Empowering Distributed Decision Making in Smart Grid

Empowering Distributed Decision Making in Smart Grid: Secure Communication and Data Management for Edge Computing

Eslam Mofreh, Phuong Nguyen, and Koen Kok
Eindhoven University of Technology, Eindhoven, The Netherlands
Email: e.mofreh@tue.nl

***Abstract*—In response to the challenges associated with the adoption of distributed decision-making systems (DDMS) in the context of modern power grids, particularly concerning the integration of distributed energy resources (DER) and increasing demand, this research introduces an innovative framework grounded in Information and Communication Technology (ICT). The proposed framework aims to enhance DDMS by incorporating secure and standardized edge computing to streamline data retrieval and local computation, thereby achieving optimal efficiency. Through authentication, authorization, and data loss prevention measures, the proposed framework guarantees a secure data exchange. In addition, it integrates the Common Information Model (CIM) and an ontology to standardize the flow of data, improving interoperability in heterogeneous systems. This study provides a concise overview of the proposed architecture, emphasizing its adaptability and efficiency in addressing contemporary issues in DDMS. In addition, an illustrative use case will be investigated to demonstrate the potential of the proposed architecture and its intricate interactions.**

***Index Terms*—Edge Computing, Decentralized Energy Systems, Secure Data Sharing, Ontology, Information Models**

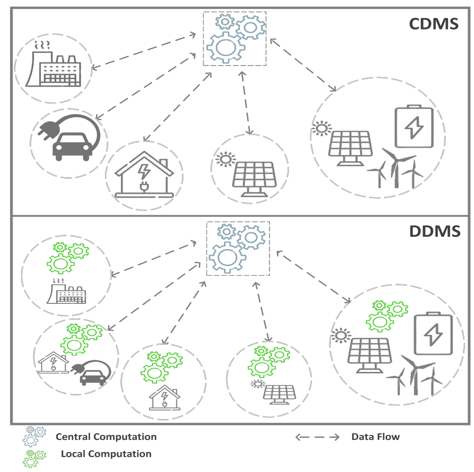

Fig. 1. CDMS vs DDMS

I. Introduction

In the rapidly evolving landscape of contemporary power grids, the adoption of DDMS has emerged as a transformative response to the challenges associated with centralized decision making systems (CDMS) [1]. As shown in figure 1 and unlike CDMS, where computation occurs centrally, DDMS empowers grid edges to make decisions autonomously, facilitating a more flexible and adaptive approach to decision-making that enhances resilience and resource management [2].

Numerous studies underscore the immense potential of DDMS in various energy systems, highlighting its crucial role in improving energy efficiency, optimizing resource allocation, and facilitating task offloading [3]–[5]. To grapple with the inherent complexity of DDMS systems, proposed solutions include the adoption of multi-agent systems, fog and edge computing, and holonic energy systems [4], [6], [7]. Advancements in DDMS, geared towards increased robustness and computational efficiency, are observable with the utilization of federated learning techniques [8]–[10]. Additionally, the integration of edge computing contributes significantly to reducing data transmission and enhancing computational efficiency [5], [11].

The integration of distributed energy resources (DER) brings about a shift towards active consumers who can actively engage with the power grid in DDMS systems for activities such as peer-to-peer trading and demand response programs. This transition leads to a significant increase in data sharing and communication within the grid, raising concerns about security and complexity [12]. Therefore, it highlights the importance of having a well-defined and efficient ICT framework to manage data and regulate communications in DDMS systems.

There are two areas of investigation in the realm of secure communication and data management (SCDM) within DDMS systems. The first pertains to the establishment of secure data sharing mechanisms, where cryptography plays a central role in fortifying communication channels and safeguarding against potential threats [13]. Research contributions have focused on cryptography for secure DDMS, examining the impact of quantum computing on modern cryptography and proposing defense strategies such as quantum key distribution (QKD) and post-quantum cryptography (PQC) [14]. Furthermore, in blockchain-based architectures, advanced lightweight cryptography can be combined with knowledge representation models and decision-making processes to improve real-time situational awareness and decision-making in the power grid [15].

Other studies focused on ensuring secure and efficient decision-making in DDMS. One approach that has been explored is the use of secure multiparty computation (SMPC), which introduces new algorithms that combine the Paillier Cryptosystem with the alternating direction multiplier method (ADMM) to achieve privacy-preserving distributed optimal energy flow [16]. The advantages of SMPC over differential privacy-based methods are also discussed in these works [16]. Another area of research addresses cryptographic considerations for securing communications in DERs, providing insight into authentication and encryption methods that have implications for the design of DER systems [17]. The role of blockchain technology in DDMS is also investigated, particularly in the context of community energy projects and the integration of DER [18]. Additionally, a proposal is made to employ homomorphic encryption in a uniform price double auction mechanism to achieve privacy-preserving transactive energy systems [19].

