# Cybersecurity For Smart Grid System Using Blockchain

Prof. Wadghule Y. M[1]. Prof. Abhale B. A[2,] Mr. Kadam Ram Suresh[3],
Mr. Wagh Abhishek Pravin[4], Mr. Patil Om Girish[5], Miss. Jadhav Mayuri Devidas[6]
*S.N.D College of engineering and research center, yeola Savitribai Phule Pune University*

*doi.org/10.64643/IJIRTV12I6-186797-459*

*Abstract*—**The rapid growth of smart grid technology is fundamentally reshaping the energy sector, enhancing power distribution and promoting more effective management of energy assets. Nevertheless, the increasing adoption of these sophisticated systems also introduces a significant challenge: cybersecurity vulnerabilities. As smart grids become increasingly interconnected and reliant on data exchange, they become susceptible to a wide array of digital threats, including unauthorized access, data breaches, an{rpfd system disruptions. Addressing these challenges is essential to preserving the resilience and security of our energy infrastructure.**

**Encouragingly, blockchain technology presents promising solutions to the cybersecurity challenges confronting smart grid systems. Originally developed to secure digital transactions in cryptocurrencies like Bitcoin, blockchain has emerged as a robust tool capable of bolstering security and trust across diverse applications. By leveraging its core attributes, such as distributed consensus, cryptographic techniques, and an immutable ledger, blockchain can help mitigate critical security concerns within smart grid systems. Furthermore, the tamper-proof nature of the blockchain ledger provides a transparent and auditable record of energy transactions and system operations, facilitating efficient monitoring, identification, and reaction to digital threats.**

*Index Terms*—**Cybersecurity; Smart Grid; Blockchain; Energy Security; Data Privacy; Smart Contracts; Decentralized Systems; IoT Security; Distributed Ledger Technology (DLT); Energy Management System; Secure Communication; Power Grid Protection.**

## I. INTRODUCTION

The rapid progress in energy delivery systems necessitates the evolution of smart grids. Integrating digital technology improves effectiveness and dependability, while also promoting environmental responsibility. Traditional, established energy systems generate power at large facilities and then transmit it through extensive networks to end-users. These older systems face numerous challenges, including limited energy management, significant waste during transmission, vulnerability to online threats, and difficulty integrating renewable energy resources. The adoption of smart grids is increasingly supported by the growing need for localized energy solutions that utilize advanced distribution strategies. Contemporary power generation and delivery rely on IT solutions to analyze and share data, as well as manage network automation.

A persistent and important difficulty involves preserving the safety, efficient operation, and dependability of the smart grid network. The convergence of digital threats targeting critical systems, coupled with concerns about data privacy and fraudulent energy usage readings, generates serious operational vulnerabilities that undermine the smart grid's effectiveness. To overcome this challenge, smart grids need creative solutions that incorporate blockchain and machine learning technologies, intending to strengthen operational resilience and enhance optimization abilities.

Blockchain provides a promising approach to address various challenges in modern power grids. Initially designed for secure financial dealings, blockchain's decentralized record-keeping system promotes open, secure, and unchangeable data sharing. By eliminating the need for central oversight, blockchain enables direct energy trading, ensuring secure transactions among users without intermediaries. This decentralized structure improves data security by guarding against unauthorized changes and reducing the risk of cyber threats. Energy trading utilizes smart contracts to automatically execute secure transactions based on pre-agreed terms. Overall, blockchain offers crucial security enhancements for smart grids and facilitates efficient energy transaction management.

