Energy Reports 14 (2025) 3783–3794

Contents lists available at ScienceDirect

Energy Reports

journal homepage: www.elsevier.com/locate/egyr

Research paper

Privacy-preserving ADMM-based multi-agent energy sharing framework between communities using Ring Signature Multi-Party Computation

Wafa Nafkha Tayari [a], Yacine Merrad [a],*, Seifeddine Ben Elghali [a], Mohamed Benbouzid [b]

[a] Aix Marseille Univ, CNRS, LIS, Marseille, 13013, France
[b] University of Brest, UMR CNRS 6027 IRDL, Brest, 29238, France

ARTICLE INFO

Keywords:
Community energy exchange
Decentralized optimization
ADMM
Multi-agent systems
JADE
Privacy preservation
Ring signature
Multi-party computation

ABSTRACT

A critical challenge in community energy management is effectively integrating numerous consumers and prosumers into scalable energy-sharing systems. This paper proposes an innovative privacy-preserving distributed optimization framework leveraging the Alternating Direction Method of Multipliers (ADMM) and Ring Signature Multi-Party Computation (RSMPC). Centralized and distributed models are compared in terms of scalability. Privacy concerns within decentralized optimization are addressed by introducing a ring signature-based cryptographic protocol. Unlike traditional methods such as differential privacy or multi-key homomorphic encryption, our proposed RSMPC scheme balances computational efficiency and rigorous privacy guarantees. The multi-agent architecture, implemented using the JADE platform, demonstrates significant improvements in scalability and privacy preservation.

1. Introduction

Centralized optimization methods for community energy management inherently face scalability issues, particularly as the number of Distributed Energy Resources (DERs), consumers, and prosumers within energy communities continues to rise (Barsanti, 2017). With increasing global penetration of renewable energy and the emergence of Energy Communities (ECs) and Virtual Power Plants (VPPs), the focus has shifted towards minimizing traditional grid reliance and maximizing energy exchanges within and between these communities (Ahmed et al., 2024). Efficiently integrating numerous entities into a scalable and responsive energy exchange system has thus become critical (Kalbantner et al., 2021).

Energy communities have emerged as a novel paradigm in the energy transition, enabling groups of prosumers and consumers to collaborate for the collective management of energy resources, reduction of costs, and promotion of renewable energy (Lowitzsch et al., 2020). These communities foster local energy sharing, enhance grid resilience, and democratize energy markets by allowing end-users to actively participate in decision-making (Lowitzsch et al., 2020).

While the concept of an energy community shares similarities with that of a microgrid, the two are not identical. A microgrid is typically defined as a localized group of interconnected loads and distributed energy resources that can operate in both grid-connected and islanded modes, with a strong focus on the technical aspects of control, protection, and reliability. In contrast, an energy community extends beyond technical operation to encompass social, economic, and strategic decision making dimensions. It emphasizes collective ownership, market participation, and fair benefit distribution among members (Hatziargyriou, 2023)

Energy trading between communities typically involves market clearing formulated as an optimization problem (Faia et al., 2024), primarily aiming to maximize social welfare when demands and supplies are flexible and perform economic dispatch for meeting fixed demands when flexibility is limited (Faia et al., 2024). Since energy communities primarily rely on renewable energy, their operational costs are generally lower than traditional grid tariffs, promoting internal and inter-community energy exchanges, resorting to grid interactions only as a last resort for balancing purposes (Barsanti, 2017). Effective balancing of supply and demand is crucial to optimizing the use of available energy resources and achieving maximum economic benefit (Faia et al., 2024).

To address scalability and flexibility concerns, this paper proposes a distributed multi-agent approach based on the Alternating Direction Method of Multipliers (ADMM). This decentralized method decomposes centralized optimization problems into smaller sub-problems handled by individual agents, allowing parallel computations and significantly enhancing scalability (Chang et al., 2014). Inspired by holonic organizational concepts (Buckhorst et al., 2022), our distributed multi-agent model organizes individual units (holons), including solar panels,

* Corresponding author.
E-mail address: yacine.merrad@lis-lab.fr (Y. Merrad).

https://doi.org/10.1016/j.egyr.2025.11.015
Received 4 July 2025; Received in revised form 27 October 2025; Accepted 9 November 2025
Available online 13 November 2025

Nomenclature

$NGrid$	Number of connected grids
$P^{Grid}_{i,t}, C^{Grid}_{i,t}$	Value and price of exchanged power with the grid
$P^{Grid}_{min}, P^{Grid}_{max}$	Minimum and maximum value of power exchanged with the grid
$NFlex$	Number of flexible participants
$P^{Flex}_{j,t}, C^{Flex}_{j,t}$	Value and price of exchanged power with flex participant j
$Nload$	Number of consumers
$P^{load}_{k,t}, C^{load}_{k,t}$	Value and price of exchanged power with consumer k
$P^{load}_{min}, P^{load}_{max}$	Minimum and maximum load exchanged
NPV	Number of photovoltaic participants
$P^{PV}_{p,t}, C^{PV}_{p,t}$	Value and price of generated PV power
P^{PV}_{max}	Maximum PV power
$NESS$	Number of energy storage systems
$P^{ESS}_{m,t}, C^{ESS}_{m,t}$	Value and price of exchanged power with ESS m
P^{ESS}_{max}	Maximum power of ESS
NW	Number of wind turbines
$P^{W}_{n,t}, C^{W}_{n,t}$	Value and price of generated wind power
P^{W}_{max}	Maximum wind power
SOC	State of charge of energy storage system
OF_j	Objective function of agent j
$OF_{Grid}, OF_{Flex}, OF_{ESS}$	Objective functions of grid, flex, and ESS agents
λ	Relaxation dual parameter
γ	Penalty dual parameter

wind turbines, batteries, and demand response units. Each agent autonomously yet collaboratively responds dynamically to production capacity, storage constraints, demand forecasts, and real-time market prices. Consumer agents specifically focus on minimizing energy costs, while flexible consumer agents proactively adjust consumption according to market signals, optimizing both grid performance and economic outcomes.

However, decentralized optimization inherently involves frequent data exchanges between distributed entities, potentially exposing sensitive operational information and posing significant privacy risks (Liu et al., 2024a). To mitigate these vulnerabilities, our approach incorporates a novel Ring Signature (Yuen et al., 2021) and Multi-Party Computation (Liu et al., 2024b) (RSMPC) privacy scheme. This scheme preserves privacy by ensuring participant anonymity and validating collective inputs without revealing individual identities.

Our proposed framework combines ADMM-based decentralized optimization to resolve scalability issues with RSMPC for robust privacy preservation. Implemented using the Java Agent Development Framework (JADE), our integrated solution leverages ring signatures and data decomposition techniques to ensure computational efficiency and strong privacy guarantees. Extensive simulations demonstrate significant improvements in scalability and privacy for multi-agent energy-sharing environments.

The remainder of this paper is structured as follows: Section 2 provides an overview of the energy trading model studied in this paper, inspired by the VPP4Islands project. Section 3 presents the mathematical formulation and simulation implementation for both centralized and decentralized optimization approaches. Section 4 highlights the privacy concerns inherent in decentralized optimization. Section 5 offers a comprehensive overview of existing privacy-preserving methods and discusses their limitations. Section 6 introduces our proposed privacy preservation method based on RSMPC. Section 7 presents simulation results comparing the scalability of centralized versus decentralized models and evaluates the computational efficiency of our privacy method compared to existing Multi-Party Homomorphic Encryption techniques. Finally, Section VIII concludes the paper, summarizing the key findings and discussing implications and potential directions for future research.

2. Energy trading model overview

This section provides an overview of the energy trading model that will be studied in both centralized and distributed architectures. As a practical case study, we adopt the model inspired by the VPP4Islands European project, specifically the pilot implemented on Formentera Island (VPP4ISLANDS Consortium, 2024a), emphasizing integrating distributed energy resources and local flexibility markets within island communities.

The model comprises two primary actors: the Market Operator (MO) and Energy Communities (ECs). Both actors collaborate to ensure secure, transparent, and efficient energy market operations.

