Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Enhancing Smart Grid Security and Renewable Energy Integration through Advanced Encryption, Game Theory, and Blockchain Solution

Shikha Kuchhal[1], Ikbal Ali[2], Ibraheem[2]

[1]Research Scholar, Department of Electrical Engineering, Jamia Millia Islamia, India
[2]Professor, Department of Electrical Engineering, Jamia Millia Islamia, India
Email: shikhakuchhal4@gmail.com

Modern technology of the smart grids' integration will help to solve problems in sustainability, security, and energy efficiency. This article proposes innovative approaches leveraging blockchain, game theory, Advanced Encryption Standard (AES) to enhance smart grid systems. AES locks real-time communication inside smart grids, therefore ensuring data security without compromising system speed. Game theory is used to construct models of interactions between smart meters, electric vehicles (EVs), and central systems so providing strategies to lower cyber-attacks including Sybil, denial-of- service (DoS), and repeat attacks. In distributed energy markets, integrated blockchain technology guarantees open, tamper-proof transactions, therefore enabling safe peer-to--peer (P2P) energy exchange. Furthermore, this work addresses the significant challenges in including solar and wind energy sources into smart networks. By use of optimisation strategies, variation is controlled, grid stability is maintained, and the sustainability of energy systems is enhanced. Combining these technologies tries to offer a whole framework improving smart grid resilience, energy distribution, and communication security. Simulations and case studies validate the proposed solutions revealing interesting advances in the fields of secure smart grid connectivity, EV security, and renewable energy integration. This effort enables sustainable, safe, and efficient energy systems capable of meeting not only the demands of present infrastructure but also the increasing cyber and operational hazards.

Keywords: Smart Grids, Advanced Encryption Standard (AES), Game Theory, Blockchain Technology, Cybersecurity, Renewable Energy Integration, Solar Energy, Wind Energy

1. Introduction

Smart grids are core of future energy infrastructure as growing worldwide needs for sustainable and efficient energy solutions as well as the increasing complexity of modern energy systems point to. Smart grids mix advanced communication and control technologies to offer real-time monitoring, efficient energy distribution, and increased dependability. But as smart grids grow more common, the challenges they bring—especially with relation to cybersecurity, integration of renewable energy sources, and communication efficacy—also advance. From cyber threats such denial-of- service attacks, Sybil attacks, and data breaches, strong security measures are required to safeguard the confidentiality, integrity, and availability of vital grid activities [1]. The Advanced Encryption Standard (AES) applied in real-time communication systems offers a feasible answer by assuring safe data transmission without compromising system efficiency. Including game theory into smart grid security also provides a strategic framework for using optimum decision-making and predictive modelling to investigate and lower cyber-attacks. Beyond security, the inclusion of renewable energy sources as solar and wind into smart networks includes extra complexity because of their natural volatility and unpredictability." Good management of these renewable sources determines whether grid stability is maintained and whether sufficiently satisfying energy needs are achieved. Thus, advanced optimisation techniques are required to balance supply and demand thereby maximising the usage of clean energy. Blockchain technology especially seems to be a transformational instrument for permitting safe, transparent, and distributed energy trade among users, thereby enhancing the resilience and efficiency of smart grids, especially in peer-to- peer (P2P) marketplaces [2]. To solve these challenges, this work suggests an integrated framework incorporating AES encryption, game-theoretic models, blockchain solutions, and renewable energy optimisation. By means of better security, sustainability, and operational efficiency of smart grids, this study aims to support the global transition to renewable energy and sustainable development in addition to being strong against developing cyber threats.

2. Background

Importance of Smart Grids in Modern Energy Systems

By redefining how power is produced, distributed, and used, smart grids meet the rising need for consistent, efficient, and sustainable energy systems in contemporary society. Smart grids include advanced communication and control technologies that permit two-way energy and information exchange between utilities and consumers, unlike traditional power grids which work on a centralised and linear paradigm. Real-time monitoring, predictive maintenance, and fast response to disturbances—that is, by means of which grid dependability is strengthened—this capability reduces outages and enhances service quality [3]. By means of demand-side technology as smart meters and dynamic pricing, smart grids also enable users to actively participate in energy management hence optimising energy use and lowering costs. Fighting climate change and lowering greenhouse gas emissions relies on the clever grid integrating solar and wind sources being included into. Smart grids help to solve the volatility of renewable energy by employing complex algorithms and energy storage devices to balance supply and demand, therefore providing a continuous and sustainable power supply.

Moreover, underscored by the development of distributed energy resources (DERs) and electric vehicles (EVs) is the need of smart grids in modernising energy infrastructure to meet new technologies. Through its ability to permit distributed energy generation and peer-to-peer energy trade, smart grids offer the route for more equitable and strong energy systems that reduce dependency on fossil fuels [4]. Their capacity to mix current technologies including artificial intelligence, machine learning, and blockchain for enhanced automation, security, and openness establishes them as a critical aspect of next energy networks. Smart grids are crucial overall since they enable energy systems to be intelligent, adaptable, and efficient infrastructures that serve changing needs of consumers, utilities, and the environment, thereby guaranteeing a sustainable and energy-secure future.