## II. LITERATURE SURVEY

| Sr. No. | Paper Title | Author Name | Year |
|---|---|---|---|
| 1 | Blockchain-empowered security and privacy protection for smart grid. | Ya-Nan Cao, Yong Ding, | 2023 |
| 2 | Study of smart grid cyber-security, examining architectures and threats. | Batoul Achaal, Mehdi Adda, Ali Awde | 2024 |
| 3 | Blockchain-powered grids: Paving the way for a decentralised energy future. | Nazir Ullah,<br>Yudi Fernando,<br>Mohammed Habes | 2024 |
| 4 | When blockchain meets smart grids: A comprehensive survey. | Yihao Guo, Zhiguo Wan, Xiuzhen Cheng | 2022 |
| 5 | Blockchain-empowered security and privacy protection for smart grid. | Ya-Nan Cao , Yong Ding, Yujue Wang | 2023 |
| 6 | A hybrid AI-Blockchain security framework for smart grids. | Yazeed Yasin Ghadi,<br>Tehseen Mazhar, Tariq Shahzad | 2025 |
| 7 | Integrating Blockchain in Smart Grids for Enhanced Demand Response. | Paraskevas Koukaras, Konstantinos D. Afentoulis, Pashalis A. Gkaidatzis | 2024 |
| 8 | A Blockchain-Integrated AI Framework for Enhancing Smart Grid Energy Management. | Kajal Singh, S.B. Goyal, Anand Singh Rajawat | 2025 |
| 9 | SOH Prediction in Li-ion Battery Energy Storage System in Power Energy Network | Xiaofen Fang, Kai Fang, Lihui Zheng, Han Zhu, Qichang Zhuo & Jianqing Li | 2023 |
| 10 | Cybersecurity in smart microgrids using blockchain: threats & mitigations | Jameel Ahmad, Muhammad Riz wan, Usman Inayat | 2025 |

## III. METHODOLOGY

This research introduces a cybersecurity structure for intelligent power networks, leveraging blockchain technology. The approach aims to enhance data accuracy, verification, confidentiality, and reliability across network participants by employing distributed ledger technologies. The suggested structure guarantees protected communication, resilience to unauthorized access, and secure energy data exchanges.

The methodology involves six key steps: System Structure Planning, Data Movement Representation, Blockchain Incorporation, Agreement Protocol Application, Automated Agreement Creation, and Security Assessment.

System Architecture Overview

The proposed system architecture consists of five core layers:

Perception Layer: Collects real-time operational data from smart meters, sensors, and IoT-enabled devices across the grid.

Communication Layer: Ensures secure data transfer between grid nodes using encryption and blockchain-based verification.

Blockchain Layer : Stores all energy transactions and communication logs in an immutable distributed ledger shared among trusted nodes.

Smart Contract Layer: Automates authentication, access control, and billing through programmable smart contracts.Decision Layer: Triggers alerts, shutdown signals, or thermal mitigation based on severity analysis.

Application Layer: Provides a user interface for grid operators, utilities, and consumers for monitoring and management.

Data Acquisition

Information is collected from both artificial and actual intelligent power grid systems, encompassing smart meters, management facilities, and decentralized power sources. Key parameters collected include:

Meter readings (energy consumption and generation)

Device identifiers and timestamps Communication logs between nodes

Intrusion attempts and unauthorized access data

Blockchain Integration and Consensus Mechanism

The blockchain network is designed as a consortium (permissioned) blockchain, ensuring participation only from verified grid nodes (e.g., control centres,, substations, utilites).

Practical Byzantine Fault Tolerance (PBFT) is selected due to its high security and how latency.Each node validates new transactions, ensuring data consistency and trust. These features enable the ML models to learn temporal dependencies and degradation behaviour.

Smart Contract Development

Smart contracts handle the automation of key cybersecurity operations, such as:

Authentication: Verifies user or device identity before granting access. Access Control: Restricts unauthorized data manipulation.

Blockchain-based smart contracts enable distributed and automated security enforcement, removing the need for third-party verification. All actions—such as data exchange, energy trading, billing, and access control—are governed by code executed across a decentralized peer-to-peer network**.** Once deployed, the contract logic cannot be altered, thus ensuring immutability and transparency**.**

Algorithm

SHA-256 (Secure Hash Algorithm-256) is a cryptographic hash function that converts any input data into a fixed-length 256-bit (64-character) hash value.It is one-way (you can't reverse the hash to get the original data).Even a tiny change in input produces a completely different hash, ensuring data integrity.

Model Evaluation and Validation:

The framework is validated using a combination of simulation and analytical testing. Evaluation Metrics include:

Latency: Time taken to record and verify transactions

Throughput:Number of verified transactions per second

Scalability: Performance with increasing number of grid nodes

Security Strength: Resistance to cyber-attacks (e.g., man-in-the-middle, DDoS, spoofing)

Tools Used:

Ethereum Testnet / Hyperledger Fabric Wireshark for network analysis

Deployment Strategy:

The implementation approach for the suggested Blockchain-based Cybersecurity System within the Smart Grid prioritizes safe, adaptable, and immediate defense for all grid functions. The system utilizes a combined structure that integrates processing at the network's edge with blockchain networks hosted in the cloud to guarantee both quick response times and dependable performance.

