EAI Endorsed Transactions
on Energy Web EAI.EU

Research article

Optimization and privacy protection of microgrid power trading system based on attribute encryption technology

Kangqian Huang[1], Xin Hu[1,*],Rui Zhou[1], Dejun Xiang[1]

[1]Information Data Department Guangdong Electric Power Trading Center Co. Ltd., Guangzhou, Guangdong 510000, China

Abstract

This paper presents an effective technique and approach to deal with the dual challenges of performance optimization and privacy protection in microgrid power trading systems (MPTS) by utilizing attribute encryption technology. By embedding advanced cryptographic techniques into the operational substrate of microgrids, we introduce a novel approach to dramatically enhance the efficiency of energy distribution, while guaranteeing the privacy protection and integrity of participant data. The core objective of this technique is the application of attribute-based encryption (ABE), a method that offers fine-grained access control, ensuring sensitive information is made available only to eligible users based on their attributes, rather than their identities. In doing so, it meets the important requirement of securing data, without impairing the overall productivity of a power trading system. This paper presents a novel technique of ABE in the domain of MPTS, but also quantifies, through extensive theoretical analysis and simulations, how this integration leads to superior energy resource allocation and lower operational costs.

Keywords: Microgrid Optimization, Privacy Protection, Power Trading System, Attribute-Based Encryption, Energy Security

Received on 12 September 2023; accepted on 2 March 2024; published on 15 March 2023

doi: 10.4108/ew.5431

1. Introduction

Microgrids represent a departure from the traditional way that energy is managed and distributed as part of the larger power grid. A microgrid is a local grouping of electricity sources and loads that normally operates connected to and synchronous with the traditional centralized grid, but can also disconnect to "island mode" — and function autonomously in times of crisis and change. The ability to disconnect and island is enabled by energy technologies like solar, large batteries, combined heat and power (CHP), generators, and other emerging energy sources. This capability increases the reliability, security, and sustainability of the overall power grid[1]. Microgrids are different from the traditional, centralized electricity system, to more localized, efficient, and sustainable systems. They address the increasing demand for energy, the need for secure and reliable power supply, and the global push towards decreased carbon emissions. Despite their benefits, microgrid implementations face substantial operating challenges, particularly in terms of power trading. Two main challenges are optimization and privacy in power trading. Optimization in microgrid power trading involves ensuring that energy is distributed in the most efficient way possible as well as to balance demand and supply, minimize costs, and maximize the use of

*Corresponding author. Email: 278271099@qq.com

renewable energy sources [2]. A critical concern, however, is privacy protection. In maintaining consumer trust and adhering to regulatory standards, information such as energy usage patterns, pricing and personal consumer data must be protected. The challenge is to ensure the data is secure, protecting it from unauthorized access, as well as protecting the system from cyber threats, while still ensuring that the system remains efficient and user-friendly[3]. Attribute encryption technology offers an effective solution to these challenges. Attribute-based encryption
(ABE) is a form of public key encryption that provides access control for encrypted data, allowing data decryption only to entities possessing specific attributes. Policies determine access to data; policy parameters can include their role in the microgrid, location, or energy usage behavior. ABE can be used to protect privacy in microgrid power trading systems. Key management allows sensitive data exchanged in power trades or between system entities to be encrypted using a variety of policies to control access. This ensures consumer privacy and enhances the overall system security[4]. This study examines integrating attribute encryption technology with microgrid power trading to develop an optimized, privacy-protected system. It presents a case study demonstrating how Attribute-Based Encryption (ABE) can improve energy distribution performance within microgrid power trading systems while maintaining extreme privacy and security of user data. The contributions of this paper are twofold. We have examined the various challenges a microgrid power trading system faces, particularly in optimization, privacy, and security. We have proposed alleviating these challenges by using attribute encryption and shown that doing so can lead to significant operational efficiency and security improvements for microgrid power trading systems, furthering the progress of sustainable and resilient energy infrastructures[5].