The second area focuses on the augmentation of interoperability and standardization in the exchange of data within these systems, employing information models and ontologies. Researchers emphasize the crucial role of ontologies, such as SAREF [20], and information models such as CIM and Industrial Data Space (IDS) [21], [22]. The significance of ontologies lies in their ability to describe subject areas and ensure interoperability among diverse systems. SAREF, supported by the ETSI SmartM2M standard, is particularly noted for providing interoperable solutions in IoT projects, including applications in smart buildings and energy management [20]. Furthermore, CIM standards and extensions are used to construct the ontology of smart distributed energy systems, which integrates seamlessly with other domain ontologies [23], [24].

These ontologies play a crucial role in the management of decentralized data at the device level within energy systems in households. This development facilitates the expansion of the scope of the data and the retrieval of additional information from the Internet, contributing to the advancement of more intelligent and adaptable decision support tools. The impact extends to electricity markets, smart grids, and energy management, enhancing the overall efficiency and flexibility of decision-making processes.

Further contributions from various research explore ontological approaches to form unified information models, enhance interoperability in electricity markets, and address data isolation issues in decentralized household energy systems. The works delve into ontology modeling for microgrid control systems [25], decision support systems to forecast the development of energy infrastructure [26], and automatic mapping technology for heterogeneous CIM [27]. Additionally, extensions like SARGON are introduced to cover the smart energy domain, showcasing advancements in ontological approaches for modeling, interoperability, and decision support within smart distributed energy systems [28].

Although the literature has been enriched with the introduction of contributions pertaining to secure communications and standardized data exchange approaches within the power grid operations, there is a lack of efficient ICT frameworks that efficiently amalgamate all together in a standardized manner.

This study introduces a new architectural framework that enhances DDMS systems that incorporate edge computing technology and addresses standardized communication and secure data-sharing complexities between edge devices.

The proposed framework strategically enhances DDMS by using secure and standardized edge computing, offering optimal efficiency in data retrieval and local computation. This study establishes the importance of the framework by identifying challenges, presenting a novel architecture, and examining its intricacies, providing a comprehensive solution to the evolving energy landscape. Subsequent sections will offer a detailed analysis and explanation of this architectural framework, providing valuable insights into its potential to reshape decision-making processes within the continually transforming realm of DDMS. An illustrative use case will be investigated to demonstrate the potential of the proposed architecture and its intricate interactions.

II. METHODOLOGY

The research employs a methodology to address the challenges of incorporating edge computing as technology for DDMS in the smart grid. The aim is to enhance decentralized decision-making, secure data sharing, and standardized communication.

Edge computing, in this context, refers to a distributed computing paradigm that involves processing data closer to the source of generation or consumption as depicted in figure 1, typically at or near the edge of the network. This approach reduces the need for centralized processing, enabling quicker data analysis and decision-making.

Classification of Communication Types

The classification of communication types is crucial for understanding the interactions between the edge devices or the edge devices and the central server. Two primary types are identified: *Data Request* and *Computation Request*.

- *Data Request:* involves requesting specific data from other edge devices or a central server. Examples include requesting energy consumption data, historical energy production information, and weather data.
- *Computation Request:* involves initiating computation tasks, such as federated learning algorithms, and complex optimization calculations.

Stages of the Proposed Framework

The proposed framework, illustrated at a high level in figure 2, encompasses smart meters at the physical level. These smart meters furnish edge devices with reading data, facilitating storage and processing. To fortify communication and manage data securely, the framework is realized as an additional ICT layer superimposed on edge devices.

The proposed architecture is visually elucidated in figure 3, offering insights into the intricate interactions and architectural nuances. Upon receiving a *Data* or *Computation* request, the

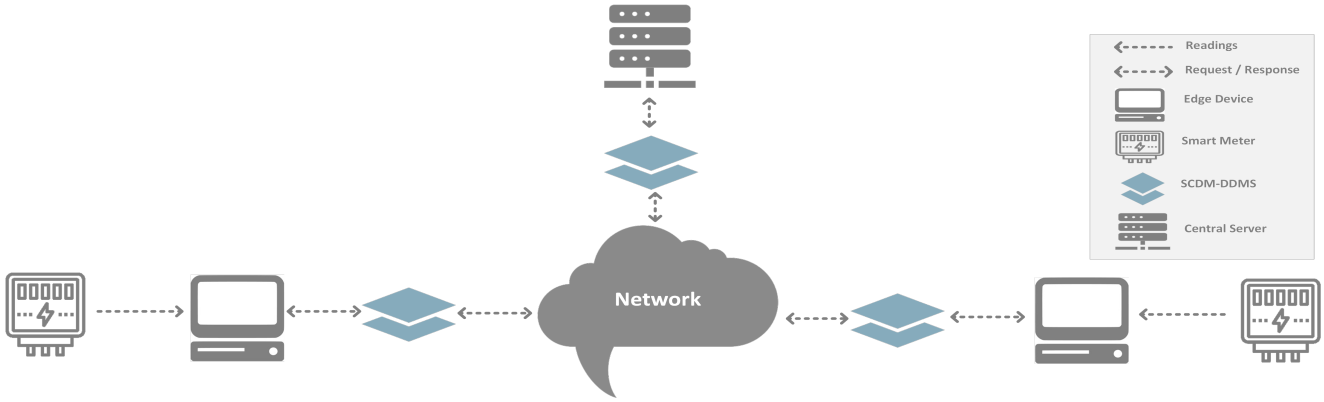

Fig. 2. Edge-to-Edge & Edge-to-Server communication

system employs a series of stages, beginning with *Authentication* and progressing through *Authorization*, *Fetch*, *Loss Data Prevention*, *Mapping Data to Concepts*, and *Ontology Alignment*. This systematic approach ensures a comprehensive and secure handling of requests.