Challenges in Security, Efficiency, and Renewable Energy Integration

Although smart grids provide many advantages, their universal adoption and optimal performance are hampered by their main challenges in security, efficiency, and renewable energy integration, therefore undermining their benefits. Security is one of the most critical problems since depending on advanced communication networks and digital technology increases vulnerability to cyberattacks like data breaches, viruses, and denial-of-service attacks. Strong cybersecurity is essential vital since these risks could compromise important data, disrupt grid operations, and jeopardise the dependability of the electrical supply [5]. Maintaining the confidentiality, integrity, and availability of data carried via the grid is essential yet challenging given the range of devices, systems, and involved parties. Efficiency is another major challenge since smart grids must maximise energy use and distribution by analysing vast amounts of real-time data, hence lowering losses [6]. Advanced algorithms and robust infrastructure are therefore needed to appropriately handle demand changes, energy storage, and distributed generation. Including renewable energy sources introduces still another degree of complication since solar and wind power are naturally inconsistent and dependent on the weather, thereby challenging grid reliability and stability.

Grid management systems, energy storage technology, and advanced forecasts help to balance the erratic supply of renewable energy with the continuous need for electricity. Moreover, incorporate distributed energy resources as community wind farms and rooftop solar panels demand overcoming technological, legal, and financial constraints to guarantee equal access to energy and smooth grid connectivity. Another challenge is interoperability between new technologies and old grid architecture since traditional systems were not designed to manage bidirectional or distributed producing of energy flow [7]. Dealing with these problems requires a whole strategy combining technological innovation, legislative support, and stakeholder engagement to ensure that smart grids may deliver their promise of generating safe, effective, and sustainable energy systems.

Challenges Faced by Smart Grids

Smart grids have various challenges that impede their implementation and operation especially in security, efficiency, and the integration of renewable energy sources, even although they are necessary for modernising energy infrastructure. Depending on connected equipment and current communication networks, smart grids are quite prone to cybersecurity problems. Important data can be compromised by denial-of- service (DoS), man-in-middle (MITM), and data breaches therefore compromising the dependability and stability of the electrical supply

[8]. The distributed character of smart grids together with their integration of millions of devices including smart meters, electric vehicles (EVs), and distributed energy supplies increases the attack surface and consequently necessitates strong security measures. Efficiency is another main challenge since smart grids have to gather and assess massive amounts of real-time data to maximise energy distribution, track grid performance, and predict demand changes.

This requires advanced data processing and infrastructure; nevertheless, poorly thought-out infrastructure can lead to system inefficiencies, energy losses, and congestion. The intermittent and irregular nature of renewable energy sources like solar and wind presents greater difficulties in integration. Advanced forecasting methods, real-time grid management, and energy storage systems enable to balance supply of renewable energy with ongoing consumption of electricity. Furthermore, the mix of modern smart technologies and legacy grid architecture causes compatibility issues since traditional systems were designed not to control bidirectional energy flow or distributed energy generation [9]. Regulatory and financial challenges also prevent the perfect integration of renewable energy since utilities and stakeholders have to adapt to new rules, standards, and business models. These challenges highlight generally the need of a comprehensive and imaginative approach to guarantee that smart grids may meet their promise of providing safe, efficient, and sustainable energy systems.

Need for Innovative Solutions

Growing complexity and susceptibility of smart grids demand innovative solutions to address security issues, operational inefficiencies, and integration challenges with renewable energy. Preventing cyberattacks and preserving operational dependability rely on security guarantees of confidentiality, integrity, and data availability distributed over the grid [10]. The dynamic and distributed aspect of smart grids renders conventional security approaches insufficient; however, modern encryption techniques such the Advanced Encryption Standard (AES) become even more important to ensure real-time communication. Moreover, game theory offers a strategic framework to replicate interactions between grid components, so facilitating the prediction and lowering of cyber risks with reference to optimal defensive strategies. Great volumes of real-time data help to increase efficiency in smart grids by means of optimisation techniques able to balance supply and demand and avoid losses. Machine learning and artificial intelligence (AI) are also applied to improve demand response systems, forecast energy use trends, and optimise use of energy storage.

Control of fluctuation and assurance of grid stability demand innovative methods addressing integration of renewable energy. Modern solar and wind energy forecasting systems together with choices for energy storage—batteries and pumped hydro storage aid to lower supply fluctuations. Furthermore, since blockchain technology enables safe peer-to--peer (P2P) energy exchange and open transaction records possible, it presents a novel solution for distributed energy markets [11]. Blockchain smart contracts aid automated energy trading even if they guarantee transaction integrity and traceability. These innovative concepts taken holistically could transform smart grids into robust, safe, efficient systems capable of meeting future energy use.

