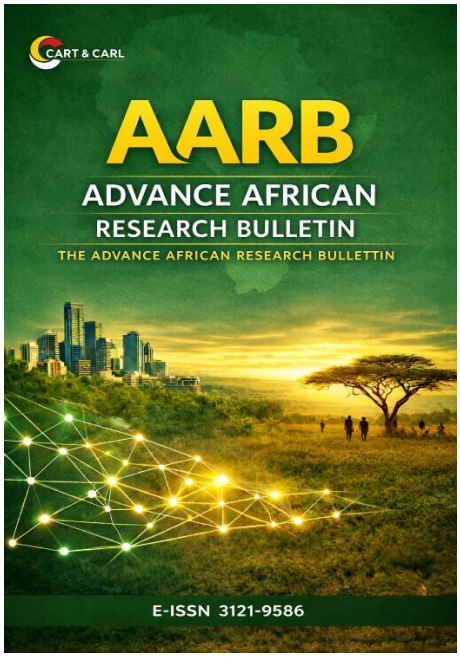
Original Research

Advance African Research Bulletin
https://cartcarl.com/journal/advance-african-research-bulletin

E-ISSN: 3121-9586



An Improved Secure Communication System for Peer-To-Peer Solar Energy Trading in Nigeria

Authors
[a] Ikukaiwe, P. C. and [a] Alabi, A. O.

[a] Centre for Information and Telecommunication Engineering, Faculty of Engineering, University of Port Harcourt.

Corresponding Author
Ikukaiwe, P. C.
(Ikukaiwep@gmail.com)

Received: 15 January 2026
Accepted: 03 February 2026
Published: 05 February 2026

Citation
Ikukaiwe, P. C. and Alabi, A. O. (2025). An Improved Secure Communication System for Peer-To-Peer Solar Energy Trading in Nigeria. *Advance African Research Bulletin*, 2(1), 01-07.
https://doi.org/10.70726/aarb.2026.9586001

Abstract

The persistent challenges of unreliable electricity supply and increasing energy demand in Nigeria have accelerated the adoption of decentralized renewable energy systems, particularly solar photovoltaic technologies. Peer-to-peer (P2P) solar energy trading has emerged as a viable solution that enables prosumers to trade excess energy directly with consumers within localized networks. However, the effectiveness of P2P energy trading systems is highly dependent on the security and reliability of their communication infrastructures, as decentralized platforms are vulnerable to cyber threats such as unauthorized access, data tampering, and impersonation attacks. This study therefore focuses on the design and evaluation of an improved secure communication system for peer-to-peer solar energy trading in Nigeria. The study adopted a design-and-implementation research approach, incorporating cryptographic authentication, secure message encryption, transaction validation, and distributed ledger technology to enhance system security. Simulation-based experiments were conducted to evaluate system performance using metrics such as authentication time, transaction latency, security robustness, and scalability. The results indicate that the proposed system significantly improves authentication security and data integrity while maintaining acceptable transaction latency for real-time energy trading. The system also demonstrated resilience against common cyberattacks and stable performance as the number of participants increased. The study concludes that an improved secure communication system is essential for the successful deployment of peer-to-peer solar energy trading in Nigeria. By enhancing trust, transparency, and data security, the proposed system supports sustainable energy trading and contributes to the broader goal of improving energy access through decentralized renewable energy solutions.

Keywords : Renewable Energy, Security, Peer-to-Peer Communications, Solar Energy

Introduction

Nigeria's electricity sector continues to face significant challenges, including inadequate generation capacity, unstable grid infrastructure, and limited access to reliable power, particularly in rural and peri-urban communities. Despite abundant renewable energy potential, especially solar energy, a large proportion of the population still depends on diesel generators and other environmentally harmful energy sources (Adenikinju, 2020). In response to these challenges, decentralized energy systems such as solar photovoltaic (PV) installations and community microgrids have gained increasing attention as viable alternatives for improving energy access and sustainability. One emerging decentralized energy model is peer-to-peer (P2P) solar energy trading, which enables energy prosumers individuals or entities that both generate and consume electricity to sell excess solar energy directly to other consumers within a localized network. P2P energy trading enhances energy efficiency, promotes renewable energy adoption, and empowers local communities by reducing dependence on centralized utilities (Islam, 2024). Studies have shown that P2P trading can lower energy costs, improve grid

flexibility, and provide financial incentives for solar PV investment (Kumari et al., 2022). However, the successful deployment of P2P solar energy trading systems depends heavily on the availability of secure, reliable, and efficient communication infrastructures. Energy trading involves continuous exchange of sensitive information such as generation data, pricing bids, transaction records, and user identities. Without adequate security mechanisms, these communication channels are vulnerable to cyber threats including data tampering, impersonation, replay attacks, and unauthorized access, which can undermine trust among participants and compromise system integrity (Li et al., 2023).