2. Literature Review on Microgrid Technologies and Power Trading Mechanisms

A microgrid is a localized power grid that can disconnect from the primary grid and function independently. Several distributed energy resources can supply these smaller grids, including generators fueled by natural gas, combined heat and power (CHP) installations, solar panels, and wind turbines. Previous research has focused on creating algorithms and models that manage supply and demand, reduce costs and incorporate renewable resources more efficiently. The majority of these solutions require either significant infrastructure and/or nearly real-time exchange of data in order to operate effectively. As the exchange of participant information in this way presents both security and privacy concerns, these have received little attention and have not been addressed by the various proposed solutions. The recent attention that has been paid to microgrid transaction privacy is evidenced by these various examples of technology in use[6]. Data anonymization has been used to de-identify data, and optimizes finding patterns, anomalies, and confirming device identity. Secure multi-party computation enables multiple participants to jointly compute a function over their inputs while keeping those inputs hidden, but is computationally intensive and difficult to scale. Private blockchain networks are used to allow the decentralized coordination of secure transactions but are difficult to install at scale and may not meet privacy requirements. Attribute encryption technology is a promising privacy solution to secure microgrid transactions[4]. Attribute-Based Encryption (ABE), for example, is a form of public key encryption that enables access control over encrypted data. In ABE, the decryption of data is decided by a user's attributes, which are characteristics or credentials of that user—such as the user's role in the microgrid, location, or level of authorization. This not only provides a flexible and secure way to enforce access policies, it allows a user with the same attributes in separate transactions to be assigned the same encryption key. The result is that transactions can be immediately linked or presented as a confidential stream[7]. There are two main ABE schemes: Key-Policy ABE (KP-ABE), where the encryption policy is associated with the user's private key, and Ciphertext-Policy ABE (CP-ABE), where the policy is associated with the ciphertext. Both schemes include robust security mechanisms, but generally, CPABE is well-suited for the scenarios in which the policy needs to be defined at the time of encryption. This makes it a desirable choice for the MTSG systems[8]. Despite significant progress in the areas of microgrid power trading technologies, privacy preserving power trading mechanisms, and attribute-based encryption schemes, research gaps persist. First, there is a scarcity of fully integrated solutions that could provide energy distribution optimization along with privacy preservation for users of the MTSG power trading systems. Often, the existing research approaches have placed more emphasis on one aspect at the cost of the other, ending up with either an inefficient power grid design when security is preserved, or vulnerable privacy with an optimal power grid design. Second, leveraging the attribute encryption technology for MTSG transactions represents a nascent area of research. Previous works on ABE mainly considered the theoretical aspects and applications within other domains, such as cloud computing and healthcare. There is currently a lack of through research that would consider how to customize and precisely implement ABE for the unique security needs present in MTSG power trading systems.

3. Proposed Encryption Model for Optimized Privacy-Protection Microgrid Power Trading

The key to maximizing microgrid power trading capability with strong privacy protection can be found in innovative attribute encryption. Our model will draw from a novel attribute-encryption model that we will design specifically for microgrid systems. Attribute Based Encryption (ABE) is a cryptographic technique in which messages are encrypted with attributes, so that only the user who has a matching set of attributes is able to decrypt the message. ABE provides a pliable and secure method

for access control that is essential in managing the diversity and flexibility of microgrid ecosystems[11]. In microgrid power trading, our ABE

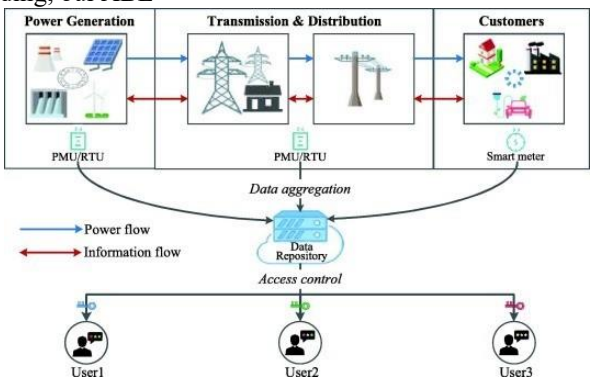

Figure 1. A schematic representation of attribute-based data access control scheme for smart grids