Technological Advancements for Smart Grids

Technological advancements are changing smart grids and also providing the tools to solve security, efficiency, and renewable energy integration challenges. Especially under high-volume, low-latency needs, encryption techniques as the Advanced Encryption Standard (AES) are critically necessary in securing smart grid communication by safeguarding data integrity and confidentiality in real-time. AES raises the general dependability of grid operations by ensuring that private data transmitted over the grid stays unreachable to illicit groups [12]. Game theory becomes a very useful tool for managing cybersecurity by providing a strategic framework to model and lower possible cyberattacks. By simulating interactions between attackers and defenders, game theory helps to identify optimal defence strategies so handling denial-of- service attacks or safeguarding of data flow in smart meters and electric vehicles (EVs.). By permitting safe peer-to--peer energy trading, blockchain technology's adoption into smart grids helps to improve security and efficiency even more. Blockchain supports distributed energy markets whereby consumers may trade extra energy, such solar electricity, straight with their neighbours and guarantees tamper-proof transaction records. Blockchain smart contracts provide openness and automatically handle transactions, therefore reducing the need for middlemen [13]. Artificial intelligence (AI) and machine learning (ML) are thus also transforming smart grids by letting predictive analytics for demand forecasting, grid optimisation, and trouble identification.

These technologies increase energy efficiency by means of real-time data-based decision automation, energy distribution optimisation, and anomaly discovery prior to its more relevance. Flow batteries and lithium-ion batteries are two important developments in energy storage technologies that help to solve the intermittency of solar and wind energy therefore enabling the integration of renewable energies [14]. Together with grid management systems, these technologies ensure constant electricity supply even in times of low renewable generating." Additionally allowing grid operators to precisely control supply and demand changes are advanced forecasting techniques predicting sun irradiation and wind patterns. "By combining these innovative technologies, so opening the path for a strong and flexible energy infrastructure, smart grids can reach hitherto unheard-of degrees of security, efficiency, and sustainability.

3. Review of literature

N. Suhaimy, (2022) study provides a comprehensive review on smart grid communication and its possible solutions for a reliable two-way communication toward supporting diversified power grid applications. Existing networking methods along with their advantages and weaknesses are highlighted for future research directions. The communication network architecture in the smart grid, with details on each networking technology, switching methods and medium for data communication, is critically reviewed to identify the existing research gaps.

K. A. Abdulsalam et al. (2023) presented an overview of the application of communication technologies in the digitalization of the power systems network. It reviews smart grid communication technologies, their features, relevance, and various roles being played toward

delivering an effective electrical service to stakeholders. Hence, this study focused on wireless and wired communication technologies applicable to smart grid applications.

P. Soni et al. (2021) provided a survey of different communication technology, applications, benefits and challenges in communication infrastructure, spatially IoT. India's electrical power system grid also known as the power grid is serving us from a very long time. In this duration, there were no major developments or changes reported in the power grid system. Electrical power consumer demand is increasing drastically and the present grid system is not able to fulfil these emerging requirements. To fulfil the requirements of future power load, we need a modified system which has to be reliable, secure, intelligent and efficient.

A. Y et al. (2023) comprehensively reviews cyber-physical, cyber-security, and key components of cyber-attacks. Then we present each section in detail and thoroughly the standards and principles of cyber-physical and cyber-security attacks in smart grid systems. This paper gives a deep understanding of cyber-security systems in smart grid system applications.

C. -M. Chen, et al. (2024) Industry 5.0, a revolutionary paradigm focused on intelligent manufacturing, has profoundly impacted the automotive industry. It offers reliable data transmission and enhances the security of vehicle network systems, meeting evolving consumer needs. With a growing emphasis on energy conservation and environmental protection, electric vehicles have become a prominent segment of clean energy vehicles. Ensuring convenient and secure charging services is crucial for their widespread adoption. To address this, we propose an authentication protocol that uses digital signatures for secure communication in consumer-centric electric vehicle charging in Industry 5.0 environments [5].

Y. Wang et al., (2023) organization and management of electricity markets worldwide are rapidly evolving, moving towards decentralized, distributed, and renewable energy-based generation with solutions based on real-time data exchange. A Vehicle-to-Vehicle (V2V) energy trading has emerged as one of the most promising alternatives for relieving the load imposed on the traditional grid enabling two individuals to buy and sell energy directly without intermediaries. However, the Internet of Electric Vehicles (IoEV) environment is thrustless, and such P2P energy trading is prone to different kinds of cyber-attacks. Blockchain technology has lately been proposed to implement V2V energy trading to securely and fairly share energy.

P. Razmjoui et al. (2024) provides a data protection assessment of radio frequency electronic system in the tire pressure monitoring system (TPMS). It is demonstrated that eavesdropping is completely feasible from a passing car, at an approximate distance up to 50 m. Furthermore, our reverse analysis shows that the static n -bit signatures and messaging can be eavesdropped from a relatively far distance, raising privacy concerns as a vehicles' movements can be tracked by using the unique IDs of tire pressure sensors.

M. Omar, et al., (2023) addresses these issues by proposing a framework of energy trading based on blockchain and smart contracts. The energy transfer between vehicles is performed via a distributed coalition of unmanned aerial vehicles transporting the electric energy from selected sellers to a needy requester vehicle. The selection mechanism of sellers aims to

maximize the service availability and fault-tolerance and minimize both the energy transportation latency and overhead.