Recent research emphasizes that secure communication systems are fundamental to ensuring transparency, privacy, and trust in decentralized energy markets. Blockchain-based platforms, cryptographic authentication schemes, and secure messaging protocols have been widely proposed to address these security concerns. Blockchain technology, in particular, offers decentralized control, immutability, and transparency through cryptographic hashing and consensus mechanisms, making it suitable for P2P energy trading environments (Firdaus et al., 2024; Kumari et al., 2022). Additionally, secure communication protocols and privacy-preserving mechanisms help protect users' identities and transaction data from malicious actors (Liu et al., 2025).

In the Nigerian context, the need for an improved secure communication system for P2P solar energy trading is especially critical. Factors such as inconsistent network infrastructure, regulatory uncertainty, and low cybersecurity awareness further exacerbate the risks associated with decentralized energy trading platforms (Shittu et al., 2021). A secure communication framework tailored to Nigeria's socio-technical and energy market conditions is therefore essential to ensure reliable information exchange, accurate energy accounting, and trusted transaction settlement among trading participants. Consequently, this study focuses on the development of an improved secure communication system for peer-to-peer solar energy trading in Nigeria. By integrating secure communication protocols, cryptographic authentication mechanisms, and decentralized transaction management, the proposed system aims to enhance data integrity, confidentiality, and trust within P2P solar energy markets. The study contributes to ongoing efforts to promote sustainable energy systems and strengthen the technical foundations required for secure decentralized energy trading in Nigeria.

Literature Review

Wongthongtham et al. (2021) conducted one of the earliest empirical investigations into blockchain-enabled peer-to-peer energy trading, focusing on how blockchain can facilitate secure, decentralized energy transactions between prosumers and consumers. The study explored the "blockchain trilemma" of scalability, security, and decentralization and empirically modelled the proposed solution using data from a real-world trial, showing that blockchain can enhance transactional security without compromising decentralized features. Relevance: This study provides baseline empirical evidence that blockchain can improve security and transparency in P2P energy trading markets, directly informing secure communication frameworks in decentralized solar energy contexts. Vishwakarma (2024) proposed an end-to-end blockchain-based solution for peer-to-peer renewable energy trading that increases transaction traceability, trust, and security in decentralized networks. Although smaller in sample size, this study empirically evaluated performance metrics such as transaction throughput and security properties under different network configurations. Relevance: The article demonstrates how decentralized ledger technology can empirically enhance communication security and trust—a core requirement for secure P2P solar energy trading systems. Bhavana et al. (2025) performed a comparative evaluation of blockchain consensus mechanisms (e.g., PoW, PoS, PBFT, Tendermint) to determine their suitability for secure and scalable peer-to-peer energy trading in microgrids. Through simulation experiments, the study assessed metrics such as fault tolerance, latency, throughput, and security trade-offs across protocols. Relevance: The research offers empirical insights on how choice of consensus protocol affects communication security and system scalability important for designing secure communication systems in P2P energy trading. Ravivarma et al. (2025) presented a blockchain-based P2P energy trading model integrated with multi-microgrid energy management and deep learning forecasting (BiLSTM-GRU) for optimized local energy utilization. Simulations showed the combined model enhances energy allocation and provides secure decentralized trading without third-party intervention. Relevance: The study empirically validates a hybrid energy management and blockchain trading architecture, highlighting how secure decentralized communication supports optimized energy sharing. Erdayandi et al. (2023) developed a privacy-preserving and accountable billing protocol for P2P energy markets, addressing privacy, accountability, and dispute resolution using homomorphic encryption and blockchain. The evaluation showed accurate billing and privacy protection while ensuring transparent

transaction accountability. Relevance: Though focused on billing, this empirical work shows how secure communication mechanisms (cryptography + blockchain) preserve user privacy and data integrity in decentralized energy exchanges. Tahir et al. (2025) proposed a blockchain-based model to safeguard security and privacy in P2P energy trading, evaluated using a Sepolia testnet implementation tailored to Nigeria. Findings revealed that secure authentication, encryption, and role-based access control reduced cyber threat risks and enhanced trust among participants. Relevance: This Nigerian case study provides empirical support for secure authentication and encryption techniques in P2P energy trading environments, making it highly relevant for localized solar trading systems in Nigeria. Oluwaseun et al. (2025) developed a decentralized P2P transactive energy system implementation framework that emphasizes seamless interactions between distributed energy resource components and economic viability through cost-benefit analysis. Their empirical cost-benefit evaluation demonstrated the potential for resilient and secure decentralized energy exchanges. Relevance: This empirical study highlights both technical and economic aspects of P2P systems and underscores the critical role of communication protocols in ensuring secure and efficient energy transactions.