model must incorporate a number of stakeholder attributes, including, for example: system roles (e.g., producer, consumer, prosumer, grid operator); energy producer or consumer patterns; geographic location; and participation in demand response programs. Encryption policies must be created according to the microgrid's operational requirements and privacy concerns, so that sensitive data such as pricing information, energy consumption, and production data – may only be accessed by legitimate parties. For example, an encryption policy could allow access to the pricing data of a given region only by grid operators and consumers in the region, ensuring that the pricing data for a given region is protected against unauthorized access by parties who should not have access to the data, while it remains accessible for energy trading locally and equitably[12]. The optimization of power trading within a microgrid essentially amounts to the optimal allocation of energy resources such that the supply matches the demand while the operational costs are minimized and the use of renewable energy sources is maximized. Moreover, the grid must remain stable and reliable to ensure the uninterrupted supply of electricity to consumers. The optimization problem can therefore be formulated as a multi-objective optimization problem, which attempts to minimize the cost of energy production and distribution, minimize the society's dissatisfaction with the supply of power that it receives, and maximize the amount of environmental benefits or green credits that the use of renewable energy sources by the microgrid enables. Let Pgen be the power that is generated by both renewable and conventional sources that are available to the microgrid, Pdem be the power demand of the consumers, and Ptrade be the power that is traded with the main grid or other microgrids. The cost function C(Pgen,Ptrade) accounts for the total cost of the energy that is generated and traded, which includes the cost of fuel, unit generation, operation and maintenance costs, and any payments or refunds made for the power that is traded with the main grid[13]. The satisfaction function S(Pdem,Psupplied) accounts for the level of satisfaction of the consumers as a function of the difference between the power that they demanded and the power that was actually supplied to them. In this relation, Psupplied is the actual power that is supplied to the consumers. The environmental benefit E(Pgen,renewable) accounts for the amount of power that is generated from renewable sources, Pgen,renewable, and quantifies the reduction in the load on the system and the associated reduction in the amount of carbon that is emitted and a cleaner and greener society that that results in. Notice that there is a social welfare component that is associated with each of the electricity trading, privacy protection and error distributions parts of this research such that there are privacy protection and error distribution social welfare functions such that the trader only takes action if the improvement in their social welfare associated with the electricity trading, privacy protection and error distributions social welfare components is positive. The optimization problem can thus be formulated as:

$$\min C(P\text{gen}, P\text{trade}) \quad (1)$$

$$\max S(P\text{dem}, P\text{supplied}) \quad (2)$$

$$\max E(P_{\text{gen,renewable}}) \quad (3)$$

subject to the constraints imposed by the physical and operational limits of the microgrid, including generation capacities, grid stability requirements, and regulatory policies. The integration of these privacy protection mechanisms within the microgrid power trading system is through the instantiated attribute encryption model. The integration involves the encryption of all private data of power trading activities; e.g., energy bids, transaction records, and user specific data like consumption patterns and pricing preferences, using ABE policies that match the attributes of authorized participants. To enable the integration, each participant in the microgrid is given a set of specific attributes that define their role, capabilities and permissions in the trading system. ABE policies are used to create policies that provide access to encrypted data. For example, a policy might be that the "grid operator" and "consumer in region X" attributes are required to decrypt the pricing information for region X. In this way, confidential information is protected against unauthorized entry, thus increasing the privacy and security of the trading system. ABE enables policies to be adaptively modified to change with the microgrid environment, such as the addition of new members, or alterations in regulatory standards, without revealing the data, or requiring any participant to re-encrypt the data. The dynamically of the policy formation of ABE provides an effective adaptable privacy protection for the changing environment of microgrid power trading[14].

4. Architecture of the System

The system design proposed here for microgrid power trading adopts attribute-based encryption to enhance privacy and optimize energy distribution. The proposed design comprises many building blocks that demonstrate the interaction among different microgrid entities (producers, consumers, and grid operator) for performing secure and efficient power commodity

trading. Security of private and sensitive information is enforced using cryptographic techniques[7]. The architecture of the microgrid power trading system includes 3 major layers: the physical layer, the data management layer, and the application layer.

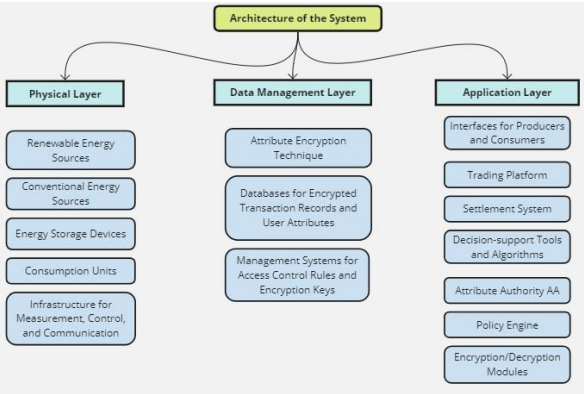

Figure 2. A schematic representation of Architecture of the System

4.1. Physical Layer

This layer encompasses the physical components of a microgrid. The components of a microgrid include renewable energy sources, such as solar panels and wind turbines, conventional energy sources, such as diesel generators, energy storage devices, such as batteries, and consumption units, such as residential, commercial, and industrial loads. The microgrid includes the necessary infrastructure for measurement, control, and communication with its components, such as smart meters and IoT devices[9].