The subsequent subsections will provide a detailed exposition of each of these stages, elucidating their significance and functionalities within the proposed framework.

1) ***Authentication****:* In the foundational stage of our proposed framework, *Authentication* serves as the bedrock for secure and authenticated interactions. The *Authentication* process is intricately designed to establish the identity of edge devices entering the system, employing robust *Public Key Infrastructure (PKI)* principles for a secure and reliable foundation. RSA (Rivest–Shamir–Adleman) is the PKI approach utilized in this stage.

- *Initiation of Registration:*
  When an edge device is introduced into the DDMS system, it initiates a registration request to the *Authentication Server*. This step is crucial for the device to establish its presence within the system and gain a secure identity.

- *Key Pair Generation:*
  The *Authentication Server* responds by generating a unique public-private key pair $(pk_{\text{edge}}, sk_{\text{edge}})$ for the edge device. The mathematical underpinning involves selecting large prime numbers, a and b, computing the modulus $p = a \cdot b$, determining the totient as depicted in eq (1)
  $$\phi(p) = (a-1)(b-1), \tag{1}$$
  and selecting a public exponent e coprime to $\phi(p)$. The private exponent d is then computed. The private exponent d is the modular multiplicative inverse of $e \bmod \phi(p)$. The equation $(d * e) \bmod \phi(p)$ equals 1. The resulting public key is $pk_{\text{edge}} = (p, e)$, and the private key is $sk_{\text{edge}} = (p, d)$.

- *Delivery of Key Pair:*
  The *Authentication Server* securely delivers the public key pk_{edge} to the edge device, maintaining the confidentiality of the private key sk_{edge} within its secure enclave.

- *Token Generation:*
  Within this framework, a *JSON Web Token (JWT)* is employed for token generation. The token facilitates the secure transmission of information between two entities. The edge device, equipped with its unique key pair $(pk_{\text{edge}}, sk_{\text{edge}})$, engages in the *Authentication* procedure by presenting its public key (pk_{edge}) to the *Authentication Server*. Utilizing its stored public key information, the server generates a token (T_{edge}) using the private key (sk_{edge}) and the roles (R_{edge}) stored in the *payload* of this token. This process can be mathematically expressed as depicted in Eq (2)
  $$T_{\text{edge}} = \text{Sign}_{sk_{\text{edge}}}(\text{Hash}(pk_{\text{edge}}, payload)) \tag{2}$$
  Here, $\text{Sign}_{sk_{\text{edge}}}$ denotes the generation of a digital signature using the private key.

- *Token Issuance:*
  The generated token T_{edge} is securely transmitted to the edge device, completing the *Authentication* process. This token serves as a secure digital credential for the edge device.

- *Usage of Token:*
  Subsequently, the edge device employs T_{edge} in its requests. The token validates the identity of the edge device, ensuring secure access to resources within the DDMS smart grid system.

2) ***Authorization****:* The *Authorization* stage is a critical component of the proposed framework, ensuring secure access to resources through roles stored in tokens. This section presents the foundation behind the *Authorization* process. As mentioned in *Authentication* section, (R_{edge}) define resource access in a