2.1. Market Operator (MO)

The Market Operator (MO) coordinates the energy trading process. Its responsibilities include initializing the trading process, collecting offers and bids from participating ECs, performing market clearing, and issuing dispatch instructions. The MO ensures market compliance and resolves energy trades to maximize social welfare without altering submitted offers and bids (VPP4ISLANDS Consortium, 2024a; Ding et al., 2022).

2.2. Energy Communities (ECs)

Energy Communities (ECs) are composed of prosumers equipped with renewable energy systems, such as solar photovoltaic (PV) installations and battery storage units. Each EC forecasts its energy production, consumption, and anticipated grid electricity prices over a 24-hour period, optimizing internal energy management strategies. This optimization includes scheduling battery usage to maximize economic benefits (VPP4ISLANDS Consortium, 2024a,b). Based on their internal optimization, ECs participate in trading by submitting two types of energy offers and demands:

- **Inflexible Offer and Demand**: Energy volumes that must be traded due to immediate operational constraints. Inflexible demand includes non-adjustable consumption requirements, and inflexible offers represent surplus energy that cannot be stored locally and must be exported (VPP4ISLANDS Consortium, 2024b).
- **Flexible Offer and Demand**: Energy volumes that can be optionally traded. Flexible demand involves additional energy purchases aimed at charging batteries for later use, whereas flexible offers denote surplus energy that may either be traded or stored locally based on economic considerations (VPP4ISLANDS Consortium, 2024b).

2.3. Concept architecture

The energy-sharing architectures studied in this paper are categorized into centralized and distributed architectures.

2.3.1. Centralized architecture

In the centralized architecture, each community consists of various Distributed Energy Resources (DERs), including renewable production sources, storage units, and consumers. The Market Operator optimizes power distribution and pricing, ensuring fair transactions and maximizing societal welfare. Buyers and sellers submit offers and bids, while the MO schedules power distribution and sets community clearing prices based on these interactions. This model facilitates efficient power distribution and promotes renewable energy integration (Ahmed et al., 2024) (See Fig. 1).

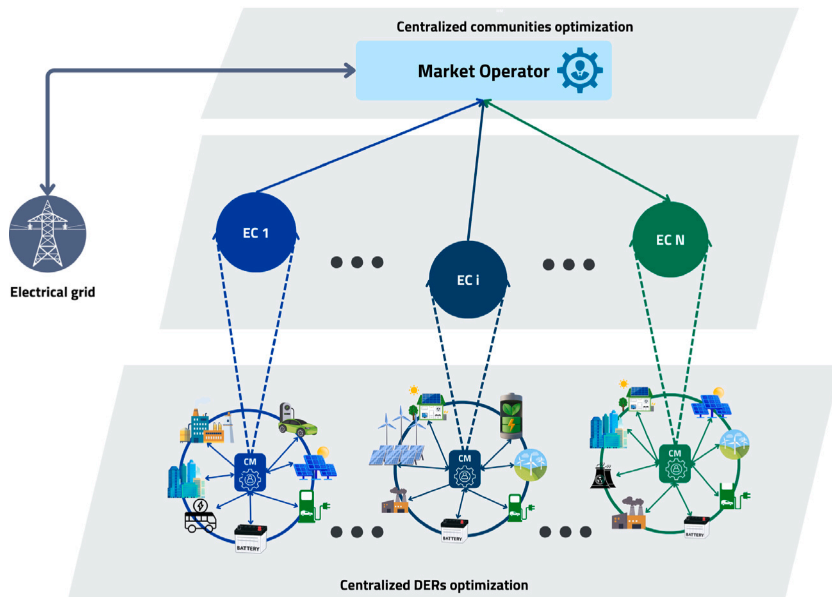

Fig. 1. P2P Centralized architecture.

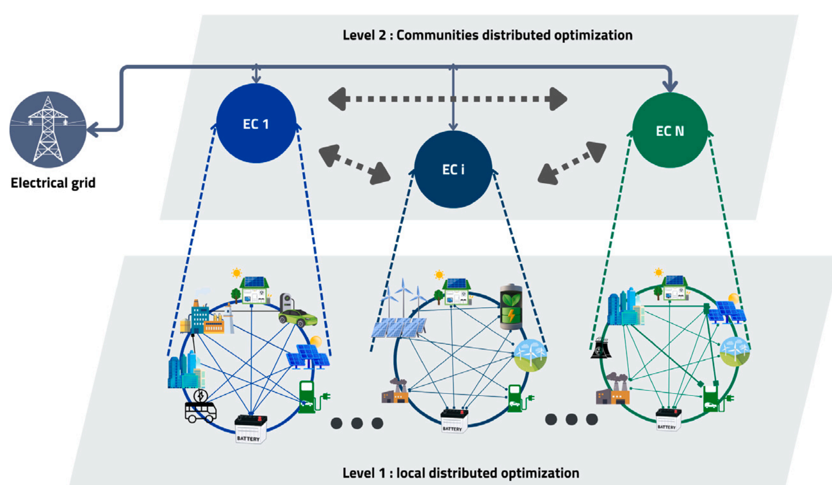

Fig. 2. P2P Distributed MAS architecture.

2.3.2. Distributed architecture: The holonic multi-agent system model

The distributed architecture utilizes a holonic multi-agent system (Buckhorst et al., 2022), where individual units (holons) function autonomously and as part of a larger system. Energy resources, including solar panels, wind turbines, batteries, and demand response units, act as holons represented by agents. These agents autonomously operate within specific environments and dynamically respond to production capacities, storage limitations, demand forecasts, and market prices (VPP4ISLANDS Consortium, 2024a,b; Heydarian-Forushani et al., 2023). Communities exchange energy production and consumption data with the MO, which ensures fair and optimal resource distribution (Ahmed et al., 2024).

In this distributed model, agents optimize profits and system constraints, with consumer agents minimizing costs and flexible consumer agents dynamically adjusting consumption based on market signals. Renewable energy agents maximize resource utilization and promote sustainability by responding to market and environmental conditions, creating a dynamic and efficient energy management system aligned with contemporary grid requirements (see Fig. 2).

3. Mathematical formulation and simulation

3.1. Energy trading centralized architecture

In this section, we present the centralized mathematical formulation of the proposed energy trading model. We adopt a two-tier centralized optimization architecture aimed at enhancing the efficiency of energy distribution and trading. The first level focuses on local optimization within each energy community, managing the allocation of distributed energy resources (DERs) and defining strategic bids and offers to be submitted to the market operator. The second level addresses cross-community optimization, coordinating energy exchanges between communities to clear the market, achieve global optimality and maximize social welfare.

3.1.1. Community-centric optimization

In this phase of centralized EC optimization, energy coordination across DERs is managed by assessing community needs and surpluses. It prioritizes renewable scheduling by balancing variable PV and wind generation using predictive data, with allowances for potential derating. Accordingly, renewable assets are incorporated into the objective function detailed in (1). The community aggregator efficiently manages flexible loads and energy storage systems (ESS) to align with renewable availability, enhancing system responsiveness and sustainability.

$$\begin{aligned} OF = \min \sum_{t=1}^{T} \Bigg[& P_t^{Deficit} * C_t^{Deficit} + \sum_{j=1}^{NFlex} P_{j,t}^{Flex} * C_{j,t}^{Flex} \\ & - P_t^{Excess} * C_t^{Excess} - \sum_{m=1}^{NESS} P_{m,t}^{ESS} * C_{m,t}^{ESS} \\ & - \sum_{p=1}^{NPV} P_{p,t}^{PV} * C_{p,t}^{PV} - \sum_{n=1}^{NW} P_{n,t}^{W} * C_{n,t}^{W} \Bigg] \end{aligned} \tag{1}$$

The objective function seeks to maximize overall energy cost efficiency within the energy community by minimizing power dependency from the grid, represented by $P^{Deficit}$, reducing reliance on demand response represented by load flexibility, and maximizing the utilization of renewable resources.