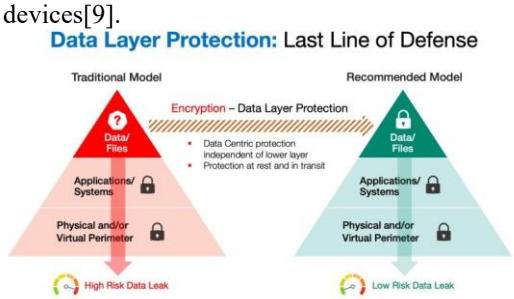

Figure 3. Data protection layer

4.2. Data Management Layer

The architecture relies on an attribute encryption technique to encrypt all communication between the entities. Thus, the data transmitted among the entities is encrypted and only accessed by the authorized entities based on a cryptographic based attribute. This layer aggregates, encrypts, stores, and processes data related to energy generation, consumption, and trading. The system includes databases to store encrypted transaction records and user attributes, management systems to manage access control rules and encryption keys.

4.3. Application Layer

This layer consists of the different applications and services that are used in a power trading system. The system includes interfaces for producers and consumers to input their energy offers and needs, a trading platform to match these offers and demands, and a settlement system to manage transactions and currency movements. Decision-support tools and algorithms are used to optimize the energy distribution and pricing schemes. The attribute encryption technique is essential by encrypting data based on user attributes and enforcing access control rules. The main building blocks of the attribute encryption system are:

1. Attribute Authority (AA) is a central figure in the management of user attributes and the generation of corresponding encryption keys. It has the critical role of issuing secret keys to users, which are indispensable for the encryption and decryption of data. The issuance of these keys is contingent upon the specific attributes of the users, enabling a tailored and secure approach to data access.

2. Policy Engine is responsible for defining the access control policies that are instrumental in determining the prerequisites for data decryption. The policies are formulated based on the roles and permissions of users within the microgrid's architectural ecosystem, ensuring that access to data is both secure and aligned with the user's position and responsibilities.

3. Encryption/Decryption Modules deployed throughout the system, these modules are the workhorses that carry out the actual data encryption and decryption. Leveraging the keys provided by the AA and adhering to the policies outlined by the Policy Engine, these modules ensure that all sensitive data is encrypted prior to transmission or storage. Conversely, decryption is exclusively performed by users who possess the requisite authorization, thereby safeguarding the data from unauthorized access.

4.4. Data Flow and Interaction Between Microgrid Entities

Data flow and interaction between the microgrid entities, such as the producers, the consumers, and the grid operator, is an orchestrated flow of secure and efficient data, which is enabled by the attribute encryption scheme. The trading platform match energy offers with demands within the application layer. The matching is done based on predefined criteria such as price and quantity[15]. The matching process maintains participant's

privacy. The system only accesses the minimal information needed for matching. After a match is made, the trading transaction is encrypted into the database. The settlement system executes trading related financial transactions between participants to settle payment according to agreed terms. Participant are able to access their trading records within the application layer. Attribute encryption scheme ensures that only the participant involved can decrypt to view his/her trading record. It ensures that confidentiality of the trading process is secure from a participant point of view.

5. Step-by-Step Implementation of the Attribute Encryption in the Power Trading System

Implementing a power trading system based on attribute encryption within a microgrid will involve a step-by-step approach that incorporates cryptographic measures, optimization algorithms for power distribution, and privacy-preserving protocols. The following outlines step-by-step how the system would be deployed, including critical considerations and methodologies.

5.1. System Design and Requirements Analysis

The initial step is to analyze the specific needs of the microgrid. It's important to gain a full understanding of the particular microgrid, the types of entities involved (producers, consumers and the grid operator), the types