Edge nodes (smart meters) Control centre (cloud) Distributed backup nodes

The system is scalable for residential, commercial, and utility-level smart grid networks.

## IV. OBJECTIVE

The main goal of this project is to create a protected and distributed cybersecurity system for smart grid networks, utilizing blockchain technology. The system intends to improve the privacy, accuracy, and accessibility of smart grid information by addressing the weaknesses of typical centralized setups. The project emphasizes incorporating blockchain-based identity verification, authorization management, and information confirmation methods to guard against cyber risks like information manipulation, impersonation, and unapproved access. By using smart agreements, the system computerizes essential security tasks, including user confirmation, energy exchange control, and irregular activity identification, ensuring openness and responsibility without outside involvement. Furthermore, the framework is engineered to offer immediate risk detection and secure interaction between spread-out grid points, guaranteeing that each exchange is permanently documented and confirmable. The application of agreement methods (like PBFT or PoS) assures confidence among grid users while keeping effective operation and minimal delays.

In conclusion, the aim is to establish a strong and unchangeable cybersecurity structure that protects important smart grid processes, encourages distributed energy control, and builds user confidence and system dependability in the future of advanced energy grids.

## V. PROBLEM DEFINATIONS

The electrical power system is rapidly transforming into a smart grid, incorporating advanced communication, IoT devices, and automated controls to improve efficiency, reliability, and sustainability. This digital shift enhances real-time oversight and distributed energy management but also introduces significant cybersecurity concerns. Traditional grid systems, once isolated and centralized, are now being replaced by interconnected smart grids heavily reliant on two-way communication and data sharing. This interconnectivity exposes the system to various cyber threats, including data alteration,unauthorized entry, denial-of-service attacks, and privacy violations.

In a smart grid, key components like smart meters, control centers, substations, and distributed energy resources (DERs) constantly exchange sensitive data over public or semi-public networks. Standard cybersecurity approaches—such as firewalls, encryption, and centralized access control—are often inadequate because they depend on a single trusted authority, which can become a point of vulnerability. If compromised, an attacker can access a large part of the network, manipulate billing information, alter power distribution commands, or disrupt significant portions of the grid. This centralized dependency also leads to challenges with expansion, lack of clarity, and high operating costs, making traditional solutions unsuitable for future smart grids.

Additionally, the increasing use of IoT-based energy devices introduces further weaknesses. Many IoT components lack strong security features, making them easy targets for malware, spoofing attacks, and man-in-the-middle intrusions. As the number of connected devices grows, so does the potential for attacks, making it harder to ensure the genuineness and completeness of every transaction and data exchange within the network. The absence of a decentralized, tamper-proof system for recording and validating grid transactions further increases the risk of data manipulation and fraud.

address these important issues, blockchain technology is emerging as a beneficial solution because of its decentralized, unchangeable, and clear nature. Blockchain enables shared trust among all participants without a central authority, ensuring all transactions are verified through a consensus process and stored permanently in a secure record. However, applying blockchain to smart grid cybersecurity is still a complex research problem. Issues like delay, expansion, energy use, and integration with existing systems must be addressed to achieve an effective and secure implementation,

Furthermore, current blockchain implementations in energy systems mainly focus on peer-to-peer (P2P) energy trading and billing clarity, often ignoring the cybersecurity aspect that protects communication, authentication, and control procedures. There is still a need for complete frameworks that combine blockchain with smart contracts to automate security procedures, manage access control, identify irregularities, and ensure data integrity across diverse grid networks.

Therefore, the main problem is developing a strong, blockchain-based cybersecurity framework capable of ensuring complete protection in smart grid environments. Such a framework must be able to withstand cyberattacks, verify the genuineness of all participants, maintain real-time transaction integrity, and operate efficiently without impacting system performance. Solving this problem is essential for building a reliable, resilient, and clear smart grid ecosystem, which is the basis for a sustainable and secure energy system in the digital age.