The optimization process must comply with following constraints to ensure feasibility:

$$\begin{aligned} & P_t^{Excess} + \sum_{k=1}^{Nload} P_{k,t}^{load} - \sum_{p=1}^{NPV} P_{p,t}^{PV} - \sum_{m=1}^{NESS} P_{m,t}^{ESS} \\ & \quad - P_t^{Deficit} - \sum_{n=1}^{NW} P_{n,t}^{W} - \sum_{j=1}^{NFlex} P_{j,t}^{Flex} = 0 \end{aligned} \tag{2}$$

$$0 \le P_t^{Excess} \le P_{max}^{Grid} \tag{3}$$

$$0 \le P_t^{Deficit} \le P_{max}^{Grid} \tag{4}$$

$$P_{min}^{load} \le P_{k,t}^{load} \le P_{max}^{load} \tag{5}$$

$$P_{min}^{W} \le P_{n,t}^{W} \le P_{max}^{W} \tag{6}$$

$$P_{min}^{Pv} \le P_{p,t}^{PV} \le P_{max}^{Pv} \tag{7}$$

$$0 \le P_{j,t}^{Flex} \le \alpha * P_{max}^{load} \qquad with \qquad 0.2 \le \alpha \le 0.5 \tag{8}$$

$$SOC_{i,t} = SOC_{i,(t-1)} - \frac{P_{i,(t-1)}^{ESS}}{P_{max}^{ESS}} \tag{9}$$

$$SOC_{min} \le SOC_{i,t} \le SOC_{max} \tag{10}$$

The equations presented establish a comprehensive framework for managing energy resources within an energy system, ensuring efficient energy balance and resource optimization. Eq. (2) defines the energy balance for each time period t, stating that the excess power P_t^{Excess}, along with the total load $\sum_{k=1}^{Nload} P_{k,t}^{load}$, must equal the combined generation from renewable sources, including photovoltaic (PV) and wind energy, as well as stored energy (ESS), while accounting for any deficits $P_t^{Deficit}$ and flexible power contributions. Eqs. (3) and (4) impose constraints on both excess and deficit power to remain within the maximum grid capacity P_{max}^{Grid}. Furthermore, each element — load power $P_{k,t}^{load}$, wind power $P_{n,t}^{W}$, solar power $P_{p,t}^{PV}$, and flexible power $P_{j,t}^{Flex}$ — must be restricted within its defined limitations to ensure a balanced and efficient energy system. Additionally, Eqs. (9) and (10) manage the state of charge (SOC) of energy storage systems, ensuring that SOC remains within specified limits while updating based on energy discharged.

Once data from various renewable energy resources (RERs) is collected, each community aggregator (CA) performs an internal optimization to meet the needs of its participants. After this optimization, each CA calculates its bids, classifying them into flexible and inflexible demands and offers. See Fig. 3, which illustrates two scenarios explaining inflexible and flexible demands and offers.

$$D_i^{flex} = min((SOC_i - SOC_{min})P_{max}^{ESS}, 0) \tag{11}$$

$$D_i^{inflex} = P^{Deficit} \tag{12}$$

$$O_i^{flex} = min((SOC_{max} - SOC_i)P_{max}^{ESS}, 0) \tag{13}$$

$$O_i^{inflex} = P^{Excess} \tag{14}$$

3.1.2. Market clearing and social welfare maximization

The market operator receives bids from various community aggregators (CAs) and performs an optimization described by the objective function (15). This function is designed to maximize social welfare by balancing energy exchanges among the CAs. The optimization process involves minimizing the overall costs associated with the power exchanged with the grid, represented by P^G, while also considering the flexible offers and flexible demands. By evaluating these components, the market operator aims to facilitate efficient transactions among communities. Additionally, the equation incorporates a mechanism to engage with the main grid, ensuring that there is always a solution available in cases where internal community exchanges may not suffice to meet energy needs.

$$\begin{aligned} OF_{c-P2P} = & \min P^G(t) \cdot C^G(t) \\ & + \sum_{i=1}^{N} \sum_{t=1}^{T} \left[O_i^{flex}(t) \cdot C_i^{flex}(t) - D_i^{flex}(t) \cdot C_i^{flex}(t) \right] \end{aligned} \tag{15}$$

$\forall i \in [1, \dots, N], \quad \forall t \in [1, \dots, T]$

The energy balance constraint ensures that the total energy offered by community aggregators (CAs) and the power sold to the grid equals the total energy demanded by the CAs and the power purchased from the grid, expressed as:

$$\begin{aligned} P_i^G(t) = & \sum_{i=1}^{N} \sum_{t=1}^{T} \left(D_i^{flex}(t) + D_i^{inflex}(t) \right) \\ & - \sum_{i=1}^{N} \sum_{t=1}^{T} \left(O_i^{flex}(t) + O_i^{inflex}(t) \right) \end{aligned} \tag{16}$$

Boundary constraints are imposed to maintain feasible limits on energy production and consumption:

$$0 \le O_i^{flex}(t) \le O_{max}^{flex} \tag{17}$$

$$0 \le O_i^{inflex}(t) \le O_{max}^{flex} \tag{18}$$

$$0 \le P^{Gsell}(t) \le P_{max}^{Gsell} \tag{19}$$

$$0 \le D_i^{flex}(t) \le D_{max}^{flex} \tag{20}$$

$$0 \le D_i^{inflex}(t) \le D_{max}^{flex} \tag{21}$$

$$0 \le P^G(t) \le P_{max}^G \tag{22}$$

The optimal allocations are iteratively reached, followed by calculating a market-clearing price by determining the highest bid among participants. The CM then communicates these results, including optimized allocations and prices, ensuring transparency and fairness in the centralized P2P energy trading system.

$$C_{clearing-market} = Max(Scheduled\ sources) \tag{23}$$

The operating algorithm is shown as follow:

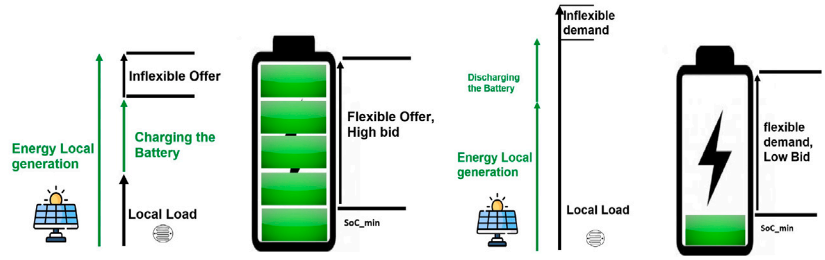

Fig. 3. Examples Illustrating Flexible and Inflexible Demand and Supply Scenarios.

Algorithm 1 Centralized Energy Trading Algorithm

```
**Initialization:**
Collect data from N communities: D_i^{flex}, D_i^{inflex}, O_i^{flex}, O_i^{inflex} for each i ∈ [1, ..., N]
**Main Loop:**
for j = 1, ..., T do
    Calculate objective function (Eq. (15))
    Check boundary and balance constraints (Eqs. (17) to (22))
    if Balance constraints are satisfied then
        Calculate clearing price (Eq. (23))
        Break the loop
    end if
end for
```

3.2. The holonic multi-agent system model

In energy communities, a multi-agent system facilitates efficient energy management by enabling decentralized decision-making and collaboration among various stakeholders (Lowitzsch et al., 2020). Each agent, equipped with hardware and software, communicates with a centralized data server that provides real-time information, allowing for localized optimizations. This setup fosters dynamic interactions among agents, ensuring that energy resources are allocated effectively to meet demand while maximizing economic returns. Agents utilize the Alternating Direction Method of Multipliers (ADMM) algorithm (Chang et al., 2014), as outlined in Eq. (24), to predict market conditions and improve revenue from energy transactions. Effective constraint management, governed by Eqs. (3) to (8), ensures compliance with storage capacities, local demand, and grid balance (Eq. (2)).