S. Shirvani et al. (2024) identify gaps in the security profiling of EVs and categorize them into five components: 1) charging station security, 2) information privacy, 3) software security, 4) connected vehicle security, and 5) autonomous driving security. Our study provides a comprehensive analysis of identified vulnerabilities, threats, challenges and attacks for different EV security aspects, along with their possible surface/subsurface and countermeasures.

W. Tushar et al., (2023) bridges this gap by 1) providing a general discussion of different types of CPS and their characteristics; 2) giving an overview of different types of game-theoretic approaches; 3) explaining why game theory is appropriate for modeling different types of CPS; and 4) finally, studying how game theory has been used in different CPS types to address their challenges.

4. Methodology:

Research Objectives

1. Secure Communication and Smart Game Theory Implementation in Smart Meters

Process Flow for Implementing Game Theory-Based Security Measures

The process flow for implementing game theory-based security measures in SCADA systems, smart meters, and electric vehicles involves several key stages. Each stage is designed to address specific challenges and ensure the effectiveness of the security strategies. Below is a detailed process flow:

Fig Process Flow for Implementing Game Theory-Based Security Measures

This process flow ensures a structured approach to developing, implementing, and validating game theory-based security measures, addressing both theoretical and practical aspects to enhance the security of SCADA systems, smart meters, and electric vehicles.

Python-Based Implementation for Game Theory-Based Security Measures

Implementing game theory-based security measures using Python involves several steps, including developing models, programming algorithms, integrating with systems, and validating results. Below is a detailed guide on how to approach this implementation:

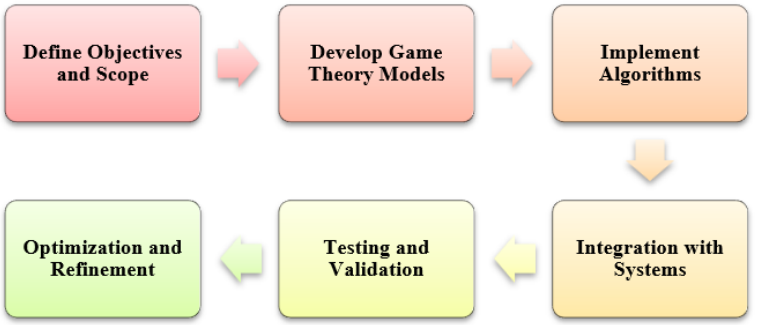


Fig Python-Based Implementation for Game Theory-Based Security Measures

1. Define Objectives and Scope

- Identify Threats: Clearly define the types of attacks you want to mitigate.
- Set Parameters: Determine the parameters and variables required for game theory models, such as utility functions, payoff matrices, and strategies.

2. Develop Game Theory Models

- Model Design: Develop the theoretical models for each type of attack using game theory principles. This includes defining:
  - Players: Entities involved in the game (e.g., attackers, defenders).
  - Strategies: Possible actions each player can take.
  - Payoff Matrix: Rewards or costs associated with different strategies.

For example, in a basic two-player game:

```
import numpy as np
 # Example payoff matrix for a simple game
 # Rows represent strategies for Player 1
 # Columns represent strategies for Player 2
 payoff_matrix = np.array([[3, 0], [5, 1]])
 # Example strategy for Player 1 and Player 2
 strategy_player1 = np.array([0.5, 0.5])  # Mixed strategy
```

```
strategy_player2 = np.array([0.5, 0.5])  # Mixed strategy
```

3. Implement Algorithms

- Algorithms for Strategy Computation: Implement algorithms to compute the optimal strategies using Python. This could involve solving for Nash equilibria or other game theory solutions.

For example, using a library like `Nashpy` to find Nash equilibria:

```
import nashpy as nash
# Define the payoff matrices for the players
A = np.array([[3, 0], [5, 1]])
B = np.array([[3, 5], [0, 1]])
# Create the game
game = nash.Game(A, B)
# Compute Nash equilibria
equilibria = game.support_enumeration()
for eq in equilibria:
    print("Nash Equilibrium:", eq)
```

- Real-Time Algorithms: Develop real-time algorithms for implementing and adjusting strategies based on live data and attack scenarios.

4. Integration with Systems

- Data Input: Implement functionality to handle real-time data from SCADA systems, smart meters, or EVs. This might involve reading data from sensors or network logs.

```
import pandas as pd
# Example of reading real-time data
data = pd.read_csv('real_time_data.csv')
```

- Security Protocols: Integrate the game theory-based algorithms with existing security protocols to enhance system protection.

5. Testing and Validation

- Simulation Testing: Test the game theory models using simulations to validate their effectiveness against various attack scenarios.

```
# Example simulation setup
def simulate_attack(model, attack_type):
# Implement logic to simulate attack and test model response
pass
```

- Real-World Testing: Deploy the models in real-world scenarios and collect data to evaluate their performance.

6. Optimization and Refinement

- Algorithm Optimization: Optimize the algorithms for performance, ensuring they can handle large-scale data and operate in real time.
- Model Refinement: Refine the game theory models based on testing results and feedback
- to improve accuracy and effectiveness.