ARCHITECTURE

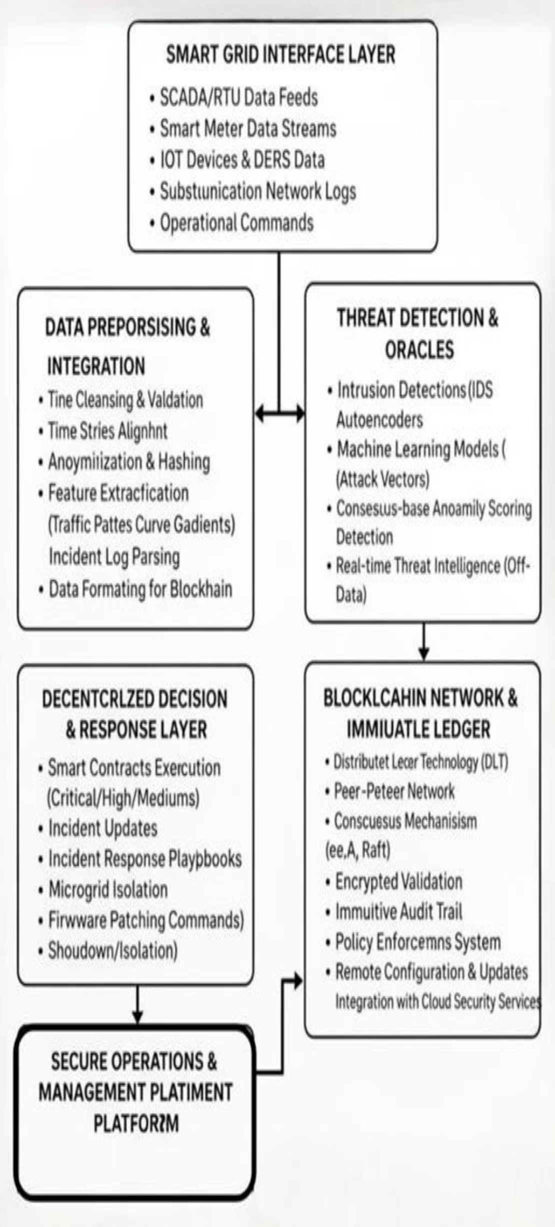
SMART GRID INTERFACE LAYER
• SCADA/RTU Data Feeds
• Smart Meter Data Streams
• IOT Devices & DERS Data
• Substunication Network Logs
• Operational Commands
DATA PREPORSISING & INTEGRATION
• Tine Cleansing & Valdation
• Time Stries Alignhnt
• Anoymiitization & Hashing
• Feature Extracfication (Traffic Pattes Curve Gadients) Incident Log Parsing
• Data Formating for Blockhain
THREAT DETECTION & ORACLES
• Intrusion Detections(IDS Autoencoders
• Machine Learning Models ( (Attack Vectors)
• Consesus-base Anoamily Scoring Detection
• Real-time Threat Intelligence (Off-Data)
DECENTCRLZED DECISION & RESPONSE LAYER
• Smart Contracts Execution (Critical/High/Mediums)
• Incident Updates
• Incident Response Playbooks
• Microgrid Isolation
• Firwware Patching Commands)
• Shoudown/Isolation)
BLOCKLCAHIN NETWORK & IMMIUATLE LEDGER
• Distributet Lecer Technology (DLT)
• Peer-Peteer Network
• Conscuesus Mechanisism (ee,A, Raft)
• Encrypted Validation
• Immuitive Audit Trail
• Policy Enforcemns System
• Remote Configuration & Updates Integration with Cloud Security Services
SECURE OPERATIONS & MANAGEMENT PLATIMENT PLATFORM