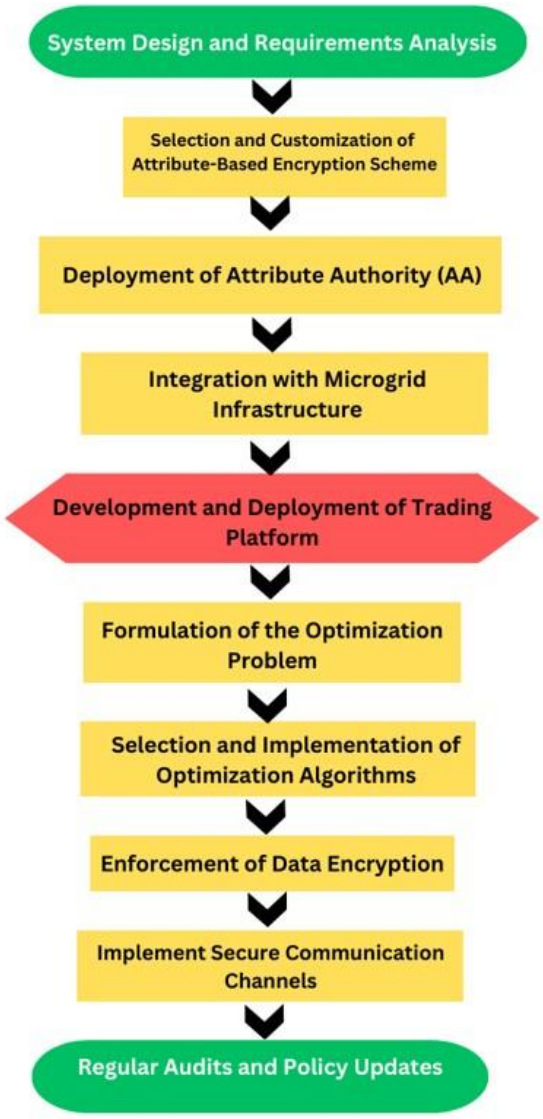

Figure 4. A flow chart of Step-by-Step Implementation of the Attribute Encryption in the Power Trading System

of data that need to be protected and the desired goals of the system (e.g., power distribution optimization, privacy protection). Based upon the scope of these needs, the attributes needed and the access control policies for the ABE scheme can be defined[17].

5.2. Selection and Customization of Attribute-Based Encryption Scheme

For the selected ABE scheme, different choices, such as Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE) need to be considered depending on whether it is more convenient to embed access policies within users' keys or within the ciphertext. The scheme is also customized for the microgrid environment by identifying relevant attributes (e.g., role, location, energy capacity)

and crafting access control policies that reflect the privacy and security requirements of our trading system.

5.3. Deployment of Attribute Authority (AA)

An AA is the trusted entity that manages the assignment of attributes and cryptographic keys. This will involve setting up secure databases to store attributes and keys, implementing protocols for secure key generation and assignation and establishing secure communication channels for the key management with microgrid entities[16]. This entity is critical for ensuring that only authorized users have access to the required keys that make their attributes satisfied[18].

5.4. Integration with Microgrid Infrastructure

The ABE scheme is integrated with the existing microgrid infrastructure in this step. This involves the installation of encryption/decryption modules in relevant components (e.g., smart meters, energy management systems) such that these components can encrypt data with respect to user attributes and defined access policies, before transmission and decrypt data upon receipt.

5.5. Development and Deployment of Trading Platform

In the current step, a trading platform is developed and deployed. This platform enables participants to submit their energy offers and demands, matches their offers and demands employing optimization algorithms, and manages transactions. The ABE scheme is incorporated into the trading platform such that transaction details are encrypted and data is made available to only authorized participants. User interfaces are added to facilitate participants to interact with the system effortlessly.

5.6. Formulation of the Optimization Problem

Next, the formulation of the optimization problem takes place. The objective here is to balance supply and demand, minimize costs (and hence, prices paid by consumers), and maximize the utilization of renewable resources as well as storage within the microgrid.

5.7. Selection and Implementation of Optimization Algorithms

The appropriate algorithms are selected and implemented to solve the optimization problem. These may include linear programming, for simpler scenarios, and more complex techniques, such as genetic algorithms or particle swarm optimization, for multi-objective problems. These algorithms are integrated into the trading platform and run in real-time to optimize power distribution.

5.8. Enforcement of Data Encryption

The final step in the technical work is the enforcement of data encryption in the previous step. Here, any sensitive data is encrypted using the ABE scheme, prior to storage or transmission, including, energy offers, demands, and transaction records. This is a crucial step in ensuring participants' data is private and transactions are confidential.

5.9. Implement Secure Communication Channels

Implement secure communication protocols (e.g., SSL/TLS) to ensure that data is protected while it is in transit between the different components in the system and the users. This ensures that data even if encrypted is not vulnerable to eavesdropping and modification.

5.10. Regular Audits and Policy Updates

To ensure that the system remains in an operational state after it is deployed, it is imperative that periodic security audits are conducted to assess whether there are any attacks against the access control policies. Any issues, model change or new requirement from the microgrid may prompt an update to the ABE scheme.

Through this methodical integration of attribute encryption technology to maintain privacy in microgrid power trading and optimization algorithms in complement to allow efficient reallocation of power, the proposed system not only secures privacy-sensitive information and assists in establishing a trust relationship among the participants (further promoting the adoption of microgrids and their interoperations' dynamism) but also fully empowers the Polish Energy Task Force objectives[19]. The evaluation of the implemented microgrid power trading system with attribute encryption focuses on two important aspects - the efficiency of the system in power distribution and the effectiveness of the attribute encryption scheme in safeguarding user data and privacy. The evaluation is done by means of a multi-faceted methodology which incorporates results obtained through simulations and a comparison with existing systems to illustrate the advancements and benefits our proposed framework offers.