5. Results:

Impact of Secure Communication and Smart Game Theory implementation in smart meters

To simulate and visualize the impact of Secure Communication and Smart Game Theory implementation in smart meters, we'll outline a simplified model using Python. In this simulation, we consider two key aspects:

1. Secure Communication: Consider an encryption mechanism (e.g., AES) that adds a computational delay but ensures secure data transmission.

2. Smart Game Theory: The model the system as a game where the utility (e.g., efficiency, cost, security) of different strategies (secure vs. insecure communication) is evaluated.

Each meter can choose between secure and insecure communication. The choice affects two outcomes: security and latency (or delay).

Simulation Parameters

- Number of smart meters: 100

- Probability of secure communication: Varies from 0 to 1

- Metrics:

  - Security Level: Higher for secure communication

  - Latency: Higher for secure communication

Implementation

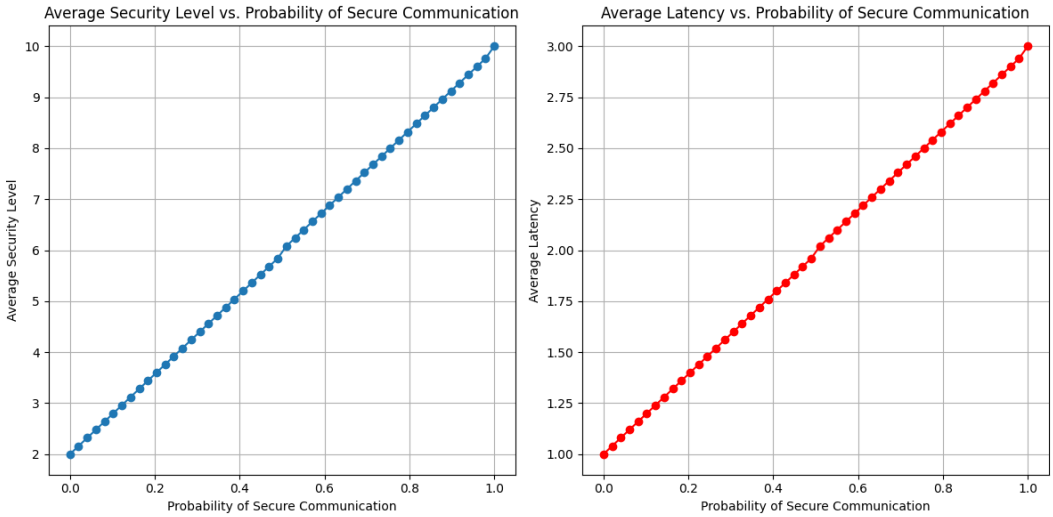
Simulation is made to plot the security level and latency for varying probabilities of choosing secure communication.

```python

import numpy as np

import matplotlib.pyplot as plt

# Parameters

num_meters = 100
```

```
probabilities = np.linspace(0, 1, 50)  # Probability of choosing secure communication
# Security and latency settings
security_insecure = 2
security_secure = 10
latency_insecure = 1
latency_secure = 3
# Arrays to hold results
avg_security_levels = []
avg_latencies = []
# Simulation
for p in probabilities:
    num_secure = int(p * num_meters)
    num_insecure = num_meters - num_secure
    avg_security = (num_secure * security_secure + num_insecure * security_insecure) / num_meters
    avg_latency = (num_secure * latency_secure + num_insecure * latency_insecure) / num_meters
    avg_security_levels.append(avg_security)
    avg_latencies.append(avg_latency)
# Plotting
plt.figure(figsize=(12, 6))
# Security Level Plot
plt.subplot(1, 2, 1)
plt.plot(probabilities, avg_security_levels, marker='o')
plt.title('Average Security Level vs. Probability of Secure Communication')
plt.xlabel('Probability of Secure Communication')
plt.ylabel('Average Security Level')
plt.grid(True)
# Latency Plot
plt.subplot(1, 2, 2)
plt.plot(probabilities, avg_latencies, marker='o', color='red')
```

```
plt.title('Average Latency vs. Probability of Secure Communication')
plt.xlabel('Probability of Secure Communication')
plt.ylabel('Average Latency')
plt.grid(True)
plt.tight_layout()
plt.show()
```

Output:



Explanation

- Security Level: The security level increases as more meters choose secure communication, providing better protection against attacks.

- Latency: The latency also increases with more secure communications due to the added overhead of encryption and other security measures.

This simulation visualizes the trade-off between security and latency in smart meter communication. By implementing secure communication, systems gain higher security at the cost of increased latency. The optimal strategy can be further analyzed using game theory, considering both the cost of security breaches and the impact of increased latency on system performance.

Simulation to visualize Attacks

To visualize that a game theory-based approach provides better security compared to a conventional security approach, we can use several metrics and charts to display the effectiveness of each approach. Some of the metrics could include:

1. Attack success rate: The percentage of attacks that succeed.

2. Defense success rate: The percentage of successful defenses.

3. Cost: The cost or resource consumption for each approach (time, computation, etc.).

4. Payoff: The overall benefit (payoff) for both attackers and defenders.

We can use several visualizations to make the comparison clearer:

1. Bar Chart: Attack Success Rate (Lower is Better)

- X-axis: Different types of attacks (Sybil, DoS, DDoS, MITM, Replay).