The general form of the objective function for each agent j is defined as follows:

$$OF_j = Max \sum_{t=1}^{T} P_j^{v}(t) * C_j^{v}(t) + \lambda^{(v-1)} * P_j^{v}(t) + \frac{\gamma}{2} * \| \sum_{k=1,k\neq j}^{M} P_k^{(v-1)}(t) - P_j^{(v)}(t) \|^2 \tag{24}$$

The procedure for updating the λ parameter is as follows:

$$\lambda^{(v)} = \lambda^{(v-1)} + \gamma * [\sum_{k=1,k\neq j}^{M} P_k^{(v-1)}(t) - P_j^{(v)}(t)] \tag{25}$$

In this context, v denotes the iteration number. Each iteration involves solving individual subproblems and updating the dual variable until convergence is achieved.

The primal residual at iteration v for agent j, denoted $r_j^{(v)}$, represents the local balance (consensus) violation that drives the dual update; it is defined in (26). The dual residual at iteration v for agent j, denoted $s_j^{(v)}$, measures the γ-scaled change of that violation between successive iterations; it is defined in (27). Convergence is declared when both residuals satisfy the stopping test in (28). At convergence, feasibility is attained and thus, the augmented quadratic penalty term *vanishes* as stated in (29).

$$r_j^{(v)} = \sum_{\substack{k=1 \\ k\neq j}}^{M} P_k^{(v-1)}(t) - P_j^{(v)}(t), \qquad \lambda^{(v)} = \lambda^{(v-1)} + \gamma\, r_j^{(v)}, \tag{26}$$

$$s_j^{(v)} \triangleq \gamma\left(r_j^{(v)} - r_j^{(v-1)}\right), \tag{27}$$

$$\left\|r_j^{(v)}\right\|_2 \le \varepsilon_{\text{pri}} \quad \text{and} \quad \left\|s_j^{(v)}\right\|_2 \le \varepsilon_{\text{dual}}, \tag{28}$$

$$\frac{\gamma}{2}\left\|r_j^{(v)}\right\|_2^2 \longrightarrow 0 \quad \text{as} \quad v \to \infty. \tag{29}$$

Renewable energy generation is inherently uncertain due to its dependence on location-specific factors such as climate and weather patterns, which significantly impact the predictability and management of resources like solar and wind energy. Therefore, advanced forecasting models are crucial, utilizing historical and real-time weather data to estimate energy production accurately. Similarly, user consumption patterns are unpredictable, relying on projections based on past consumption data, which can vary due to changes in user behavior and unexpected events. To effectively manage these uncertainties, the model incorporates flexible agents: flexible consumption, and batteries. These agents work together to help maintain system balance and enhance overall reliability. For energy communities to operate optimally, a centralized database is employed for efficient information exchange among distributed agents. This database consolidates crucial data for each agent, identified by unique names and IP addresses, and provides access to historical energy quantities, pricing data, and renewable resource forecasts. These data points empower agents to make informed and strategic decisions.

During each iteration, agents update their optimized values and retrieve data from one another, maintaining a continuous cycle of information exchange. This iterative data sharing enables agents to respond dynamically to system changes, enhancing the overall efficiency and stability of the energy communities. Considering the N communities examined in the previous section, the information exchanges between two communities, i and j ($\forall i, j \in [1, \dots, N]$ *and* $i \neq j, N$), are structured as follows:

- From community i to the supervisor:

$$\left[D_i^{(v),\text{flex}}, C_i^{(v),\text{flex}}, O_i^{(v),\text{flex}},\ D_i^{(v),\text{inflex}}, C_i^{(v),\text{inflex}}, O_i^{(v),\text{inflex}}\right] \tag{30}$$

- From the supervisor to community i:

$$\begin{bmatrix} D_j^{(v-1),\text{flex}} & D_{j+1}^{(v-1),\text{flex}} & \dots & D_N^{(v-1),\text{flex}} \\ C_j^{(v-1),\text{flex}} & C_{j+1}^{(v-1),\text{flex}} & \dots & C_N^{(v-1),\text{flex}} \\ O_j^{(v-1),\text{flex}} & O_{j+1}^{(v-1),\text{flex}} & \dots & O_N^{(v-1),\text{flex}} \\ D_j^{(v-1),\text{inflex}} & D_{j+1}^{(v-1),\text{inflex}} & \dots & D_N^{(v-1),\text{inflex}} \\ C_j^{(v-1),\text{inflex}} & C_{j+1}^{(v-1),\text{inflex}} & \dots & C_N^{(v-1),\text{inflex}} \\ O_j^{(v-1),\text{inflex}} & O_{j+1}^{(v-1),\text{inflex}} & \dots & O_N^{(v-1),\text{inflex}} \end{bmatrix} \tag{31}$$

and the grid information:

$$\left[P^{(v),G_{\text{buy}}}, C^{(v),G_{\text{buy}}}, C^{(v),G_{\text{sell}}}, P^{(v),G_{\text{sell}}}\right] \tag{32}$$

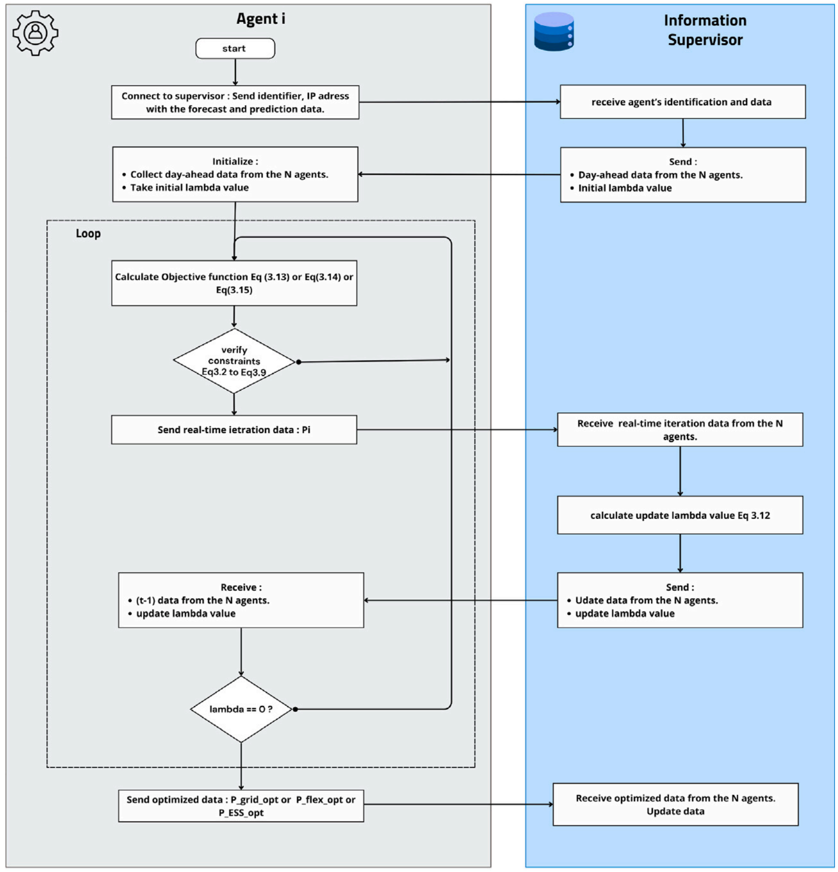

Fig. 4. Flowchart MAS.

This flow of information is illustrated in Fig. 4, which shows the flow chart of data exchange between agent j and the information supervisor.