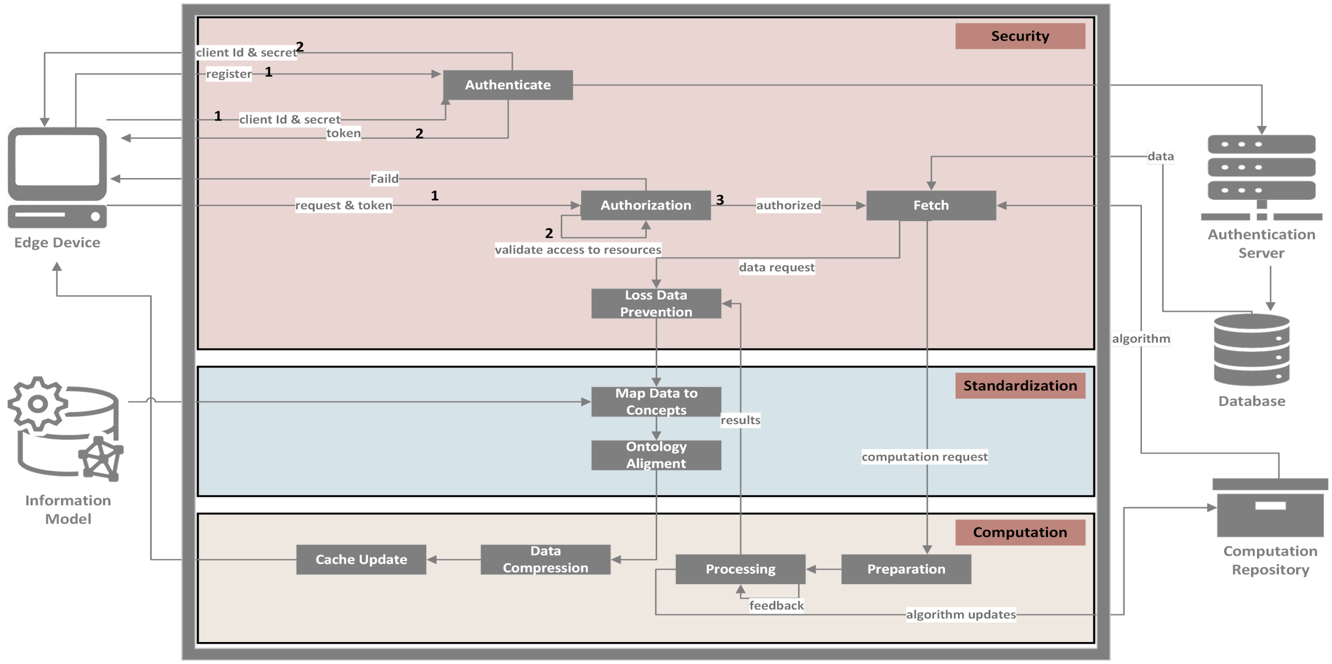

Fig. 3. Secure Communication and Data Management in DDMS (SCDM-DDMS)

token (T_{edge}). Each role denoted r_i is associated with a set of policies p_j that specifies the authorized actions of an edge on a resource as mathematically represented by eq (3).

$$p_j = (r_i, a_k, rs_l), \tag{3}$$

where a_k is the (k$^{\text{th}}$) action (such as Read/Write/Execute) that can be taken by r_i, and rs_l is the (l$^{\text{th}}$) resource. The subsequent stages are only accessible to authorized requests, while non-authorized requests are redirected back to the requesting edge.

*3) **Fetch**:* As shown in figure 3, in the *Fetch* stage of our proposed framework, authorized requests proceed to retrieve data from *Local Storage* or computation algorithms from a *Computational Registry* based on the specified request type.

*4) **Loss Data Prevention (LDP)**:* This layer plays a critical role in securing data in transit by employing encryption techniques. This stage addresses the protection of sensitive information, ensuring that unauthorized entities cannot access or compromise critical data. Identification of sensitive data is achieved through metadata, including binary variables that indicate whether specific data elements are sensitive.

- *Sensitive Data Identification:* The proposed framework utilizes a local metadata configuration data store such as a metadata file or database table. Each local data element is marked as sensitive or nonsensitive using a binary variable. Let (S_{data}) represent the set of sensitive data elements and it is defined as shown in eq (4).

$$S_{\text{data}} = \{d_i \mid M_{\text{metadata}}(d_i) = \text{Sensitive}\}, \tag{4}$$

where d_i is data element of requested data D

- *Encryption Process:* The LDP layer initiates the encryption process for every sensitive data element d_i identified. Let $E(d_i)$ represent the encryption of the sensitive data element d_i as depicted in eq (5).

$$E(d_i) = \text{Encrypt}(d_i) \tag{5}$$

The resulting data set D_{masked} contains encrypted sensitive data and is represented by eq (6).

$$D_{\text{masked}} = D \text{ with } S_{\text{data}} \text{ replaced by } \{E(d_i) \mid d_i \in S_{\text{data}}\} \tag{6}$$

*5) **Mapping Data to Concepts**:* In the *Mapping Data to Concepts* stage, the framework establishes a link between the original data and standardized concepts from CIM concepts depending on the use case. This stage is crucial for promoting interoperability and ensuring a common understanding of the information exchanged within the system. Mapping involves associating each data element (d_i) with relevant CIM concepts (c_j). For example, `cim:TransactionBid`, `cim:TransactionBidClearing` are relevant to a scenario where we simulate P2P trading. Mathematically, this can be expressed as represented by eq (7):

$$M_{\text{mapping}} = \{(d_i, c_j) \mid d_i \in D, c_j \in C_{\text{CIM}}\}, \tag{7}$$

where D is the original data, M_{mapping} is the mapping from original data to CIM concepts.

*6) **Ontology Alignment**:* The *Ontology Alignment* stage ensures that the mapped data and concepts are aligned with a predefined ontology based on the system's use case. This process establishes a standardized representation of data to enhance interoperability and facilitate seamless communication.

- *Building Ontology Based on Use Case:* The ontology is constructed with elements relevant to the specific use case, adhering to a standard format for data exchange within the system. Development tools such as Resource Description Framework (RDF) and W3C Web Ontology Language (OWL) can be employed for this purpose.