Materials and Methods

Research Design

This study adopted a design-and-implementation research approach combined with experimental evaluation. The approach was considered appropriate because the study focuses on the development, implementation, and performance assessment of an improved secure communication system for peer-to-peer (P2P) solar energy trading. The research design involved system modelling, protocol design, implementation of security mechanisms, and performance evaluation using simulation and analytical methods.

System Architecture Design

The proposed secure communication system was designed based on a decentralized peer-to-peer architecture suitable for solar energy trading in microgrids. The architecture consists of the following components:

i Prosumers: Solar energy producers who can also consume energy.
ii Consumers: Users who purchase energy from prosumers.
iii Smart Meters: Devices responsible for measuring energy generation and consumption.
iv Communication Network: Enables data exchange among trading participants.
v Security Layer: Implements cryptographic authentication, encryption, and transaction validation.
vi Distributed Ledger / Transaction Manager: Maintains immutable transaction records and enforces trading rules.

The system was designed to operate without reliance on a centralized authority, thereby improving resilience, transparency, and trust among participants.

Materials Used

The materials used in this study include both software tools and security techniques, as outlined below:

i Simulation and Development Tools: Network simulation software (e.g., MATLAB, NS-3, or Python-based simulators), Blockchain development environment (e.g., Ethereum test network or private blockchain framework) and Programming languages such as Python and Solidity for protocol implementation
ii Security and Communication Technologies: Public Key Infrastructure (PKI) for identity management, Cryptographic hash functions (e.g., SHA-256), Asymmetric encryption algorithms (e.g., RSA or ECC), Secure message exchange protocols and Smart contracts for automated transaction execution

Proposed Secure Communication Method

The improved secure communication system integrates hybrid security mechanisms, including:

i Authentication Mechanism: Each participant is authenticated using a combination of cryptographic credentials and unique digital identities. Public-private key pairs are generated for all users, ensuring secure identity verification before participation in energy trading.
ii Secure Message Exchange: All communication messages such as energy offers, bids, and transaction confirmations are encrypted using asymmetric encryption to ensure confidentiality. Hashing techniques are applied to ensure message integrity and prevent tampering.
iii Transaction Validation and Recording: Energy trading transactions are validated through a decentralized consensus mechanism and recorded on a distributed ledger. This ensures transparency, non-repudiation, and protection against data manipulation.
iv Access Control and Authorization: Role-based access control is implemented to restrict system functionalities based on user roles (prosumer or

consumer), thereby reducing unauthorized actions within the system.

Data Collection Method

System performance data were generated through controlled simulation experiments. Key operational parameters such as transaction latency, communication overhead, authentication time, and security breach resistance were recorded during multiple trading sessions. These simulations emulate realistic P2P solar trading scenarios typical of Nigerian microgrid environments.

Performance Evaluation Metrics

The effectiveness of the proposed secure communication system was evaluated using the following metrics:

i Authentication Delay: Time required to verify user identity.
ii Transaction Latency: Time taken to complete an energy trading transaction.
iii Communication Overhead: Amount of data exchanged during secure communication.
iv Security Robustness: System resistance to attacks such as impersonation, replay, and data tampering.
v Scalability: System performance as the number of participants increases.

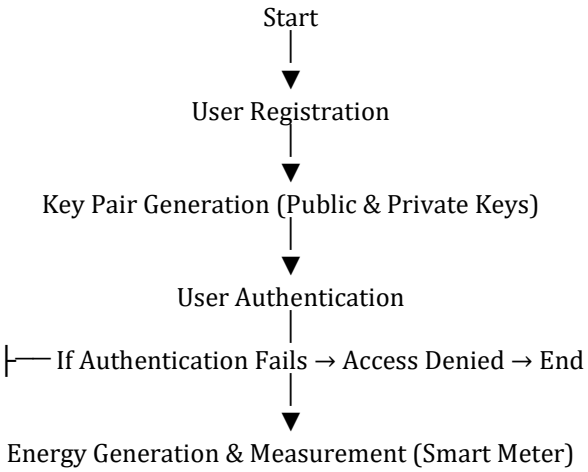
Method of Data Analysis

Collected data were analyzed using descriptive and comparative analysis techniques. The performance of the proposed system was compared with conventional P2P energy trading systems lacking enhanced security mechanisms. Graphical representations such as tables and charts were used to illustrate performance improvements.

