International Journal on
Technical and Physical Problems of Engineering
(IJTPE)
Published by International Organization of IOTPE

ISSN 2077-3528
IJTPE Journal
www.iotpe.com
ijtpe@iotpe.com

September 2025 | Issue 64 | Volume 17 | Number 3 | Pages 68-74

PROPOSED CYBERSECURITY FRAMEWORK FOR SMART GRIDS WITH BLOCKCHAIN INTEGRATION

I. Hammouti   A. Addaim   Z. Guennoun

*Smart Communications Research Team, University Center for Research in Space Technologies,
Mohammadia School of Engineers, Rabat, Morocco
iliasshammouti@research.emi.ac.ma, addaim@emi.ac.ma, zouhair@emi.ac.ma*

Abstract- The integration of conventional power grids with smart city technologies has paved the way for interactive, bidirectional communication within energy systems. Ongoing innovations in this field aim to improve the efficiency, reliability, cost-effectiveness, and environmental sustainability of electricity generation, distribution, and transmission through the deployment of smart grid solutions. To unlock the full potential of smart grids, it is essential to overcome major challenges associated with connectivity and the coordination of complex systems. Among the most pressing concerns are security risks linked to energy resource management and the stability of grid operations, both of which are crucial for maintaining safety and reliability. Additionally, the growing scale of data transmission within smart grid infrastructures introduces new demands related to cybersecurity and overall system efficiency. This study explores essential aspects of smart grid systems, with an emphasis on communication networks, demand response mechanisms, and, most notably, cybersecurity. It also investigates the integration of blockchain technology as a means to address these challenges, particularly in the context of managing decentralized energy sources.

Keywords: Smart Grids, Cybersecurity, Blockchain, Artificial Intelligence (AI), Data Protection, Peer-to-Peer (P2P) Energy Trading, Machine Learning, Predictive Maintenance, System Scalability.

1. INTRODUCTION

The transformation of the energy sector through smart grid technologies has introduced a complex, decentralized, and highly dynamic ecosystem. This evolution enables advanced demand response, distributed generation, electric vehicle integration, and bidirectional communication between utilities and end-users. However, the increased interconnectivity and digitalization expose the grid to significant cybersecurity vulnerabilities. The communication infrastructure underpinning smart grids is intrinsically sophisticated and continues to evolve with the integration of IoT, cloud computing, and real-time monitoring systems. Additionally, the expectation for continuous connectivity across all grid elements significantly amplifies their vulnerability to cyber threats. Attacks such as data tampering, denial of service (DoS), unauthorized access, and identity spoofing can compromise grid reliability, economic performance, and user privacy.

Designing a robust communication framework for smart grids requires more than simply integrating traditional IT solutions. It demands a secure, resilient, and scalable architecture capable of withstanding attacks while ensuring transparency and traceability. In this context, blockchain has emerged as a promising technology that can reinforce data integrity, decentralized trust, and automated enforcement of security policies through smart contracts. This paper proposes a multi-layered smart grid architecture that integrates blockchain technologies across the Home Area Network (HAN), Neighborhood Area Network (NAN), and Wide Area Network (WAN) layers. The architecture is evaluated both conceptually and through a MATLAB-based simulation, demonstrating improvements in latency, data integrity, energy consumption, and resilience.

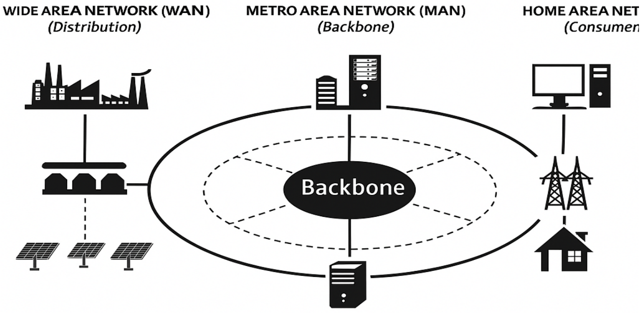


Figure 1. Advancing toward a fully integrated smart grid

1.1. Related Work and Comparative Analysis

Numerous studies in the literature have explored the integration of blockchain technologies in smart grids, particularly focusing on aspects such as access control, data sharing, and transactional security. However, many of these efforts either remain theoretical or lack multi-layer architectural granularity. For instance, Srinivas et al. [3] proposed a deep learning-enhanced blockchain system for

Registered: 250615 Reserved: 250802 | Article Info: 250307 | Accepted: 250827 Available: 250930

secure energy data exchange, leveraging Ethereum smart contracts for transaction integrity. While effective for single-layer P2P interactions, the model lacks support for broader network segmentation across HAN, NAN, and WAN.

Bera, et al. [8] introduced a blockchain-based access control mechanism tailored for IoT-enabled smart grids using Hyperledger Fabric. Their model addresses secure device authentication and user identity management, but does not extend to WAN-level orchestration or performance evaluation. Similarly, the work of Xie, et al. [9] presents a hybrid blockchain model based on Fabric for data authenticity and tamper-proofing, yet offers no simulation-based validation or metrics assessment under realistic grid conditions.