- *RDF:* It serves as a tool for building ontologies, utilizing triples (subject, predicate, object) to express relationships. In the context of system representation, the subject signifies a data element, the predicate indicates a mapping, and the object represents the associated CIM concept. An illustration is provided below:

```
(DataElement1, hasCIMConcept, CIMConcept)
(:Substation123, :hasVoltageLevel, "138 kV
    ")
```

- *OWL:* It was designed for the Semantic Web, which is a tool for ontology construction. It allows for the comprehensive representation of knowledge about objects and their connections. OWL facilitates the expression of CIM concepts and ontology elements, as demonstrated in the following OWL declaration:

```
<Class IRI="#CIMConcept"/>
```

- *Communication Representation in an Ontology Format:* Various formats, such as RDF/XML, Turtle (.ttl), N-Triples (.nt), N3 (Notation3), and JSON-LD (JSON for Linking Data), can be employed to represent an ontology. In this context, RDF/XML is utilized to declare each concept, property, or class in XML tags, as exemplified by the following RDF/XML serialization:

```
<cim:EnergySource rdf:ID="_8E2HG73F-6234-1
    ABC-D9EF-5A1C82BC4D6A">
  <cim:IdentifiedObject.name>source</
      cim:IdentifiedObject.name>
  <cim:Equipment.EquipmentContainer
      rdf:resource="#_1A2BC3D4E-5678-9F01-2
      GHI-JK34LM567NOP"/>
  <cim:EnergySource.voltageMagnitude>60</
      cim:EnergySource.voltageMagnitude>
</cim:EnergySource>
```

  This RDF/XML example showcases the serialization of an EnergySource object from CIM, embodying statements that describe attributes such as name, EquipmentContainer, and voltageMagnitude.

The following two stages are optional stages to enhance the system's responsiveness and speed.

*7) **Data Compression**:* The *Data Compression* stage within the proposed SCDM-DDMS framework plays a pivotal role in optimizing communication efficiency. In the context of power grid applications, the need for efficient data transmission is critical, especially considering the vast amounts of data generated by sensors, meters, and grid components, and the different computation techniques such as Federated Learning that need model parameters exchange from edge devices to the central server.

Various compression algorithms, such as Huffman coding, Lempel-Ziv-Welch (LZW), or Run-Length Encoding, can be applied based on the characteristics of the data and the specific requirements of the power grid use case. The goal is to reduce the size of the data representation while preserving essential information, thereby optimizing bandwidth utilization during communication.

*8) **Cache Update**:* The *Cache Update* stage is essential for maintaining the integrity and relevance of the cached information within the SCDM-DDMS framework. In the dynamic environment of power grids, where operational data constantly evolves, efficient cache management is crucial for ensuring that decision-making processes are based on the most recent and accurate information. The cache update process involves checking for changes or additions to incoming data, updating the relevant entries in the cache, and ensuring that the cached information is aligned with the current state of the power grid.

III. Case Study: Peer-to-Peer Energy Trading

In this section, we present a detailed case study illustrating the application of our proposed architecture in the context of edge computing DDMS for peer-to-peer (P2P) energy trading. This case study explores a simple scenario involving two prosumers, Prosumer A and Prosumer B, engaging in a secure and efficient energy exchange facilitated by edge computing.

A. Initialization

The scenario begins with the initialization phase, where Prosumer A and Prosumer B authenticate themselves within the DDMS. Each prosumer obtains a unique client ID and secret key, establishing a secure identity for subsequent interactions.

B. Trade Proposal (Data Request)

Prosumer A initiates a trade proposal by creating a bid for energy exchange. The components of the proposed framework come into play:

- **Authentication and Authorization:** Prosumer A authenticates using a token generated by its client ID and secret key, and the system authorizes the trade proposal request based on these credentials.
- **Loss Data Prevention:** Energy amount, bidding price, time, region, and participant id data require hiding in this step.
- **Map Data to Concepts and Ontology Alignment:** The bid is mapped to the CIM concepts `cim:Bid`, `cim:Price`, `cim:TimeInterval`, `cim:MarketRegion`, `cim:TradeType`, `cim:MarketParticipant`, providing a standardized representation.

```
<cim:Bid rdf:about="#bid123">
    <cim:FloatQuantity rdf:about="#
        bidQuantity">
      <cim:FloatQuantity.unitSymbol>kg</
          cim:FloatQuantity.unitSymbol>
      <cim:FloatQuantity.unitMultiplier
          rdf:datatype="http://www.w3.org
          /2001/XMLSchema#int">
          XY3sLp82qRAzNf1bT6HOdEJ7gK9I</
          cim:FloatQuantity.unitMultiplier>
      <cim:FloatQuantity.value
          rdf:datatype="http://www.w3.org
          /2001/XMLSchema#decimal"
      >GJ7pQy2bLz4vX9tA1eN3wFm5sR8v</
          cim:FloatQuantity.value>
    </cim:FloatQuantity>

   <cim:Price rdf:about="#bidPrice">
      <cim:Price.category>Euro per kWh</
          cim:Price.category>
      <cim:Price.amount rdf:datatype="
          http://www.w3.org/2001/XMLSchema#
          decimal"
      >RJ2wXr8vDp9eN1lY3QkA4sFm7T</
          cim:Price.amount>
   </cim:Price>

   <cim:TimeInterval>
    <cim:TimeInterval.end rdf:datatype="
        http://www.w3.org/2001/XMLSchema#
        dateTime">
        Rb2yXs8L5hZTkN3nD7QpFgV1rEaW</
        cim:TimeInterval.end>
   <cim:TimeInterval.start rdf:datatype="
       http://www.w3.org/2001/XMLSchema#
       dateTime">
       XZ3rLy895HJFQaP2bP7xKw9sRgT</
       cim:TimeInterval.start>
   </cim:TimeInterval>

   <cim:MarketRegion>
     <cim:GeographicalRegion>
        US4uUm7410GPeM9mY9WCOpKVQkA=</
        cim:GeographicalRegion>
   </cim:MarketRegion>

   <cim:MarketParticipant rdf:resource="#
       sellerId"/>
   <cim:IdentifiedObject.mRID>
       RJ2hLs8bFgXpZrN3iQ6oKuYv5AaC</
       cim:IdentifiedObject.mRID>
   </cim:MarketParticipant>

   <cim:TradeType>Bid</cim:TradeType>
 </cim:Bid>
```