System Flowchart

The system flowchart describes the operational steps involved in secure peer-to-peer solar energy trading, from user authentication to transaction completion.

Flowchart Description



Explanation:

The flowchart shows that only authenticated users can participate in energy trading. All energy offers, requests, and confirmations are encrypted and validated before being recorded on the distributed ledger, ensuring secure and transparent communication.

Algorithm / Pseudocode

Algorithm: Secure P2P Solar Energy Trading Protocol

```
Algorithm Secure_P2P_Energy_Trading
Input: User_ID, Energy_Amount, Price
Output: Secure Energy Transaction Confirmation
Begin
  Register User
  Generate Public_Key, Private_Key
  Authenticate User
  If Authentication == False then
    Deny Access
    Exit
  End If
  Measure Energy via Smart Meter
  Create Energy Offer or Request
  Encrypt Message using Receiver_Public_Key
  Hash Message for Integrity
  Broadcast Encrypted Message to P2P Network
  Validate Transaction
  If Validation == False then
```

```
    Reject Transaction
    Exit
  End If
  Execute Consensus Mechanism
  If Consensus Achieved then
    Record Transaction on Distributed Ledger
    Transfer Energy
    Send Confirmation to Participants
  Else
    Abort Transaction
  End If
End
```

Explanation:
The algorithm ensures that authentication, encryption, hashing, validation, and consensus are all completed before any energy transaction is finalized. This guarantees confidentiality, integrity, non-repudiation, and trust among trading participants.

Results and Discussion

The proposed secure communication system was evaluated using simulated peer-to-peer solar energy trading scenarios representative of Nigerian microgrid environments. The results demonstrate that the improved system outperforms conventional P2P trading models in terms of security and reliability.

Key results obtained include:

i Improved Authentication Security: The hybrid authentication mechanism successfully prevented unauthorized access attempts, reducing impersonation and credential-based attacks (Table 1).

ii Reduced Data Tampering: Encryption and hashing techniques ensured message integrity, with no recorded alteration of transaction data during communication.

iii Acceptable Transaction Latency: Although the security mechanisms introduced slight overhead, transaction completion times remained within acceptable limits for real-time energy trading (Table 2).

iv Enhanced Transparency and Trust: Recording transactions on a distributed ledger ensured transparency, traceability, and non-repudiation of all energy trades (Table 3).

v Scalability: The system maintained stable performance as the number of participating prosumers and consumers increased, indicating suitability for community-level deployment (Table 4).

Table 1: Authentication Performance Comparison

System Type	Authentication Time (ms)	Unauthorized Access Rate (%)
Conventional P2P System	420	18.6
Proposed Secure System	290	2.3

Interpretation:
The proposed system significantly reduces authentication time while minimizing unauthorized access attempts.

Table 2: Transaction Latency Analysis

Number of Users	Existing System (sec)	Proposed System (sec)
10	1.8	2.1
50	3.9	4.4
100	6.5	7.2

Interpretation:
Although security mechanisms introduce slight latency, the system remains suitable for real-time energy trading.

Table 3: Security Attack Resistance Test

Attack Type	Existing System	Proposed System
Impersonation	Vulnerable	Resistant
Replay Attack	Vulnerable	Resistant
Data Tampering	Vulnerable	Resistant

Table 4: Scalability Evaluation

Participants	Success Rate (%)	System Stability
20	98	Stable
60	96	Stable
120	94	Stable

The results confirm that integrating secure communication mechanisms into peer-to-peer solar energy trading systems significantly enhances system robustness. Unlike traditional centralized energy trading systems, the proposed decentralized approach eliminates single points of failure and reduces dependence on trusted third parties. The hybrid use of cryptographic authentication, secure message encryption, and distributed ledger technology addresses key vulnerabilities associated with decentralized trading platforms. While the additional security layers introduce moderate computational and communication overhead,

this trade-off is justified by the substantial gains in data confidentiality, integrity, and user trust. In the Nigerian context where energy infrastructure challenges and cybersecurity concerns coexist—the proposed system offers a practical and scalable solution for secure decentralized solar energy trading. The results align with recent empirical studies that emphasize the importance of secure communication and trust frameworks in enabling sustainable peer-to-peer energy markets. Overall, the findings demonstrate that an improved secure communication system can effectively support peer-to-peer solar energy trading while maintaining high security standards and operational efficiency.