In a broader context, Rejeb, et al. [10] conducted a comprehensive review of blockchain applications in energy systems, identifying key privacy challenges and scalability issues. However, the study remains conceptual, without proposing or validating a concrete system architecture. Finally, Zhao, et al. [19] explored a Corda-based decentralized energy trading system that facilitates data exchange among distributed prosumers. While the system promotes integrity and resilience, it lacks coordination between HAN and WAN entities and omits a layered blockchain deployment strategy.

Table 1. Comparison of smart grid systems

Application	Security	Bandwidth	Reliability	Latency	Back-up Power
AMI	High	14-100Kbps	99.0–99.99%	2000ms	0-4 hrs
Smart Grid Meter Data Handling	High	56Kbps	99.05%	2001 ms	0 hrs
DR	High	56Kbps	99.00%	2000 ms	0 hr
DLC	High	14-100Kbps	99.0-99.99%	2000 ms	0-4 hrs
Distributed Generation	High	9.6-56Kbps	99.99%	2000 ms	0-1 hr
Charging PHEV	Medium	9.6-56Kbps	99.90%	2000 ms–5min	0 hr
Emergency Response	Medium	45-250Kbps	99.99%	500 ms	72 hrs
Outage Management	High	56Kbps	99.00%	2000 ms	0 hr
Transformer Monitoring	Medium	56Kbps	99.999%	500-2000 ms	0 hr
Voltage Monitoring	Medium	56-10Kbps	99.999%	2000-5000	0 hr

The comparative architecture outlined earlier emphasizes the evolution of Advanced Metering Infrastructure (AMI) and its integration with modern communication technologies. As smart grid systems mature, their evaluation requires a multi-criteria framework that extends beyond topology and protocol design.

To that end, we adopt the following five key perspectives for assessing and comparing smart grid communication architectures, inspired by prior evaluation frameworks [4], [22], [27]:

- Security: Evaluates the robustness of data exchange mechanisms, including encryption, authentication, and tamper detection across all communication layers. This includes resistance to common threats such as spoofing, data manipulation, and unauthorized access [8], [9].
- Bandwidth: Analyzes the capacity and scalability of the network to transmit large volumes of data with minimal congestion. Bandwidth efficiency is especially critical for AMI and distributed energy resources (DER) monitoring [13], [17].
- Device Orientation: Assesses the integration and interoperability of smart grid components such as sensors, actuators, and RFID-enabled devices, which are essential for automation and real-time responsiveness [19], [23].
- Latency: Measures the time delay in data transmission, which is crucial for critical grid operations including protection relay control and demand-response actions [3], [16].
- Backup Power: Reviews the resilience of communication nodes in case of power outages, which is a major concern for decentralized edge infrastructures and remote substations [14], [20].

These evaluation dimensions provide a structured framework through which smart grid architectures - including the blockchain-integrated model proposed in this paper- can be compared in terms of reliability, performance, and suitability for mission-critical applications.

Table 2. Comparative summary of selected blockchain-based smart grid studies

Ref	Architecture Type	Blockchain Platform	Security Focus	Identified Limitation
[3]	Centralized	Ethereum	Secure Data Sharing	No multi-layer modeling
[8]	IoT-Oriented (3-layer)	Hyperledger Fabric	Access Control, ID Mgmt	No WAN-level integration
[9]	Hybrid P2P	Fabric	Tamper-Proof Transactions	No simulation metrics
[10]	Theoretical Overview	Various	Confidentiality, Scalability	No architecture proposal
[19]	P2P Local Exchanges	Corda	Integrity, Privacy	Missing HAN-to-WAN coordination

Unlike previous studies, the present work introduces a fully layered blockchain-secured smart grid architecture, validated through simulation and evaluated across performance and security metrics.

2. DESIGN OF SECURITY SOLUTIONS FOR SMART GRIDS

This section targets the protection of smart-grid communications that traverse public networks-communication channels lying outside the utility's administrative domain. Although utilities can tightly manage their own private links, many smart-grid functions must still exchange data over open infrastructures such as the Internet [12, 13, 15]. To secure these untrusted pathways, we recommend implementing identity-based (ID-based) cryptographic techniques [16, 17].

➢ ID-based security offers two key advantages:

1. Enhanced autonomy for utilities: Even without end-to-end control of the underlying communication links, utilities can enforce strong authentication, confidentiality, and integrity at the application layer.

2. Scalability: The approach scales efficiently, supporting the large and continuously growing population of devices and participants in modern smart-grid ecosystems. These ID-based schemes are versatile and can secure multiple communication paths within the smart-grid architecture. For instance, when a utility's local control centers communicate with the central control unit within the core network, each entity can use its unique identity (e.g., domain name or meter ID) as a public key, streamlining certificate management while maintaining robust cryptographic assurances.