- Y-axis: Attack success percentage.

- Two bars for each attack type (one for the conventional approach and one for the game theory approach).

2. Bar Chart: Defense Success Rate (Higher is Better)

- X-axis: Different defense mechanisms.

- Y-axis: Defense success percentage.

- Again, two bars for each defense mechanism (conventional vs. game theory).

3. Line Plot: Cost Over Time

- X-axis: Time.

- Y-axis: Resource cost (computation, time, energy, etc.).

- Two lines representing cost growth for the conventional approach and game theory approach over time.

4. Scatter Plot: Payoff Matrix Comparison

- X-axis: Payoff for defenders.

- Y-axis: Payoff for attackers.

- Two sets of points (one for the conventional approach, one for the game theory approach).

- Nash equilibria points highlighted to show the optimal strategies under game theory.

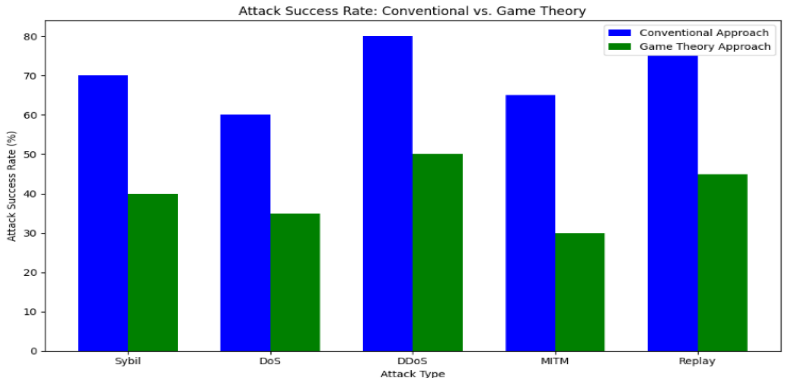


Fig Attack Success Rate

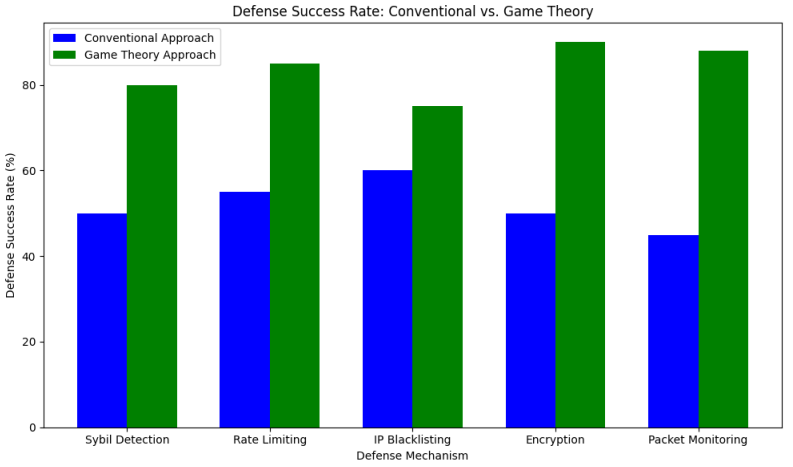


Fig Defense Success Rate

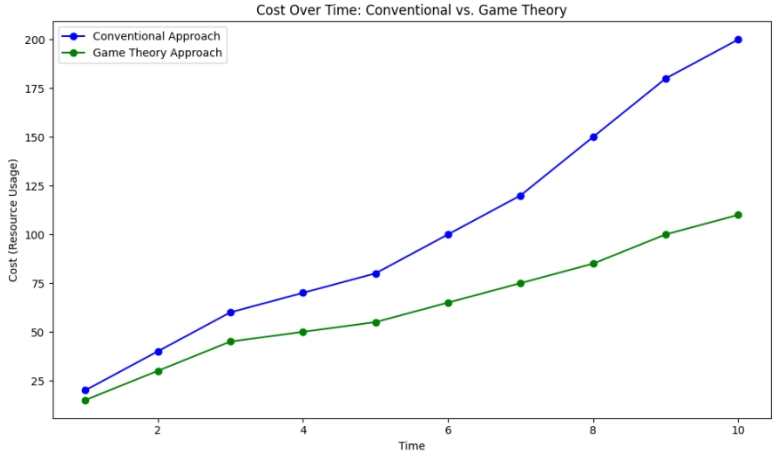


Fig Simulation of Cost over time

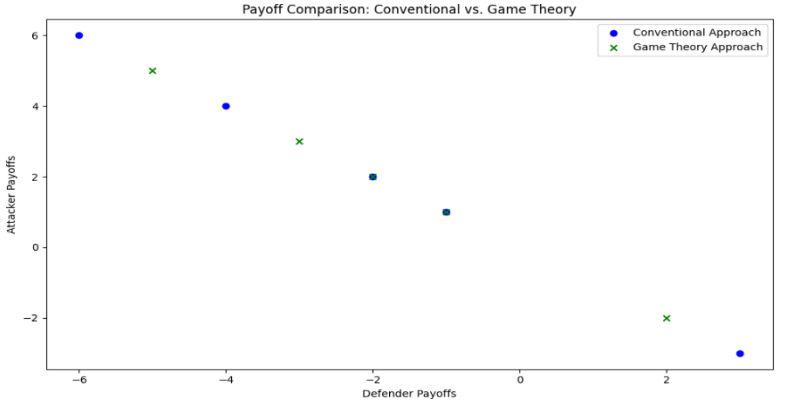


Fig Simulation of Attacker Payoff

Explanation:

1. Attack Success Rate Bar Chart:

- This shows the comparison of how frequently attacks succeed. A lower bar for the game theory approach indicates better security (fewer successful attacks).

2. Defense Success Rate Bar Chart:

- This compares the effectiveness of defenses. The higher success rate in the game theory approach indicates better defensive strategies.

3. Cost Over Time Line Plot:

- This shows how the resource consumption evolves over time for both approaches. The game theory approach tends to be more efficient with lower costs over time.

4. Payoff Comparison Scatter Plot:

- This visualizes the payoffs for attackers and defenders in both approaches, showing that game theory achieves a better balance (often at a Nash equilibrium) where attackers are less successful and defenders are more efficient.

Interpretation:

These visualizations illustrate that the game theory approach leads to a higher defense success rate, a lower attack success rate, and more efficient resource usage over time compared to a conventional security approach.

6. Conclusion

Solving the several difficulties of modern smart grids depends mostly on the integration of advanced technologies including AES encryption, game theory, and blockchain. The way these developments improve security, operational effectiveness, and the flawless integration of renewable energy sources into grid systems is shown in this study. Game theory maximises strategic decision-making to reduce cyber dangers, AES guarantees strong and real-time data security, and blockchain lets clear and tamper-proof energy transactions in distributed marketplaces.

Results of simulations support the effectiveness of these solutions by showing notable increases in grid resilience, cybersecurity, and renewable energy integration. Although issues including latency and implementation expenses still exist, the shown trade-offs between security and efficiency highlight the need of complete systems.

Future studies should concentrate on scaling these technologies for more general use, improving algorithms for real-time flexibility, and investigating policy and legal frameworks to enable general acceptance. Smart grids may develop into safe, effective, and sustainable energy systems by tackling these elements, therefore establishing the basis for a strong energy future.

References

1. N. Suhaimy, N. A. M. Radzi, W. S. H. M. W. Ahmad, K. H. M. Azmi and M. A. Hannan, "Current and Future Communication Solutions for Smart Grids: A Review," in IEEE Access, vol. 10, pp. 43639-43668, 2022, doi: 10.1109/ACCESS.2022.3168740.
2. K. A. Abdulsalam, J. Adebisi, M. Emezirinwune, and O. Babatunde, “An overview and multicriteria analysis of communication technologies for smart grid applications,” e-Prime - Advances in Electrical Engineering, Electronics and Energy, vol. 3. Elsevier BV, p. 100121, Mar. 2023. doi: 10.1016/j.prime.2023.100121.
3. P. Soni and J. Subhashini, “Future smart grid communication-deployment of IoT: opportunities and challenges,” Indonesian Journal of Electrical Engineering and Computer Science, vol. 23, no. 1. Institute of Advanced Engineering and Science, p. 14, Jul. 01, 2021. doi: 10.11591/ijeecs.v23.i1.pp14-22.
4. Y and A. S. Poornima, "Cyber-Physical Security System in Smart Grid-A Review," 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1-7, doi: 10.1109/ICCCNT56998.2023.10307396.
5. M. Chen, Q. Miao, F. Khan, G. Srivastava and S. Kumari, "Sustainable Secure Communication in Consumer-Centric Electric Vehicle Charging in Industry 5.0 Environments," in IEEE Transactions on Consumer Electronics, vol. 70, no. 1, pp. 1544-1555, Feb. 2024, doi: 10.1109/TCE.2023.3338818.
6. Y. Wang et al., "A Fast and Secured Vehicle-to-Vehicle Energy Trading Based on Blockchain Consensus in the Internet of Electric Vehicles," in IEEE Transactions on Vehicular Technology, vol. 72, no. 6, pp. 7827-7843, June 2023, doi: 10.1109/TVT.2023.3239990.
7. P. Razmjoui, A. Kavousi-Fard, T. Jin, M. Dabbaghjamanesh, M. Karimi and A. Jolfaei, "A Blockchain-Based Mutual Authentication Method to Secure the Electric Vehicles’ TPMS," in IEEE Transactions on Industrial Informatics, vol. 20, no. 1, pp. 158-168, Jan. 2024, doi: 10.1109/TII.2023.3257294.
8. M. Omar, A. Baz, H. Alhakami and W. Alhakami, "Reliable and Secure X2V Energy Trading Framework for Highly Dynamic Connected Electric Vehicles," in IEEE Transactions on Vehicular Technology, vol. 72, no. 7, pp. 8526-8540, July 2023, doi: 10.1109/TVT.2023.3251859.
9. S. Shirvani, Y. Baseri and A. Ghorbani, "Evaluation Framework for Electric Vehicle Security Risk Assessment," in IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 1, pp. 33-56, Jan. 2024, doi: 10.1109/TITS.2023.3307660.
10. W. Tushar et al., "A Survey of Cyber-Physical Systems From a Game-Theoretic Perspective," in IEEE Access, vol. 11, pp. 9799-9834, 2023, doi: 10.1109/ACCESS.2023.3239834.
11. C. Jatoth and S. Patil, “Price Optimization in Smart Grids through Blockchain in Cloud Computing based on Collocation Game Theory,” Proceedings of the 2024 13th International Conference on Software and Computer Applications. ACM, Feb. 2024. doi: 10.1145/3651781.3651832.
12. R. Masum, “A Review On Game Theory With Smart Grid Security.” arXiv, 2023. doi: 10.48550/ARXIV.2304.11738.
13. C. N. Priyanka and N. Ramachandran, "Analysis on Secured Cryptography Models with Robust Authentication and Routing Models in Smart Grid," International Journal of Safety & Security Engineering, vol. 13, no. 1, 2023.
14. A. Zibaeirad, F. Koleini, S. Bi, T. Hou, and T. Wang, "A Comprehensive Survey on the Security of Smart Grid: Challenges, Mitigations, and Future Research Opportunities," arXiv preprint arXiv:2407.07966, 2024.
15. G. Sharma, A. M. Joshi, and S. P. Mohanty, "sTrade: Blockchain based secure energy trading using vehicle-to-grid mutual authentication in smart transportation," Sustainable Energy Technologies and Assessments, vol. 57, p. 103296, 2023.