Fig. Smart grid security architecture with blockchain integration

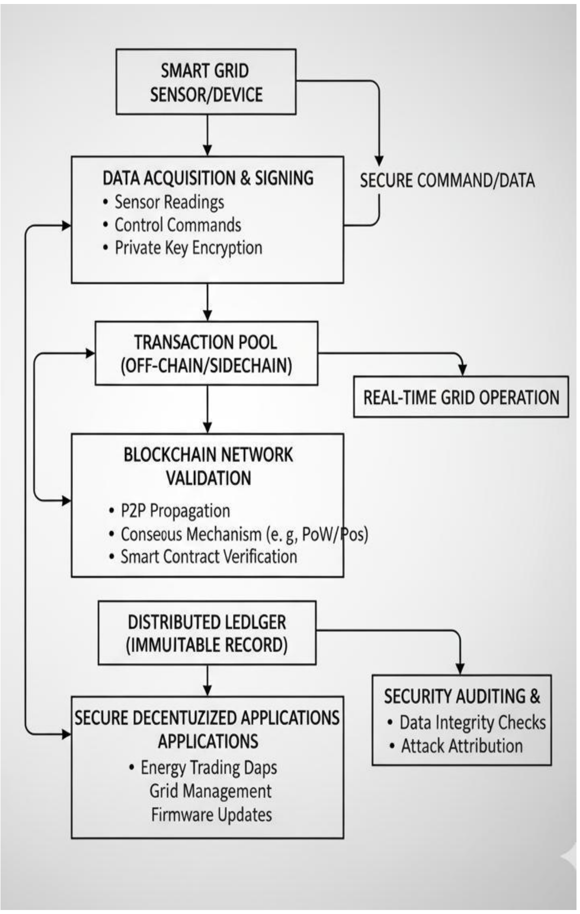

Fig. Transaction lifecycle in blockchain-based smart grid security

Blockchain Transaction Management

- Each grid transaction shall be recorded on a distributed ledger for immutability and traceability.
- The blockchain shall validate transactions using a consensus mechanism such as Practical Byzantine Fault Tolerance (PBFT)

## VI. FUCTIONAL REQUIREMENTS

The functional requirements define the essential features and operations of the proposed Blockchain-based Cybersecurity Framework for Smart Grid Systems. These requirements ensure secure communication, decentralized data integrity, and automated access control within the smart grid infrastructure.

Real-Time Data Acquisition:

- The system shall continuously collect real- time operational data from smart meters, IoT sensors, and distributed energy resources (DERs).

- Data types include:
- Power usage and generation values
- Device identifiers and timestamps
- Node communication logs or Proof of Stake (PoS).
- The ledger shall maintain a complete, tamper-proof record of all energy and communication events.
  - Transaction frequency patterns
  - Node authentication logs
  - Data integrity hash values
  - Network latency and packet flow rates
  - Energy transaction consistency metrics

Smart Contract Execution:

- The system shall use smart contracts to automate key cybersecurity operations, including:
  - User and device authentication
  - Access control and role-based permissions
  - Peer-to-peer (P2P) energy trading validation
  - Incident response to detect and isolate malicious nodes

Authentication and Access Control:

- Every device and user must undergo cryptographic authentication before participating in the network.
- The system shall generate public/private key pairs for all nodes.Access rights shall be assigned based on node roles (e.g., consumer, provider, control center).

Intrusion and Anomaly Detection:

- The system shall continuously monitor blockchain transactions and communication patterns to detect suspicious activity.
- Anomaly detection modules shall identify deviations such as:
  - Repeated failed authentication attempts
  - Unusual energy data patterns
  - Tampering or replay attacks
- Detected anomalies shall trigger alerts and activate smart contract-based isolation measures.

Data Privacy and Encryption:

- All communication between smart grid entities shall be encrypted using AES or RSA algorithms.
- Data stored on the blockchain shall be hashed using SHA-256 to ensure integrity and non-repudiation.
- Sensitive information such as user identity and billing details shall be pseudonymized to preserve privacy.

Monitoring and Reporting Dashboard:

- The system shall provide a real-time monitoring dashboard for grid administratos:
- The dashboard shall display:
  - Active blockchain transactions
  - Detected threats and alerts
  - Network performance statistics
- Reports shall be automatically generated for audit and compliance purposes.

Scalability and Interoperability:

- The framework shall support integration with multiple blockchain networks and grid systems.
- It shall allow seamless addition of new nodes without disrupting existing operations.
- The system shall maintain performance and latency below predefined thresholds as node count increases.

Alert and Response Mechanism:

- Upon detecting any cyber incident, the system shall:
  - Notify authorized administrators in real time
  - Record the incident in the blockchain ledger
  - Execute smart contract-based containment measures
  - Generate a security report for review and analysis

Fault Logging and Diagnostic Reporting:

- The system shall generate and store logs for all detected faults and abnormal events.
- Diagnostic reports shall include:
  - Timestamps
  - Sensor readings at the time of the event
  - Risk level classification
- The system shall support exporting logs in standard formats (e.g., CSV, JSON) for maintenance and post-event analysis.