For each agent, we consider controllable parameters such as flexible energy demands or supplies, and the energy exchanged with the electrical grid as variables to be optimized in our mathematical model. All other energy forms are treated as external data that are shared among the various communities. Consequently, the objective function (33) is defined as follows :

$$\begin{aligned}
OF_{i-decen-P2P} \;=\; & \min \sum_{i=1}^{N}\sum_{t=1}^{T}\Big[O_i^{v,flex}(t)\cdot C_i^{v,flex}(t) \\
& + P_i^{v,G}(t)\cdot C_i^{v,G}(t) - D_i^{v,flex}(t)\cdot C_i^{v,flex}(t)\Big] \\
& - \lambda^{v-1}\Big[\big(O_i^{v,flex}(t) + O_i^{v,inflex}(t) + P_i^{v,G}(t)\big) \\
& - \big(D_i^{v,flex}(t) + D_i^{v,inflex}(t)\big)\Big] \\
& + \frac{\gamma}{2}\cdot\Big\| \sum_{j=1,j\neq i}^{N}\big(O_i^{v,flex}(t) + O_j^{(v-1),flex}(t) \\
& + O_j^{(v-1),inflex}(t) + O_i^{v,inflex}(t) + P_i^{v,G}(t)\big) \\
& - \big(D_i^{v,flex}(t) + D_j^{(v-1),flex}(t) + D_i^{v,inflex}(t) \\
& + D_j^{(v-1),inflex}(t)\big)\Big\|^2
\end{aligned} \tag{33}$$

The supervisory level updates the dual parameter according to the following equation:

$$\lambda^{v} = \lambda^{(v-1)} + \gamma\sum_{i=1}^{N}\Big[O_i^{v,flex} + O_i^{v,inflex} + P_i^{v,G} - \big(D_i^{v,flex} + D_i^{v,inflex}\big)\Big] \tag{34}$$

By structuring the objective function in this way, a robust framework is established that enables each agent to optimize its operations independently while preserving system-wide coherence and stability. This approach not only promotes efficient local decision-making but also ensures that the collective actions of all agents contribute to a balanced and optimal state across the entire network.

The following algorithm outlines the steps in the operation of the Multi-Agent System (MAS).

Algorithm 2 Distributed P2P Trading

1. **Connect to Supervisor:** Send identifier, IP address, forecast, and prediction data [Eq. (30)]
2. **Initialize:**
   (a) Exchange day-ahead predicted data [Eq. (31), (32)]
   (b) Set initial values for λ and γ
3. **Loop:** For each time step $j \in [1,\ldots,T]$:
   (a) Calculate the objective function [Eq. (33)]
   (b) Verify boundary and balance constraints [Eqs. (17) to (22)]
   (c) Send real-time iteration data to supervisor
   (d) Receive updated values:
      - Iteration $(j-1)$ data from N agents
      - Updated λ and γ values [Eq. (34)]
4. **Check Convergence:** If λ and γ converge to zero
5. **Output:** Send optimized values to Market Operator (MO)

The optimization process begins with each agent sharing its identifier and forecast data with a supervisor, enabling data exchange across connected communities. Each agent then iteratively calculates its objective function and sends results to the supervisor, who updates the dual variable (λ) and integrates data from all agents to maintain

Table 1
Decentralized optimization: Generators, constraints, and costs.

Generator	Constraints	Cost function
1	$10 \le P_1 \le 50$	$f_1(P_1) = 25\,P_1$
2	$10 \le P_2 \le 20$	$f_2(P_2) = 20\,P_2$
3	$10 \le P_3 \le 30$	$f_3(P_3) = 10\,P_3$

coordination. This iterative exchange ensures agents optimize based on both local and shared data, aligning their efforts toward system-wide goals. The process continues until convergence, resulting in a balanced and efficient decentralized energy trading system that benefits all agents through coordinated optimization.

3.3. Case study and simulation setup

This section describes the case study and simulation framework used to evaluate the proposed peer-to-peer (P2P) energy trading models. The simulated scenario comprises two interconnected energy communities, each consisting of distributed energy resources (DERs) such as solar photovoltaic (PV) systems, wind turbines, battery storage units, and demand response capabilities. These communities are connected to an external power grid, enabling energy exchanges both within and between communities.

Both centralized and distributed energy trading architectures are explored. In the centralized approach, a single Market Operator (MO) manages all transactions, optimization decisions, and resource allocation. The MO collects energy offers and bids from each community, performs centralized market clearing, and issues dispatch instructions accordingly, ensuring the optimization of resources and maximal societal welfare.

In contrast, the distributed architecture employs a Holonic Multi-Agent System (MAS), where each energy resource and community functions autonomously yet collaboratively. Individual agents represent various DERs, making local decisions based on factors such as forecasted energy generation, storage capacity constraints, anticipated energy demands, and real-time market conditions. This decentralized coordination is implemented using the Java Agent DEvelopment Framework (JADE), chosen for its robustness in modeling multi-agent systems and facilitating scalable inter-agent communication. Optimization within this framework utilizes the Gurobi solver, known for efficiently handling complex mathematical computations.

The case study scenario was carefully designed to reflect realistic energy trading dynamics, emphasizing interactions among different types of agents, their operational constraints, and the impact of decentralized versus centralized decision-making. The simulations enabled detailed analysis of energy exchanges, resource management strategies, and the efficacy of each architecture under consistent environmental and operational conditions.

3.4. Privacy issues of the decentralized optimization used in the holonic multi-agent

Decentralized optimization used in the holonic multi-Agent system Model, involves multiple agents collaboratively solving optimization problems while aiming to keep their individual data private (Huo and Liu, 2021). Privacy preservation in such systems is challenging due to the decentralized nature of the data and computation (Huo and Liu, 2021; Yue et al., 2025). Fig. 5 presents a flowchart illustrating the overall process of decentralized optimization.

To demonstrate the privacy issues in decentralized market clearing we use the example three generators (indexed by 1, 2, and 3), each with its own decision variable P_i and local cost function $f_i(\cdot)$. They must meet a total demand D, subject to individual constraints. Table 1 summarizes the setup.

Table 2
Final iteration for different demands.

Demand	Iteration	P_1	P_2	P_3	λ
35	11	10.0	10.0	15.0	10.0
55	13	10.0	15.0	30.0	20.0
65	12	15.0	20.0	30.0	25.0
70	9	20.0	20.0	30.0	25.0

They collectively meet demand D, i.e.,

$$P_1 + P_2 + P_3 = D.$$

Each generator's local objective also includes a term penalizing deviation from the current estimate of the demand shortfall, e.g., for generator 1:

$$f_1(P_1) - \lambda P_1 + 0.1\left(D - P_1 - P_2^{(f)} - P_3^{(f)}\right)^2,$$

where λ is a Lagrange multiplier and $P_2^{(f)}, P_3^{(f)}$ are the most recent values from the previous iteration. Similar expressions apply to generators 2 and 3.

We vary the demand D and run the iterative procedure until convergence. Originally, the results for $D = 35, 55, 65$, and 70 were shown in four separate tables. Below, we show only the *final* iteration for each demand in one combined table (Table 2).

From the results presented in Table 2, we observe that as D increases from 35 to 55, both P_2 and P_3 increase their generation, while P_1 remains unchanged. This suggests that P_1 is operating at its minimum generation level, which is 10, and that the Lagrange multiplier value of 10 corresponds to its marginal cost. Furthermore, when P_2 begins to increase its generation, we can infer that it was previously constrained at its lower limit. Additionally, from the observed changes in power generation, we can deduce that the upper generation limits for P_2 and P_3 are 20 and 30, respectively.

4. Existing privacy-preserving methods

We examine two primary methods: differential privacy and multi-key homomorphic encryption.

4.1. Differential Privacy

Differential Privacy (DP) (Yang et al., 2024) involves adding noise to the data or queries to mask the contribution of individuals. While effective in preserving privacy, DP introduces a trade-off between privacy and accuracy, potentially degrading the utility of the data (Kim et al., 2021).

Differential privacy is mathematically defined by a privacy parameter ϵ, which quantifies the privacy level. The function's sensitivity, which measures the maximum change in output by altering a single individual's data, guides the noise scale.

Sensitivity and noise addition. The sensitivity Δf of a function f is defined as:

$$\Delta f = \max_{D_1, D_2} \|f(D_1) - f(D_2)\|_1 \tag{35}$$

where D_1 and D_2 are datasets differing by one element. Noise is typically added from a Laplace distribution as:

$$\mathrm{Lap}(x|\lambda) = \frac{1}{2\lambda} e^{-\frac{|x|}{\lambda}} \tag{36}$$

where $\lambda = \frac{\Delta f}{\epsilon}$.