- **Compression and Cache Update:**
The trade proposal data are compressed to optimize communication efficiency, and the system updates the cache with the compressed data for efficient retrieval in future trade proposal data requests.

C. Bid Processing (Computation Request)

Upon receiving the bid, Prosumer B processes the bid to create a bid response. The framework steps unfold as follows:

- **Authentication and Authorization:** Prosumer B authenticates using a token generated by its client ID and secret key, and the system authorizes the bid processing request based on these credentials.
- **Loss Data Prevention:** Participant id data is required to be hidden in this step.
- **Map Data to Concepts and Ontology Alignment:** The bid response is mapped to the CIM concepts `cim:Bid`, `cim:Status`, `cim:MarketParticipant`.

```
 <cim:Bid rdf:about="#bid123">
   <cim:Status>
      <cim:Status.reason>Bid Accepted</
          cim:Status.reason>
      <cim:Status.dateTime rdf:datatype="
          http://www.w3.org/2001/XMLSchema#
          dateTime"
      >2024-02-15T12:00:00</cim:Status.
          dateTime>
   </cim:Status>

   <cim:MarketParticipant rdf:resource="#
       buyerId"/>
   <cim:IdentifiedObject.mRID>
       FR2sBn8351XLqP7pZ8ROHgFJtYD</
       cim:IdentifiedObject.mRID>
   </cim:MarketParticipant>

 </cim:Bid>
```

- **Compression and Cache Update:**
The response data is compressed and the system updates the cache with the compressed data for efficient retrieval in future bid processing responses.

D. Bid Matching and Transaction Generation (Computation Request)

The system matches bids from Prosumer A and Prosumer B based on amoung, trade type and price. The framework steps include the following:

- **Authentication and Authorization:** The system authenticates and authorizes the bid-matching request.
- **Loss Data Prevention:** The matched bid is used to form a bid transaction to be sent to both participants. So, the sensitive information provided for that bid is required to be hidden and put in a transaction format.
- **Map Data to Concepts and Ontology Alignment:** The transaction response is mapped to the following CIM concepts `cim:Transaction`, `cim:Price`, `cim:TimeInterval`, `cim:MarketRegion`, `cim:TradeType`, `cim:MarketParticipant`.

```
 <cim:EnergyTransaction rdf:about="#
     energyTransaction1">
   <cim:FloatQuantity rdf:about="#
       bidQuantity">
   <cim:FloatQuantity.unitSymbol>kg</
       cim:FloatQuantity.unitSymbol>
   <cim:FloatQuantity.unitMultiplier
       rdf:datatype="http://www.w3.org
       /2001/XMLSchema#int">
       XY3sLp82qRAzNf1bT6HOdEJ7gK9I</
       cim:FloatQuantity.unitMultiplier>
```

```
    <cim:FloatQuantity.value rdf:datatype="http://www.w3.org/2001/XMLSchema#decimal">GJ7pQy2bLz4vX9tA1eN3wFm5sR8v</cim:FloatQuantity.value>
  </cim:FloatQuantity>

    <cim:Price rdf:about="#bidPrice">
      <cim:Price.category>Euro per kWh</cim:Price.category>
      <cim:Price.amount rdf:datatype="http://www.w3.org/2001/XMLSchema#decimal">RJ2wXr8vDp9eN1lY3QkA4sFm7T</cim:Price.amount>
    </cim:Price>

    <cim:TimeInterval>
     <cim:TimeInterval.end rdf:datatype="http://www.w3.org/2001/XMLSchema#dateTime">Rb2yXs8L5hZTkN3nD7QpFgV1rEaW</cim:TimeInterval.end>
    <cim:TimeInterval.start rdf:datatype="http://www.w3.org/2001/XMLSchema#dateTime">XZ3rLy895HJFQaP2bP7xKw9sRgT</cim:TimeInterval.start>
    </cim:TimeInterval>
    <cim:MarketRegion>
      <cim:GeographicalRegion>US4uUm7410GPeM9mY9WCOpKVQkA=</cim:GeographicalRegion>
    </cim:MarketRegion>

     <cim:Status>
       <cim:Status.reason>Transaction Accepted!</cim:Status.reason>
    </cim:Status>

    <cim:MarketParticipant rdf:resource="#sellerId"/>
    <cim:IdentifiedObject.mRID>RJ2hLs8bFgXpZrN3iQ6oKuYv5AaC</cim:IdentifiedObject.mRID>
    </cim:MarketParticipant>

    <cim:MarketParticipant rdf:resource="#buyerId"/>
    <cim:IdentifiedObject.mRID>FR2sBn8351XLqP7pZ8ROHgFJtYD</cim:IdentifiedObject.mRID>
    </cim:MarketParticipant>

  </cim:EnergyTransaction>
```

- **Compression and Cache Update:**
  The trade transaction data and related invoices are compressed and the system updates the cache with the compressed data.

