

# 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

### 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 was first coined by Franklin et al to describe a new paradigm for data management [1]. The objective is to offer a consolidated perspective of data gathered from diverse origins, encompassing databases, files, and web services. Data spaces are built to be adaptable and expandable, enabling users to incorporate new data sources as required. They also facilitate

data integration and sharing among various applications and systems. Typically, data spaces employ a federated architecture, where each data source is represented as a network node, interconnected by links that depict relationships between the data sources. This setup empowers users to query data from multiple sources using a unified query language. Moreover, data spaces are designed with scalability in mind, allowing users to add new nodes and links as necessary, accommodating the growing volume of data. Security is a crucial aspect of data spaces, enabling users to control access to their data through access control policies that define authorized data access. Furthermore, data spaces are designed to be extensible, enabling users to incorporate additional data sources and links without altering the existing ones. Interoperability is also a fundamental feature, enabling data sharing between diverse applications and systems by establishing data exchange formats that outline the rules for data interchange. In other words:

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

## **Related Work**

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 confidentiality agreements and regular physical meetings with the same members. [3]

## **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 dataspace: a new abstraction for information management,” *ACM SIGMOD Record*, vol. 34, pp. 27–33, Dec. 2005.

- [2] A. Reiberg and C. Niebel, “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.