## VII. NON FUCTIONAL REQUIREMENTS

The non-functional requirements ensure that the proposed ML-enhanced Battery Management System operates reliably, securely, efficiently, and is maintainable and scalable for long-term solar energy storage applications.

Performance:

- The system shall estimate SOC and SOH with:
  - Mean Absolute Error (MAE) ≤ 2%
  - Root Mean Square Error (RMSE) ≤ 3%
- The anomaly detection subsystem shall detect thermal events at least 10–15 minutes before critical thresholds are reached.
- The system shall respond to detected faults or anomalies within 500 milliseconds (latency requirement for safety actions).

Reliability:

- The system shall maintain an uptime of ≥ 99.5% under continuous operation.
- The thermal anomaly detection module shall achieve an F1-score of ≥ 0.90 on test datasets involving real and synthetic faults.

Compliance:

- The system shall comply with relevant safety and electrical standards for battery management systems, such as:
  - IEC 62619 (Safety for rechargeable batteries in industrial applications)
  - IEEE 1725 / 1625 (Battery system certifications)
  - Local data protection laws (e.g., GDPR, if applicable)

## VIII. CONCLUSION

The integration of blockchain technology into the cybersecurity architecture of smart grid systems represents a fundamental paradigm shift from centralized, perimeter- based security to a decentralized, trust-based model. Theoretically, this approach directly addresses the most critical vulnerabilities inherent in modern energy infrastructure by leveraging the core principles of decentralization, immutability, and cryptographic transparency.

Enhanced Resilience through Decentralization: By distributing control and data across numerous nodes, a blockchain- based architecture eliminates single points of failure. A successful cyberattack on one component (e.g., a substation or control center) would not compromise the entire network's integrity. This inherent resilience is critical for mitigating the risk of large-scale blackouts caused by targeted attacks like Denial-of-Service (DoS).

## REFERENCES

[1] Aklilu, Y. T., & Ding, J. (2022). Survey on Blockchain for Smart Grid Management, Control, and Operation. Energies, 15(1), 193. https://doi.org/10.3390/en15010193

[2] Appasani, B., Mishra, S. K., Jha, A. V., Mishra, S. K., Enescu, F. M., Sorlei, I.S., Bîrleanu, F.G., Takorabet, N., Thounthong, P., & Bizon, N. (2022). Blockchain-Enabled Smart Grid Applications: Architecture, Challenges, and Solutions. Sustainability, 14(14), 8801. https://doi.org/10.3390/su14148801

[3] "Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems." Journal of Modern Power Systems and Clean Energy, 2018, 6, 958-967.

[4] Guan, Z., Si, G., Zhang, X., Wu, L., Guizani, N., Du, X., & Ma, Y. (2018). Privacy- Preserving and Efficient Aggregation based on Blockchain for Power Grid Communications in Smart Communities. arXiv preprint, arXiv:1806.01056.

[5] Do Hai Son; Tran Thi Thuy Quynh; Tran Viet Khoa; Dinh Thai Hoang; Nguyen Linh Trung; Nguyen Viet Ha; Dusit Niyato; Nguyen N. Diep; Eryk Dutkiewicz (2022). An Effective Framework of Private Ethereum Blockchain Networks for Smart Grid. arXiv preprint, arXiv:2203.14633.

[6] Qing Yang, & Hao Wang (2021). Privacy-Preserving Transactive Energy Management for IoT-aided Smart Homes via Blockchain. arXiv preprint, arXiv:2101.03840.

[7] Luo, B., Xu, G., Xie, J., Wang, Y. (2022). A Blockchain-based Security Framework for Secure and Resilient Smart Grid. Journal of Physics: Conference Series.

[8] "Consortium blockchain based secure and

efficient data aggregation and dynamic billing system in smart grid.” Peer-to-Peer Networking and Applications, 2024, vol. 17, pp. 2717-2736.

[9] Yuanyuan Ma, Peng Yang, Huijie Guo, & Wenli Jia. Survey on the Application of Blockchain in Enhancing Mutual Trust in Smart Grid Transactions. Academic Journal of Science and Technology. “Frontiers | An efficient blockchain-based

[10] privacy preservation scheme for smart grids”. Communications and Networks (2025)

[11] “RETINA: Distributed and Secure Trust Management for Smart Grid Applications and Energy Trading.” Vaios Boulgouras, Thodoris Ioannidis, s