IV. Exploring the Versatility of the Framework: Potential Use Cases

The proposed SCDM-DDMS framework, leveraging edge computing in the smart grid context, exhibits a remarkable degree of versatility, making it well-suited for a spectrum of diverse use cases beyond the realm of peer-to-peer energy trading. Scientific inquiry into the framework's applicability to different scenarios prompts us to delve into the underlying reasons for its adaptability and the criteria integral to its successful implementation across varied domains. The scientific foundation of the SCDM-DDMS framework's adaptability lies in its core architectural elements designed to enhance decentralized decision-making, secure data sharing, and standardized communication, addressing critical challenges faced by power grid systems. The staged approach, encompassing Authentication, Authorization, Fetch, Loss Data Prevention, Mapping Data to Concepts, and Ontology Alignment, provides a structured and robust framework adaptable to different application scenarios within the smart grid domain.

The classification of communication types, namely Data Request and Computation Request, offers flexibility in addressing diverse information exchange needs within the smart grid. The systematic stages ensure secure and comprehensive handling of communication types, laying the foundation for the framework's applicability across power grid use cases with varying communication requirements.

In considering the adoption of the SCDM-DDMS framework for the smart grid, several scientific criteria merit careful examination.

1) *Data Sensitivity and Encryption Requirements in Grid Operations:* The framework's robust Loss Data Prevention (LDP) stage ensures secure data transmission through encryption. In the power grid context, where data integrity and confidentiality are paramount, the framework's ability to identify and encrypt sensitive data elements aligns with challenges in securing critical information during grid operations.
2) *Interoperability and Standardization for Smart Grid Integration:* The stages of Mapping Data to Concepts and Ontology Alignment contribute to the framework's adaptability within the smart grid by promoting interoperability. In power grid scenarios, which involve diverse equipment, protocols, and data formats, the framework facilitates seamless communication and integration, addressing challenges associated with heterogeneous systems.
3) *Decentralized Decision-Making in Grid Management:* The core objective of the framework to enhance decentralized decision making aligns with the challenges of the power grid. In scenarios like load balance, demand response, and distributed energy resource management, the framework supports edge decision making, contributing to the resilience and efficiency of power grid operations.
4) *Communication Type Variability in Grid Control Systems:* The framework's classification of communication types in the framework accommodates both data requests and computation requests, addressing the varied needs of

power grid control systems. Examples include retrieving real-time sensor data (Data Request) and initiating complex optimization calculations for grid control (Computation Request).

V. Conclusion

In conclusion, the proposed methodology, centered on enabling edge computing as technology for DDMS in the smart grid, addresses challenges related to decentralized decision-making, secure data sharing, and standardized communication. Employing edge computing enhances the efficiency of data retrieval and local computation. The framework's stages, including Authentication, Authorization, Fetch, Loss Data Prevention, Mapping Data to Concepts, and Ontology Alignment, collectively ensure secure and comprehensive handling of communication types. A detailed case study on Peer-to-Peer Energy Trading exemplifies the practical application of the framework. Moreover, the architecture exhibits versatility, extending its impact to microgrid management, energy trading platforms, demand response programs, and beyond, making it a valuable asset across interconnected sectors. Overall, the proposed framework stands as a robust solution poised to advance the efficiency and security of decentralized energy systems in diverse applications.

VI. Acknowledgement

This research was funded by the research program "MegaMind—Measuring, Gathering, Mining and Integrating Data for Self-management in the Edge of the Electricity System", (partly) financed by the Dutch Research Council (NWO) through the Perspectief program under number P19–25.