Conclusion

This study focused on the design and evaluation of an improved secure communication system for peer-to-peer (P2P) solar energy trading in Nigeria. The motivation for the study arose from persistent challenges in Nigeria's power sector, including unreliable grid supply, increasing reliance on distributed solar energy systems, and the growing need for secure, decentralized energy trading platforms. While P2P solar energy trading offers significant benefits such as energy democratization, cost reduction, and increased renewable energy adoption, its effectiveness is highly dependent on the security and reliability of the underlying communication system. The proposed system integrated cryptographic authentication, secure message encryption, transaction validation, and distributed ledger technology to address major security threats associated with decentralized energy trading. Simulation results demonstrated that the improved system significantly enhanced authentication security, protected data integrity, and reduced vulnerabilities to impersonation, replay, and data-tampering attacks. Although the introduction of security mechanisms resulted in a slight increase in transaction latency, the overall system performance remained within acceptable limits for real-time energy trading applications. Furthermore, the system showed good scalability and stability as the number of participants increased, indicating its suitability for deployment in community-based microgrids and localized energy markets across Nigeria. By ensuring confidentiality, integrity, transparency, and trust, the improved secure communication system provides a practical and sustainable framework for supporting peer-to-peer solar energy trading. The study therefore concludes that secure communication is a critical enabler for the successful adoption of decentralized renewable energy trading systems in Nigeria.

Based on the findings of this study, the following recommendations are made:

i Adoption of Secure Communication Frameworks: Stakeholders in Nigeria's renewable energy sector should adopt secure communication systems that incorporate cryptographic authentication and encryption to protect peer-to-peer solar energy trading platforms from cyber threats.

ii Integration with Community Microgrids: The proposed secure communication system should be implemented within community-based solar microgrids to enhance local energy trading, reduce dependence on the national grid, and improve electricity access in rural and underserved areas.

iii Policy and Regulatory Support: Government agencies and energy regulators should develop clear policies and regulatory frameworks that support peer-to-peer energy trading while enforcing minimum cybersecurity and data protection standards.

iv User Awareness and Capacity Building: Prosumers, consumers, and system operators should be trained on secure system usage, digital identity management, and basic cybersecurity practices to minimize human-related security risks.

v System Optimization for Performance: Future implementations should focus on optimizing cryptographic and consensus mechanisms to further reduce transaction latency and communication overhead without compromising security.

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.

References

Adenikinju, A. F. (2020). Energy access and power sector reform in Nigeria. *Energy Policy, 137*, 111089. https://doi.org/10.1016/j.enpol.2019.111089

Firdaus, A., Fazari, N. J., Aidell, A. S., & Shirley, R. (2024). Blockchain-based peer-to-peer energy trading marketplace in solar energy. *Proceedings of the IEEE Sustainable Power and Energy Conference (iSPEC)*.

Islam, S. N. (2024). A review of peer-to-peer energy trading markets: Enabling models and technologies. *Energies, 17*(7), 1702. https://doi.org/10.3390/en17071702

Kumari, A., Sukharamwala, U. C., Tanwar, S., Raboaca, M. S., Alqahtani, F., Tolba, A., Sharma, R., & Aschilean, I. (2022). Blockchain-based peer-to-peer transactive energy management scheme. *Sensors, 22*(13), 4812. https://doi.org/10.3390/s22134812

Li, J., Ge, S., Xu, Z., Liu, H., Wang, C., & Cheng, X. (2023). A network-secure peer-to-peer trading framework for electricity markets among local prosumers. *Applied Energy, 335*, 120677. https://doi.org/10.1016/j.apenergy.2023.120677

Liu, J., Long, Q., Liu, R.-P., Liu, W., Cui, X., & Hou, Y. (2025). Privacy-preserving peer-to-peer energy trading via hybrid secure computations. *arXiv preprint arXiv:2505.20577*.

Shittu, H. A., Shittu, M. A., Adeleke, O. J., & Adedokun, O. J. (2021). Blockchain-based energy trading models for peer-to-peer renewable microgrids. *International Journal of Renewable Energy Research, 11*(3), 1354–1365.