The differential privacy guarantee is expressed as:

$$\Pr[f(D_1) + \text{noise} \in S] \le e^{\epsilon} \Pr[f(D_2) + \text{noise} \in S] \tag{37}$$

for any output set S, ensuring indistinguishability between the datasets D_1 and D_2.

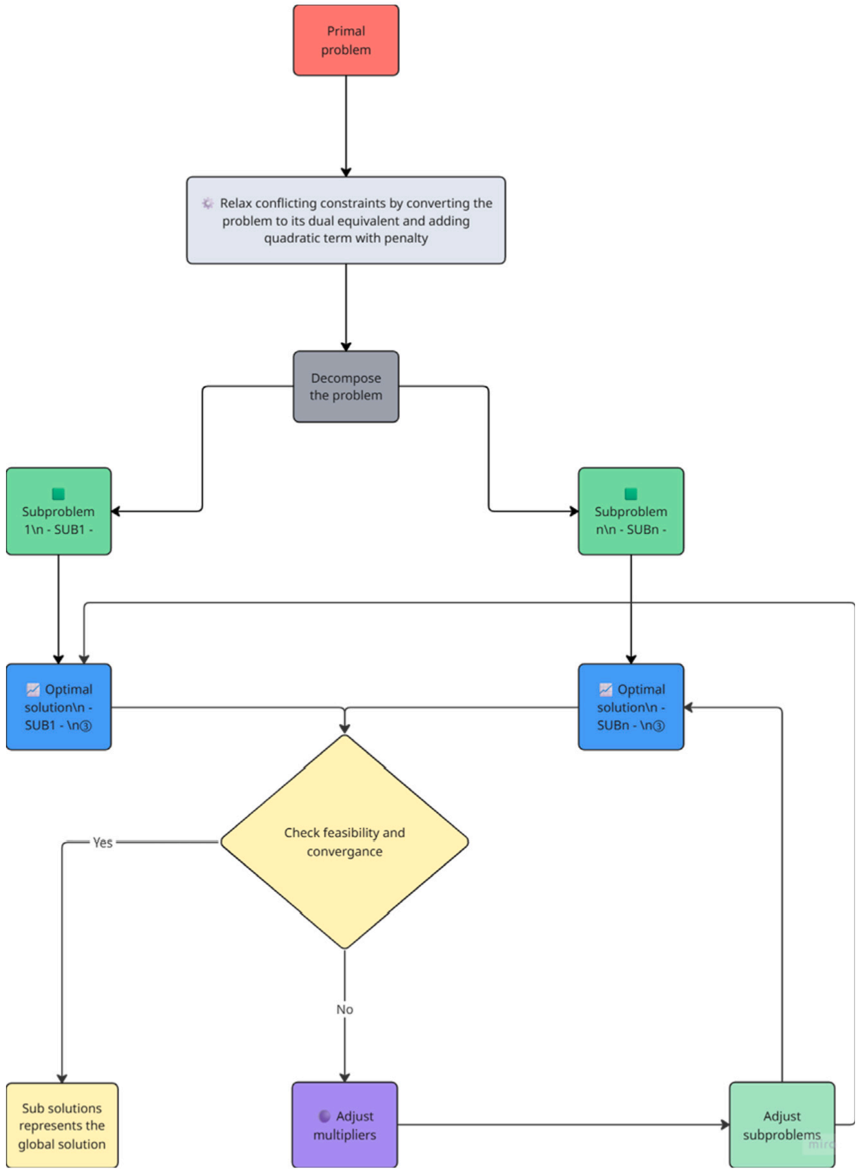

Fig. 5. Decentralized optimization flowchart.

another well-known challenges of differential privacy is Cumulative Noise Addition. When multiple queries are made on the same dataset, noise accumulates, leading to further degradation of accuracy (Dwork et al., 2010).

4.2. Multi-key Homomorphic Encryption

Multi-key Homomorphic Encryption (MKHE) (Chen et al., 2019) allows computations on encrypted data from multiple users. Despite its robust security, MKHE suffers from high computational overhead and long execution times, making it impractical for real-time applications (Ma et al., 2022).

While there are several MK-FHE approaches, a general outline is:

4.2.1. Key generation

Each user i samples a secret key sk_i and produces a corresponding public key pk_i:

$$(\mathsf{pk}_i, \mathsf{sk}_i) \leftarrow \mathsf{KeyGen}(\text{params}).$$

These keys are published or shared so that encryptors and evaluators have the public keys, while each user holds their own private key.

4.2.2. Encryption

To encrypt a message m (e.g., an integer or polynomial):

$$ct_i \leftarrow \mathsf{Enc}(\mathsf{pk}_i, m),$$

which produces a ciphertext ct_i under the ith user's key. If multiple users encrypt data for a joint computation, we get $\{ct_1, ct_2, \ldots, ct_n\}$.

4.2.3. Evaluation

In an MK-FHE scheme, there is typically a *re-linearization* or *key-switching* procedure that transforms ciphertexts under multiple keys into a form decryptable by a single "aggregated" or "combined" key. Hence, an evaluation might look like:

$$ct_{\text{out}} \leftarrow \mathsf{Eval}\big(\{\mathsf{pk}_i\}, f, ct_1, ct_2, \ldots, ct_n\big).$$

The function f can be any polynomial-sized circuit. The output ct_{out} is a *multi-key ciphertext* associated with all $\{\mathsf{pk}_i\}$.

4.2.4. Partial decryption and combination

To decrypt ct_{out}, each user i may perform a *partial decryption*:

$$pd_i \leftarrow \mathsf{PartialDec}(\mathsf{sk}_i, ct_{\text{out}}),$$

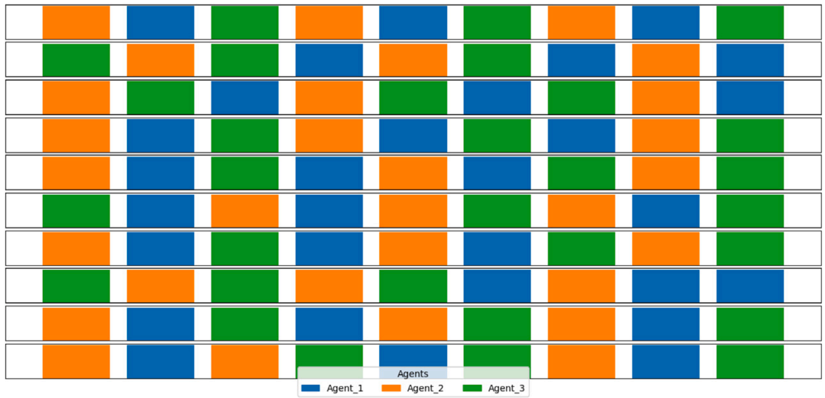

Fig. 6. Visualization of randomized data transmission by three agents.

resulting in a partial decryption share pd_i. A final Combine algorithm aggregates these shares:

$$m_{\text{out}} \leftarrow \text{Combine}(pd_1, pd_2, \ldots, pd_n).$$

This final step recovers the plaintext m_{out} if all (or a threshold of) users collaborate. No single user learns others' private keys, yet correctness is guaranteed.

5. Proposed RSMPC privacy scheme

Our method introduces a hybrid approach utilizing ring signatures and data decomposition to preserve privacy while maintaining computational efficiency. This approach does not rely on the addition of noise (as in DP) and is computationally less intensive than MKHE.

Our privacy model leverages a decentralized cryptographic protocol that allows each agent to participate in the computation without revealing their individual data. The model ensures that only aggregated, non-identifiable information is exposed during computations. The method addresses privacy concerns in decentralized economic dispatch by proposing a method that leverages ring signatures and data decomposition. While each generator independently solves its local subproblem, the overall method ensures that the central coordinator receives aggregate information without compromising individual agents' private generation data or demand profiles. We illustrate how ring signatures and data decomposition provide anonymity, protect sensitive operational parameters, and allow iterative dispatch and market clearing to converge accurately. We propose a privacy scheme that employs *ring signatures* and *data decomposition*. The goal is to ensure that, although each generator shares information needed for iterative updates, their private generation data remain anonymous to the central coordinator and between the agents.