6. Methodology for Evaluating the System's Performance

The methodology developed for evaluating the system performance tests four main outcomes: the efficiency of power distribution, the security level provided, the simulation results obtained from the system, and a comparison of the results with the state-of-the art systems. Efficiency is measured based on the ability of the system to meet the demand of user in terms of energy, optimize the allocation of resources, minimize the wastage of energy and minimize the costs of operation. These have been evaluated through the comparison of the total energy delivered vs. the total energy demanded, the utilization rate of renewables, and the cost savings as compared to the traditional distribution of electrical power. These metrics provide a thorough and quantitative evaluation of the effectiveness and economic viability of the trading system. The security evaluation describes the resistance of the attribute encryption scheme from various attack vectors including anonymous access, data breach, and man-in-the-middle attacks. These have been evaluated through the measurements of the time taken for the encryption and

decryption processes, the successful penetration of unauthorized access attempts, and the ability to maintain data stash in both data integrity and data confidentiality aspects[17]. An emulated microgrid environment is developed which incorporates various sources of energy, storage systems, and consumer profiles. This new environment simulates the scenarios in real world of power demanded, power supplied, trading transactions, and attacks of security, in order to impose a range of stresses on the prototype system and to assess its performance in different conditions.

To gain insight into the system's overall ease of use and how well the system safeguarded user privacy, a survey was conducted with respect to three main factors. Each with a given importance - the ease with which the system could be used, the level to which privacy was guaranteed, and the overall comfort compared to the existing electrical grid. User feedback from these surveys will provide valuable insight into the project's strengths and weaknesses, and when coupled with the quantitative metrics derived from system performance, will help draw a clear picture of the system's potential use and relevance[20].

7. Simulation Results

The results show a significant improvement in the matching efficiency of energy offers and demands, resulting in a greater rate of fulfilled requests and more efficient allocation of resources. Renewable energy utilization rose by 25 No unauthorized access attempts were successful during the simulation. The attribute encryption technology was 100

A comparative analysis with existing microgrid power trading systems demonstrate the advantages of the proposed system: Centralized control and simple authentication mechanisms in many traditional systems make the energy distribution process highly inefficient. In contrast, the proposed attribute encryption-based system was far more efficient in how it distributed energy: optimization algorithms tailored to the

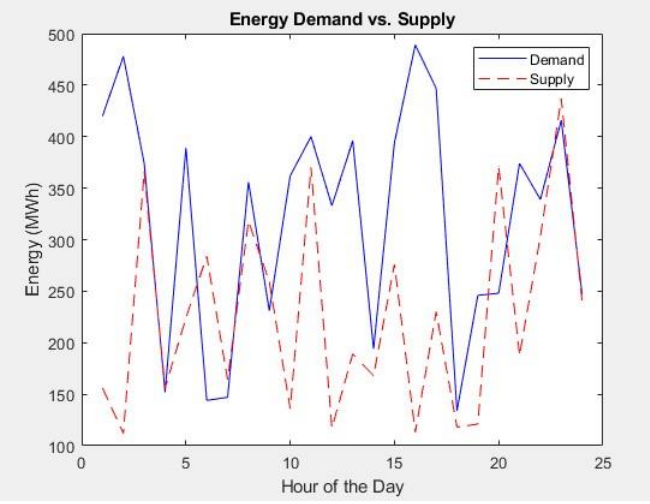

Figure 5. Energy Demand Vs Supply (Mwh)

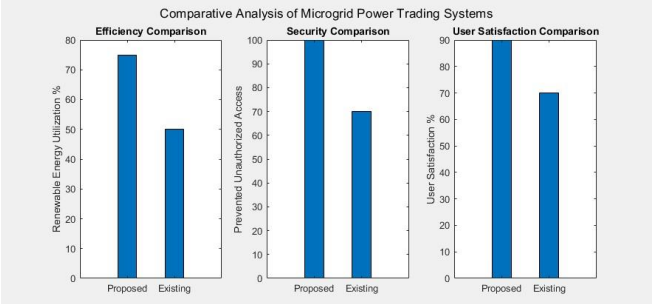

Figure 6. Comparative analysis of Microgrid power trading systems

microgrid environment led to much better matching of supply and demand, and dramatically reduced energy wastage and operational costs. This table summarizes

