al to describe a new paradigm for data management [1]. It solves some data integration tasks by offering a consolidated perspective of data residing in diverse origins, encompassing databases, files, and web services without physically transfer the data. He proposed a DataSpace Suppport Platform (DSSP) that helps developers by enabling them to query and manipulate the data from multiple sources using a single query language with the help of this unified view of data sources.

Beside its technological definition, one could define data spaces from an economic point of view, where data spaces is a form of data exchange. In this viewpoint, dataspaces describes a situation where two or more organizations exchnage data to gain a common benefit. [2]

However, there is not a single definition of data spaces. Dataspaces is a concept to fulfill several requirements. In different contexts, different requirements are more important than others.

Data sharing or integration is one requirement. Data spaces could be used to integrate data from different sources. It could also be viewed as a data exchange platform in some contexts.

Another crucial requirement, that makes data spaces interesting, is the sovereignty of data. Sovereignty can generally be defined as supreme authority. In the context of data, it denotes the right of the owner to control how and by whom will the data be used. Data spaces could fulfill this requirement by keeping the data in the data source and providing a unified view of the data to the consumers with respect to the access control policies defined by the owner of the data.

Another aspect of data spaces is its governance. It is required to define a set of policies, rules and protocols to ensure a smooth exchange of data. Therefore, a governance body is expected to be established to define and enforce these policies. [2]

Data spaces should be open, meaning anyone complying with the policies should be able to join without restriction. This encourages a fair and non-monopolistic market. This entails an easy access, which means, anyone could be able to connect with a limited effort.

Data spaces are usually designed to be decentralized and federated. Meaning there is no entity having direct control over all data exchanges. Different participants could interact with each other directly. This emphasizes the role of interoperability. This is only possible when certain open standards are established. Consequently, data spaces complying to the same standards could be embedded inside each other enabling cross-data-space exchange [2].

> ”Data Spaces are defined as: A federated, open infrastructure for sovereign data sharing, based on common policies, rules and standards.” [2]

3.2 Related Work

EE-ISAC

European Energy Information Sharing and Analysis Centre (EE-ISAC) is a non-profit organization that facilitates the exchange of cyber threat information between its members. Since its foundation in 2015 it acquired over 30 members from utilities, academia, governmental and non-governmental organizations. Members exchange cyber threat information through plenary meetings, working groups, and a dedicated platform (based on MISP). EE-ISAC facilitates trust based information exchange which is not present in the mandatory information sharing in the NIS directive. This trust is achieved by confideniality agreements and regular physical meetings with the same members. [3]

IDS

The International Data Spaces (IDS) is an initiative with the goal of designing a distributed software architecture for data exchange with sovereignty. It was launched in 2015 as a Fraunhofer research project funded by the German Federal Ministry for Education and Research [4]. Shortly after that, in 2016, the IDS Association (IDSA) was founded as a non-profit organization to continue the research. It resulted in definition of the IDS Reference Architecture Model (IDS RAM). The IDS RAM is the description of IDS components and their interactions without being technology specific [4]. IDS RAM allows anyone to implement the IDS compliant components using any technology. The IDSA also provides a reference implementation of different IDS components called IDS Testbed.

Components [5]

Gaia-X

Gaia-X is a European initiative to create a federated data infrastructure for Europe. It is a non-profit organization that aims to create a secure,

4 Use case and Requirements

5 Conceptual Approach

6 Realisation / Implementation

7 Evaluation

8 Timeline / Milestones / Project Plan

References

[1] M. Franklin, A. Halevy, and D. Maier, "From databases to dataspaces: a new abstraction for information management," *ACM SIGMOD Record*, vol. 34, pp. 27–33, Dec. 2005.

[2] Reiberg, A. a. Niebel, and Crispin, "What is a Data Space?," 2022.

[3] T. Wallis and R. Leszczyna, "EE-ISAC—Practical Cybersecurity Solution for the Energy Sector," *Energies*, vol. 15, p. 2170, Mar. 2022.

[4] B. Otto, “The Evolution of Data Spaces,” in *Designing Data Spaces : The Ecosystem Approach to Competitive Advantage* (B. Otto, M. ten Hompel, and S. Wrobel, eds.), pp. 3–15, Cham: Springer International Publishing, 2022.

[5] H. Pettenpohl, M. Spiekermann, and J. R. Both, “International Data Spaces in a Nutshell,” in *Designing Data Spaces : The Ecosystem Approach to Competitive Advantage* (B. Otto, M. ten Hompel, and S. Wrobel, eds.), pp. 29–40, Cham: Springer International Publishing, 2022.