The steps involved in the proposed method are:

- **Decomposition:** Each agent g decomposes data that need to be sent to the central coordinator into parts. For example, the total demand D_g is split into parts $D_g^{(1)}, D_g^{(2)}$ such that $D_g = D_g^{(1)} + D_g^{(2)}$. Each part is transmitted separately.
- **Randomized Transmission:** To conceal patterns, these parts are sent in a random sequence and with random delays. Each agent transmits three data packages using a randomized strategy. As shown in Fig. 6, the reception sequence lacks recognizable patterns. Each agent is simulated on a separate thread using a multithreaded approach.
- **Ring Signatures:** Each transmitted part is signed using a ring signature to anonymize the sender. The signature proves that a legitimate participant from the ring signed it without revealing which one.
- **Iterative Process & Convergence:** The coordinator updates the Lagrange multiplier:

$$\lambda^{(v+1)} = \lambda^{(v)} + \alpha \left(D - \sum_{g=1}^{N} p_g^{(v)} \right), \tag{38}$$

and distributes it back. The process repeats until convergence: $\sum_{g=1}^{N} p_g = D$.

The cryptographic framework combines ring signatures for anonymity with data decomposition techniques to minimize data exposure. This combination ensures that individual contributions are masked, yet allows for the computation of collective results without reconstructing individual inputs. The method is illustrated in the flowchart in Fig. 7.

We implemented a prototype of our proposed system and evaluated its performance primarily in terms of computational overhead. Furthermore, we conducted a comparative performance analysis against the Multi-Key Fully Homomorphic Encryption (MKFHE) schemes presented by Xu et al. in Xu et al. (2023), specifically focusing on computational overhead to highlight the efficiency improvements of our approach.

6. Results

6.1. Scalability analysis

To quantify scalability, we simulated both models with community sizes ranging from 10 to 1,000. As shown in Fig. 10, centralized systems experience a non-linear scalability curve. Initially, performance improves with increasing participants, but eventually plateaus and declines due to computational saturation at the coordinator. In contrast, the distributed model (Fig. 11) scales more gracefully, with parallel agent-based operations balancing the computational load. Despite a slight drop in scalability growth rate at higher community counts, the distributed system sustains better performance and latency metrics, thanks to localized computation and reduced data centralization. The optimal solutions obtained through the distributed method are consistent with those produced by the centralized approach. Any observed deviations between the two are negligible and arise solely due to the convergence tolerance settings used in the distributed ADMM solver. results have now been clearly illustrated in Figs. 8 and 9 respectively.

6.2. Privacy scheme performance and suitability

We also evaluated the performance of our proposed privacy-preserving communication scheme compared to existing multi-key fully homomorphic encryption (MKFHE) methods. In a simulated environment, we ran 10 agents on dedicated threads. Each agent split its encrypted data into two independent packages. The average time for

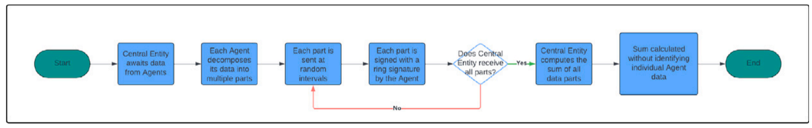

Fig. 7. Flowchart illustrating the proposed RSMPC privacy scheme.

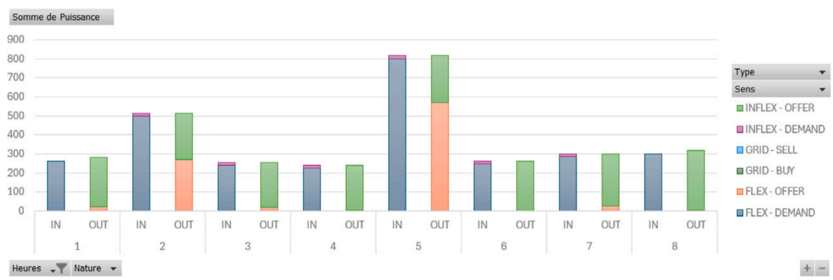

Fig. 8. Simulation result of the centralized trading model use case.

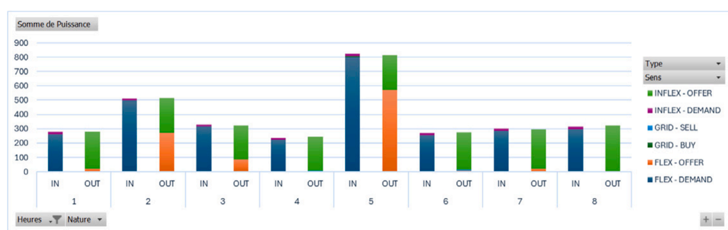

Fig. 9. Simulation results of the distributed trading model use case.

Table 3
Comparison of time overheads for proposed vs. MKFHE methods.

Method	# Agents	Time overhead (ms)
Proposed	3	1.8
Proposed	10	53
Proposed	16	87
MK-TFHE (Xu et al., 2023)	3	698
MK-TFHE (Kwak et al., 2024)	10	15 170
MK-TFHE (Kwak et al., 2024)	16	24 720

the central coordinator to receive and decrypt both packages was measured and compared against MKFHE schemes in both 3, 10 and 16 agents setting (see Table 3).

These results demonstrate that our package-based privacy-preserving scheme is well-suited for distributed optimization. Unlike MKFHE methods designed for centralized or limited-party computation, our approach aligns with the distributed model's architecture, offering lightweight, scalable, and secure communication. Its efficiency in execution time makes it more adaptable to real-time multi-agent environments where responsiveness is critical.

This lighter footprint also makes trustless on-chain coordination feasible, lower computational complexity reduces gas and fits within block-gas limits, so a smart contract (Zarir et al., 2021) can act as the autonomous coordinator while preserving transparency and privacy.

7. Conclusion

This paper introduced a novel privacy-preserving decentralized energy trading framework between energy communities, combining the scalability of ADMM-based optimization with the anonymity and data integrity of Ring Signature Multi-Party Computation (RSMPC). Our architecture addresses key challenges in community energy exchanges, including the need for distributed control, agent-level privacy, and real-time responsiveness.

Through comprehensive simulations, we demonstrated that decentralized optimization via a holonic multi-agent system significantly improves scalability over centralized models, particularly as the number of participants grows. Furthermore, the proposed communication protocol outperforms conventional Multi-Key Fully Homomorphic Encryption (MKFHE) methods in terms of computational efficiency and execution time, making it suitable for real-time deployment. The randomness in data packet reception further strengthens privacy by preventing traffic analysis and inference attacks.

Our results validate that this integrated approach offers a robust, secure, and scalable solution for energy trading between communities in future smart grid infrastructures.

CRediT authorship contribution statement

Wafa Nafkha Tayari: Writing – original draft, Visualization, Validation, Software, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Yacine Merrad:** Writing – original draft, Visualization, Validation, Software, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Seifeddine Ben Elghali:** Writing – review & editing, Validation, Supervision, Resources, Project administration, Methodology, Funding acquisition. **Mohamed Benbouzid:** Writing – review & editing, Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This work has been carried out within the framework of the European Union's Horizon Europe research and innovation programme under Grant Agreements No. 101096946 (FlexCHESS) and No. 101096836 (MASTERPIECE).