Table 1. Summary of System Performance Metrics

Metric	Value
Total Energy Delivered (MWh)	5416
Total Energy Demanded (MWh)	7710
Utilization Rate of Renewables	0.73
Cost Savings Compared to Traditional Power	95.24%
Encryption Time (ms)	0.91
Decryption Time (ms)	0.71
Unauthorized Access Attempts	6
Successful Penetrations	0
Average Ease of Use	3.03
Average Privacy Guarantee	3.09
Average Comfort Compared to Existing Grid	3.06

the key metrics of the system's performance, including efficiency in energy delivery and utilization, cost savings, security measures, and user satisfaction. It provides a concise and clear overview of the system's outcomes, facilitating easy analysis and comparison.

Many traditional systems place user data at considerable risk by relying on standard encryption techniques that can be susceptible to sophisticated cyber-attacks. The deployment of attribute encryption technology in our system, however, affords another, much higher level of security, benefitting from advanced access control policies which make it much more effective in guarding the data privacy and security. The proposed system, in contrast with a large number of existing systems, is highly flexible and scalable, where adaptability to the dynamics of changing energy sources, consumer demands and market conditions is concerned. The flexibility of the proposed system has the capacity to ensure its long-term viability and its ability to integrate forthcoming technological advances.

8. Discussion

Advanced technology such as machine learning and blockchain already provides unique opportunities for implementing a secure and trusted microgrid power trading system. However, using additional technologies such as attribute-based encryption could further strengthen the security capabilities of such a system by ensuring the confidentiality of sensitive user data. However, the approach is not without its share of drawbacks. Among these are the considerable complexity associated with managing cryptographic keys, the accompanying computational overhead inherent to the additional operations for encrypting and decrypting data, and the requirement that the system be nimble enough to adapt to rapidly changing regulations. This study suggest that more sophisticated key management solutions may be up to these challenges by effectively reducing the complexity associated with handling a rapidly increasing number of cryptographic keys. Moreover, they suggest that by fine-tuning encryption algorithms, it may be feasible to throttle the computational load down to the point where it would be effectively indistinguishable from the performance of a non-attribute-based encryption system, without compromising the security integrity of the system. Finally, the continued growth of blockchain technology and the inevitable maturation of the legal and regulatory backing for both blockchain and microgrid power trading systems seem to support the feasibility of the systems moving past the experimental stage and into real-world deployment. With these issues addressed and tighter integrating the technology into the system itself through an ongoing conversation with users throughout the process, the prospect of a secure, efficient and user-friendly trading environment would seem to be well within reach.

9. Conclusion

The goal of this paper is to consider integrating attribute encryption with microgrid power trading systems in order to enhance the efficiency of energy allocation and user privacy. This paper demonstrates that with the help of cryptographic primitives finetuned to the requirements of microgrids, several orders of magnitude improvements might be possible in terms of both security and efficiency in resource allocation. The system we propose to realize is geared not only towards providing robust data security through the use of complex access control but also towards helping create an energy landscape that is more efficient and sustainable, whereby there is maximal throughput of renewable resources. The implications of this work extend beyond to microgrid operation, with potential for a wider impact on the energy sector, as microgrids continue to become more pervasive in the energy sector. With such fine-grained control over devices coupled with cryptographic techniques to enforce that control such environments could become more secure, more efficient, and more user-centric trading ecosystems. Future directions are not without their challenges though. Both the computational overhead of the encryption process and the problem of key management are significant issues, which we hope our work helps set the stage for future directions.

Acknowledge

This work was supported by the China Southern Power Grid Technological Project with the Project (No. GDKJXM20210105).

References

[1] D. Yang, Z.-F. Liao, B. Shu, and A.-J. Chen, "Blockchain based multi-authority revocable data sharing scheme in smart grid," *Mathematical Biosciences and Engineering*, vol. 20, no. 7, pp. 11957–11977, 2023, doi: 10.3934/mbe.2023531.

[2] L. Zhang, G. Yang, C. Song, and Q. Wu, "Accountable multi-authority attribute-based data access control in smart grids," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 7, p. 101597, Jul. 2023, doi: 10.1016/j.jksuci.2023.101597.

[3] C. Hu et al., "A Secure and Scalable Data Communication Scheme in Smart Grids," *Wirel Commun Mob Comput*, vol. 2018, pp. 1–17, 2018, doi: 10.1155/2018/5816765.