16. Gozgor, G.; Mahalik, M.K.; Demir, E.; Padhan, H. The impact of economic globalization on renewable energy in the OECD countries. Energy Policy 2020, 139, 111365.
17. Wei, L.; Yi, C.; Yun, J. Energy drive and management of smart grids with high penetration of renewable sources of wind unit and solar panel. Int. J. Electr. Power Energy Syst. 2021, 129, 106846.
18. Liu, B.; Rodriguez, D. Renewable energy systems optimization by a new multi-objective optimization technique: A residential building. J. Build. Eng. 2021, 35, 102094.
19. Noorollahi, Y.; Senani, A.G.; Fadaei, A.; Simaee, M.; Moltames, R. A framework for GIS-based site selection and technical potential evaluation of PV solar farm using Fuzzy-Boolean logic and AHP multi-criteria decision-making approach. Renew. Energy 2022, 186, 89–104.
20. Rajawat, A.S.; Mohammed, O.; Shaw, R.N.; Ghosh, A. Renewable energy system for industrial internet of things model using fusion-AI. In Applications of AI and IOT in Renewable Energy; Academic Press: Cambridge, MA, USA, 2022; pp. 107–128.
21. Imran, A.; Hafeez, G.; Khan, I.; Usman, M.; Shafiq, Z.; Qazi, A.B.; Khalid, A.; Thoben, K.-D. Heuristic-based programmable controller for efficient energy management under renewable energy sources and energy storage system in smart grid. IEEE Access 2020, 8, 139587–139608.
22. Hai, T.; Zhou, J.; Muranaka, K. Energy management and operational planning of renewable energy resources-based microgrid with energy saving. Electr. Power Syst. Res. 2023, 214, 108792.
23. Azad,A.; Shateri, H. Design and optimization of an entirely hybrid renewable energy system (WT/PV/BW/HS/TES/EVPL) to supply electrical and thermal loads with considering uncertainties in generation and consumption. Appl. Energy 2023, 336, 120782.
24. Worighi, I.; Maach, A.; Hafid, A.; Hegazy, O.; Van Mierlo, J. Integrating renewable energy in smart grid system: Architecture, virtualization and analysis. Sustain. Energy Grids Netw. 2019, 18, 100226.
25. Behera, S.; Choudhury, N.B.D. Adaptive Optimal Energy Management in Multi-Distributed Energy Resources by using Improved Slime Mould Algorithm with considering Demand Side Management. e-Prime-Adv. Electr. Eng. Electron. Energy 2023, 3, 100108.
26. Xia, M.; Shao, H.; Ma, X.; de Silva, C.W. A stacked GRU-RNN-based approach for predicting renewable energy and electricity load for smart grid operation. IEEE Trans. Ind. Inform. 2021, 17, 7050–7059.
27. Rehman,A.U.; Wadud, Z.; Elavarasan, R.M.; Hafeez, G.; Khan, I.; Shafiq, Z.; Alhelou, H.H. An optimal power usage scheduling in smart grid integrated with renewable energy sources for energy management. IEEE Access 2021, 9, 84619–84638
28. Dawoud, S.M. Developing different hybrid renewable sources of residential loads as a reliable method to realize energy sustainability. Alex. Eng. J. 2021, 60, 2435–2445.