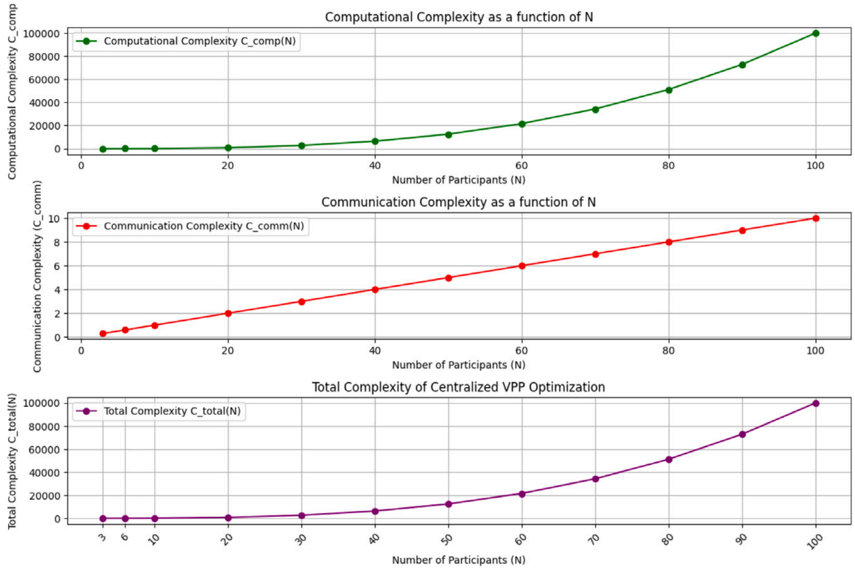

Fig. 10. Scalability of centralized P2P market trading.

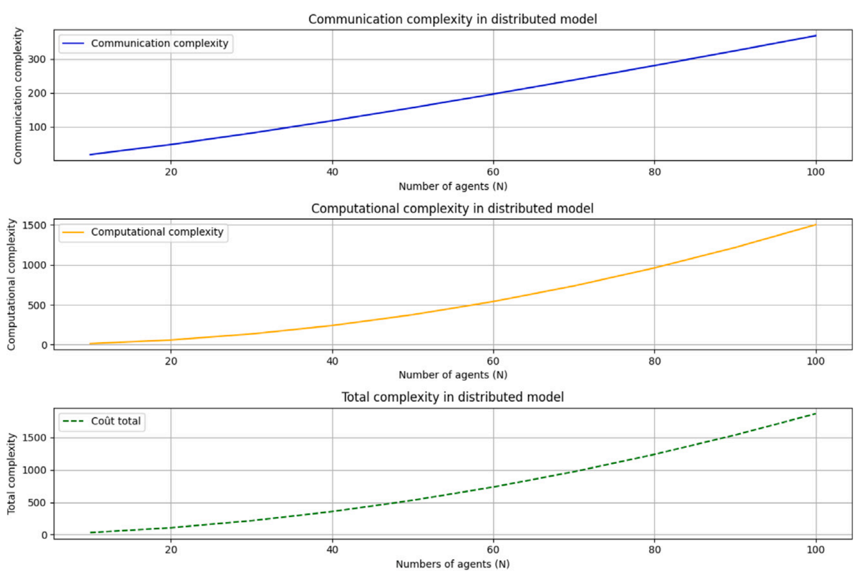

Fig. 11. Scalability of Distributed model.

Data availability

The authors do not have permission to share data.

References

Ahmed, S., Ali, A., D'angola, A., 2024. A review of renewable energy communities: concepts, scope, progress, challenges, and recommendations. Sustainability 16 (5), 1749.

Barsanti, M., 2017. Optimized home energy management system in prosumers networks. To be completed.

Buckhorst, A.F., Grahn, L., Schmitt, R.H., 2022. Decentralized holonic control system model for line-less mobile assembly systems. Robot. Comput.-Integr. Manuf. 75, 102301.

Chang, T.-H., Hong, M., Wang, X., 2014. Multi-agent distributed optimization via inexact consensus ADMM. IEEE Trans. Signal Process. 63 (2), 482–497.

Chen, H., Chillotti, I., Song, Y., 2019. Multi-key homomorphic encryption from TFHE. In: Advances in Cryptology–ASIACRYPT 2019: 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8–12, 2019, Proceedings, Part II 25. Springer, pp. 446–472.

Ding, T., Jia, W., Shahidehpour, M., Han, O., Sun, Y., Zhang, Z., 2022. Review of optimization methods for energy hub planning, operation, trading, and control. IEEE Trans. Sustain. Energy 13 (3), 1802–1818.

Dwork, C., Rothblum, G.N., Vadhan, S., 2010. Boosting and differential privacy. In: 2010 IEEE 51st Annual Symposium on Foundations of Computer Science. IEEE, pp. 51–60.

Faia, R., Lezama, F., Soares, J., Pinto, T., Vale, Z., 2024. Local electricity markets: A review on benefits, barriers, current trends and future perspectives. Renew. Sustain. Energy Rev. 190, 114006.

Hatziargyriou, N., 2023. Differences and synergies between local energy communities and microgrids. Oxf. Open Energy 2, oiac013.

Heydarian-Forushani, E., Bahramara, S., Sheikhahmadi, P., Zeraati, M., Elghali, S.B., 2023. A proactive strategy for virtual power plants including multiple private owners equipped with energy storages. J. Energy Storage 66, 107514. http://dx.doi.org/10.1016/j.est.2023.107514.

Huo, X., Liu, M., 2021. Privacy-preserving distributed multi-agent cooperative optimization—paradigm design and privacy analysis. IEEE Control. Syst. Lett. 6, 824–829.

Kalbantner, J., Markantonakis, K., Hurley-Smith, D., Akram, R.N., Semal, B., 2021. P2PEdge: A decentralised, scalable P2P architecture for energy trading in real-time. Energies 14 (3), 606.

Kim, M., Günlü, O., Schaefer, R.F., 2021. Federated learning with local differential privacy: Trade-offs between privacy, utility, and communication. In: ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing. ICASSP, IEEE, pp. 2650–2654.

Kwak, H., Min, S., Song, Y., 2024. Towards practical multi-key TFHE: parallelizable, key-compatible, quasi-linear complexity. In: IACR International Conference on Public-Key Cryptography. Springer, pp. 354–385.

Liu, C., Bastianello, N., Huo, W., Shi, Y., Johansson, K.H., 2024a. A survey on secure decentralized optimization and learning. arXiv preprint arXiv:2408.08628.

Liu, F., Zheng, Z., Shi, Y., Tong, Y., Zhang, Y., 2024b. A survey on federated learning: a perspective from multi-party computation. Front. Comput. Sci. 18 (1), 181336.

Lowitzsch, J., Hoicka, C.E., van Tulder, F.J., 2020. Renewable energy communities under the 2019 European clean energy Package–Governance model for the energy clusters of the future? Renew. Sustain. Energy Rev. 122, 109489.

Ma, J., Naas, S.-A., Sigg, S., Lyu, X., 2022. Privacy-preserving federated learning based on multi-key homomorphic encryption. Int. J. Intell. Syst. 37 (9), 5880–5901.

VPP4ISLANDS Consortium, 2024a. VPP4ISLANDS. URL https://vpp4islands.eu/index.php/demo-site/#demo-site-2. (Accessed 28 April 2025).

VPP4ISLANDS Consortium, 2024b. VPP4ISLANDS P2P. URL https://vpp4islands.eu/index.php/Results/#p2p. (Accessed 28 April 2025).

Xu, K., Tan, B.H.M., Wang, L.-P., Aung, K.M.M., Wang, H., 2023. Multi-key fully homomorphic encryption from NTRU and (R) LWE with faster bootstrapping. Theoret. Comput. Sci. 968, 114026.

Yang, M., Guo, T., Zhu, T., Tjuawinata, I., Zhao, J., Lam, K.-Y., 2024. Local differential privacy and its applications: A comprehensive survey. Comput. Stand. Interfaces 89, 103827.

Yue, X.-Y., Xiao, J.-W., Liu, X.-K., Wang, Y.-W., 2025. Differentially private linearized ADMM algorithm for decentralized nonconvex optimization. IEEE Trans. Inf. Forensics Secur.

Yuen, T.H., Esgin, M.F., Liu, J.K., Au, M.H., Ding, Z., 2021. DualRing: generic construction of ring signatures with efficient instantiations. In: Annual International Cryptology Conference. Springer, pp. 251–281.

Zarir, A.A., Oliva, G.A., Jiang, Z.M.J., Hassan, A.E., 2021. Developing cost-effective blockchain-powered applications: A case study of the gas usage of smart contract transactions in the ethereum blockchain platform. ACM Trans. Softw. Eng. Methodol. 30 (3), http://dx.doi.org/10.1145/3431726.