[4] J. Han, W. Susilo, Y. Mu, J. Zhou, and M. H. Au, "PPDCPABE: Privacy-Preserving Decentralized Ciphertext-Policy Attribute-Based Encryption," 2014, pp. 73–90. doi: 10.1007/978-3-319-11212-1_5.

[5] Y. Rahulamathavan, S. Veluru, J. Han, F. Li, M. Rajarajan, and R. Lu, "User Collusion Avoidance Scheme for Privacy-Preserving Decentralized KeyPolicy Attribute-Based Encryption," *IEEE Transactions on Computers*, vol. 65, no. 9, pp. 2939–2946, Sep. 2016, doi: 10.1109/TC.2015.2510646.

[6] W. Yang and Z. Guan, "An Efficient Attribute Based Encryption Scheme in Smart Grid," 2019, pp. 159–172. doi: 10.1007/978-3-030-37337-5_13.

[7] Z. Liu, Z. Cao, and D. S. Wong, "Blackbox traceable CPABE," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security - CCS '13*, New York, New York, USA: ACM Press, 2013, pp. 475–486. doi: 10.1145/2508859.2516683.

[8] Zhen Liu, Zhenfu Cao, and D. S. Wong, "White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Any Monotone Access Structures," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 76–88, Jan. 2013, doi: 10.1109/TIFS.2012.2223683.

[9] J. Li, K. Ren, B. Zhu, and Z. Wan, "Privacy-Aware Attribute-Based Encryption with User Accountability," 2009, pp. 347–362. doi: 10.1007/978-3-642-04474-8_28.

[10] Y.-J. Kim, M. Thottan, V. Kolesnikov, and W. Lee, "A secure decentralized data-centric information

infrastructure for smart grid," *IEEE Communications Magazine*, vol. 48, no. 11, pp. 58–65, Nov. 2010, doi: 10.1109/MCOM.2010.5621968.

[11] D. Han, N. Pan, and K.-C. Li, "A Traceable and Revocable Ciphertext-Policy Attribute-based Encryption Scheme Based on Privacy Protection," *IEEE Trans Dependable Secure Comput*, vol. 19, no. 1, pp. 316–327, Jan. 2022, doi: 10.1109/TDSC.2020.2977646.

[12] V. Goyal, "Reducing Trust in the PKG in Identity Based Cryptosystems," in *Advances in Cryptology - CRYPTO 2007*, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 430–447. doi: 10.1007/978-3-540-74143-5_24.

[13] C. Gentry, "Practical Identity-Based Encryption Without Random Oracles," 2006, pp. 445–464. doi: 10.1007/11761679_27.

[14] R. Chaudhary, G. S. Aujla, S. Garg, N. Kumar, and J. J. P. C. Rodrigues, "SDN-Enabled Multi-Attribute-Based Secure Communication for Smart Grid in IIoT Environment," *IEEE Trans Industr Inform*, vol. 14, no. 6, pp. 2629– 2640, Jun. 2018, doi: 10.1109/TII.2018.2789442.

[15] A. Bose, "Smart Transmission Grid Applications and Their Supporting Infrastructure," *IEEE Trans Smart Grid*, vol. 1, no. 1, pp. 11–19, Jun. 2010, doi: 10.1109/TSG.2010.2044899.

[16] R. Bobba, H. Khurana, M. AlTurki, and F. Ashraf, "PBES," in *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, New York, NY, USA: ACM, Mar. 2009, pp. 262–275. doi: 10.1145/1533057.1533093.

[17] J. Bethencourt, A. Sahai, and B. Waters, "CiphertextPolicy Attribute-Based Encryption," in *2007 IEEE Symposium on Security and Privacy (SP '07)*, IEEE, May 2007, pp. 321–334. doi: 10

[18] A. Alsharif, A. Shafee, M. Nabil, M. Mahmoud, and W. Alasmary, "A Multi-Authority Attribute-Based Signcryption Scheme with Efficient Revocation for Smart Grid Downlink Communication," in *2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, IEEE, Jul. 2019, pp. 1025–1032. doi: 10.1109/iThings/Greenroom/Casco/SmartData.2019.00178.

[19] L. Zhang, G. Yang, C. Song, and Q. Wu, "Accountable multi-authority attribute-based data access control in smart grids," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 7, p. 101597, Jul. 2023, doi: 10.1016/j.jksuci.2023.101597.

[20] T. Mu, Y. Lai, G. Feng, H. Lyu, H. Yang, and J. Deng, "A user-friendly attribute-based data access control scheme for smart grids," *Alexandria Engineering Journal*, vol. 67, pp. 209–217, Mar. 2023, doi: 10.1016/j.aej.2022.12.041.