References

[1] Data sharing in energy systems. *Advances in applied energy*, 2023.
[2] Chongyang Zhang and Zefeng Wu. Shared data privacy protection method, system, terminal and medium. 2018.
[3] H. Bhatti and M. Danilovic. Making the world more sustainable: enabling localized energy generation and distribution on decentralized smart grid systems. *World Journal of Engineering and Technology*, 06(02):350–382, 2018.
[4] C. Pop, T. Cioara, C. Antal, I. Anghel, I. Salomie, and M. Bertoncini. Blockchain based decentralized management of demand response programs in smart energy grids. *Sensors*, 18(2):162, 2018.
[5] M. Kim, J. Lee, K. Park, Y. Park, and Y. Park. Design of secure decentralized car-sharing system using blockchain. *IEEE Access*, 9:54796–54810, 2021.
[6] C. Pop, M. Antal, T. Cioara, I. Anghel, I. Salomie, and M. Bertoncini. A fog computing enabled virtual power plant model for the delivery of frequency restoration reserve services. *Sensors*, 19(21):4688, 2019.
[7] Quy Nguyen Minh, Van-Hau Nguyen, Vu Khanh Quy, Le Anh Ngoc, Abdellah Chehri, and Gwanggil Jeon. Edge computing for iot-enabled smart grid: The future of energy. *Energies*, 15(17), 2022.
[8] Haoyuan Cheng and Qian Ai. Federated learning application in distributed energy trading in integrated energy system. *Energy Reports*, 10:484–493, 2023.
[9] F. Bellizio, S. Karagiannopoulos, P. Aristidou, and G. Hug. Optimized local control for active distribution grids using machine learning techniques. 2018.
[10] M. Soto and H. Adeli. Multi-agent replicator controller for sustainable vibration control of smart structures. *Journal of Vibroengineering*, 19(6):4300–4322, 2017.
[11] Wei Li, Ting Yang, Flávia Delicato, Paulo Pires, Zahir Tari, Samee Khan, and Albert Zomaya. On enabling sustainable edge computing with renewable energy resources. *IEEE Communications Magazine*, 56:94–101, 05 2018.
[12] Wenqing Liu and Juntao Peng. Data encryption and decryption method, device and system. 2019.
[13] Secure sensitive data sharing using rsa and elgamal cryptographic algorithms with hash functions. *Information*, 2022.
[14] Jongmin Ahn, Hee-Yong Kwon, Bohyun Ahn, Kyuchan Park, Taesic Kim, Mun-Kyu Lee, Jinsan Kim, and Jaehak Chung. Toward quantum secured distributed energy resources: Adoption of post-quantum cryptography (pqc) and quantum key distribution (qkd). *Energies*, 15(3), 2022.
[15] Abubakar Sadiq Sani, Dong Yuan, Stephen Ogaji, and Zhao Yang Dong. *CyreumE: A Real-Time Situational Awareness and Decision-Making Blockchain-Based Architecture for the Energy Internet*, pages 787–835. Springer Nature Singapore, Singapore, 2022.
[16] Fangyuan Si, Ning Zhang, Yi Wang, Peng-Yong Kong, and Wenjie Qiao. Distributed optimization for integrated energy systems with secure multiparty computation. *IEEE Internet of Things Journal*, 10(9):7655–7666, 2023.
[17] Christine Lai, Patricia Cordeiro, Adarsh Hasandka, Nicholas Jacobs, Shamina Hossain-McKenzie, Deepu Jose, Danish Saleem, and Maurice Martin. Cryptography considerations for distributed energy resource systems. In *2019 IEEE Power and Energy Conference at Illinois (PECI)*, pages 1–7, 2019.
[18] Nallapaneni Manoj Kumar. Blockchain: Enabling wide range of services in distributed energy system. *Beni-Suef University Journal of Basic and Applied Sciences*, 7(4):701–704, 2018.
[19] Magda Foti. Privacy-preserving market-driven transactive energy system using homomorphic encryption. In *2023 19th International Conference on the European Energy Market (EEM)*, pages 1–8, 2023.
[20] Laura Daniele, Frank den Hartog, and Jasper Roes. Created in close interaction with the industry: The smart appliances reference (saref) ontology. pages 100–112, 08 2015.
[21] Mathias Uslar, Michael Specht, Sebastian Rohjans, Jörn Trefke, and José M. González. *The Common Information Model CIM: IEC 61968/61970 and 62325 - A Practical Introduction to the CIM*. Springer Publishing Company, Incorporated, 2012.
[22] Boris Otto, Sören Auer, Jan Cirullies, Jan Jürjens, Nadja Menz, Jochen Schon, and Sven Wenzel. Industrial data space: Digital souvereignity over data, 02 2016.
[23] Mathias Uslar, Michael Specht, Sebastian Rohjans, Jörn Trefke, and José Manuel Gonzalez Vazquez. *The Common Information Model CIM: IEC 61968/61970 and 62325 - A practical introduction to the CIM*, volume 66. 01 2012.
[24] Fedor S. Nepsha, Alexei A. Nebera, Alexander A. Andrievsky, and Mikhail I. Krasilnikov. Development of an ontology for smart distributed energy systems *. *IFAC-PapersOnLine*, 55(9):454–459, 2022. 11th IFAC Symposium on Control of Power and Energy Systems CPES 2022.
[25] Aravind Ingalalli, Ravish Kumar, and Srijit Kumar Bhadra. Ontological formulation of microgrid control system for interoperability. In *2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA)*, volume 1, pages 1391–1398, 2018.
[26] Alex Kopaygorodsky. Ontology-based decision support system for forecasting of energy infrastructure development. In *2018 3rd Russian-Pacific Conference on Computer Technology and Applications (RPC)*, pages 1–5, 2018.
[27] Zhang Hong, Liu Dong, Lu Yiming, Lv Guangxian, Wang Kairui, and Xiong Xiaofang. Ontology-based automatic mapping technology for heterogeneous common information model. In *2016 China International Conference on Electricity Distribution (CICED)*, pages 1–5, 2016.
[28] M. Haghgoo, I. Sychev, A. Monti, and F. H. P. Fitzek. Sargon – smart energy domain ontology. *IET Smart Cities*, 2:191–198, 2020.