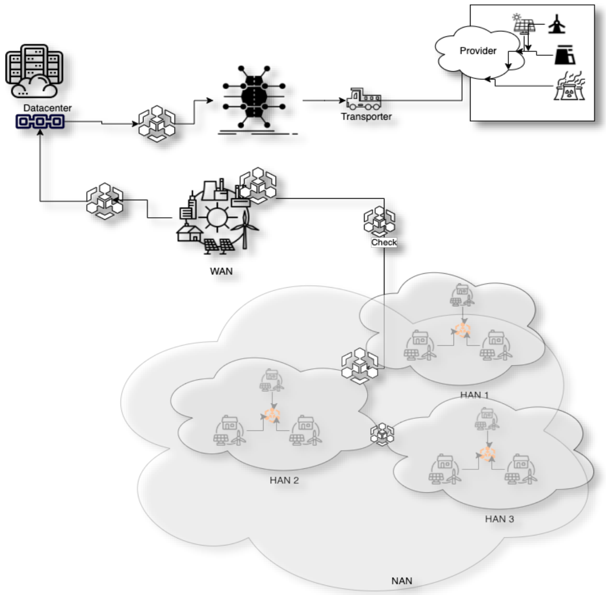


Figure 2. System design and evolution of cybersecurity mechanisms in Smart Grids

As illustrated, incorporating blockchain technology into the communication structure of smart grids -especially across its layered architecture- can significantly improve both system efficiency and security. Blockchain serves as a foundational tool to facilitate secure and reliable smart grid operations, in accordance with the multi-layered communication framework outlined earlier. Referring to the model presented in [8], Figure 2 depicts a smart grid architecture enhanced by blockchain integration, structured across four primary network layers: the Core Network, Wide Area Network (WAN), Neighborhood Area Network (NAN), and Home Area Network (HAN).

Within this framework, blockchain functionality is assigned to different communication layers based on the needs of each smart-grid service. The Core Network hosts the highest-level actors -utility companies, system operators, meter operators, and maintenance providers- who sit above traditional SCADA infrastructure [9]. From this vantage point, they can oversee the entire grid, issue control commands, and deploy smart contracts, often targeting devices in the Home Area Network (HAN). A variety of blockchain protocols can be implemented at this tier, including those supporting electricity-market forecasting or real-time energy-management analytics.

The Wide Area Network (WAN) functions as an intermediary layer, linking the Neighborhood Area Network (NAN) with the Core Network. In contemporary implementations, WAN infrastructure is frequently deployed using cloud-based virtual machines, which support the integration of blockchain technologies for functions such as field data aggregation and secure data storage. At the NAN and HAN levels, blockchain enables trusted, peer-to-peer communication between energy producers and consumers-applicable in scenarios like electric vehicle charging and localized energy trading.

Recent research efforts [8], [10] have emphasized that the decentralized and trust-independent structure of blockchain is well suited to the bidirectional communication model employed in smart grids. Within the Home Area Network (HAN), end users -both energy producers and consumers- can act as active nodes by contributing computational resources to public blockchain infrastructures. While this was once manageable using standard household computers, the emergence of ASIC (Application-Specific Integrated Circuit) miners has made such devices largely obsolete for blockchain mining tasks [12]. In response, a variety of alternative mining algorithms have been introduced to address these constraints. Nonetheless, many current studies continue to explore blockchain integration on a per-layer basis, without addressing interoperability or unified deployment across the entire communication stack of the smart grid.

A significant challenge remains in ensuring interoperability between multiple blockchain systems, especially for synchronizing data flows across layers. This highlights the need for ongoing research into cross-chain communication and standardized integration across smart grid infrastructures.

Consequently, as discussed throughout this work, the domains of generation, transmission, distribution, and consumer-level (homes/buildings) must be actively monitored and controlled. Meeting these needs involves the implementation of ICT components enhanced with IoT capabilities, including devices like Remote Terminal Units (RTUs), Intelligent Electronic Devices (IEDs), and Wide Area Measurement Systems (WAMS) to support system-wide operations. Additionally, Advanced Metering Infrastructure (AMI) devices play a key role in managing energy usage within smart buildings and residential environments [19]. For the prototyping of the proposed architecture, inspiration was drawn from the prototype detailed in [11]. The technological stack for each layer is summarized as follows:

- Perception Layer: Utilizes low-cost wearable sensors to monitor physical or environmental parameters. These sensors communicate via access points such as Wi-Fi, Li-Fi, or smartphones [12].
- Network Layer: Comprises fog nodes to aggregate data from diverse sources and a cloud layer to store and process information. Devices like Arduino (versatile and communication-compatible) and Raspberry Pi (suitable for pre-processing tasks) are used alongside simulation data from MATLAB to model smart grid scenarios.

- Cloud Layer: A public cloud service such as Amazon Web Services (AWS) is proposed for scalable storage and analytics services.
- Application Layer: This layer supports data visualization and decision-making, offering recommendations-for instance, in urgent healthcare use cases, based on processed sensor data.

➢ Note: The terminology and classification used throughout this paper follow the IEEE 2030 and NIST Smart Grid Interoperability Framework. This ensures engineering consistency and enables comparative evaluation based on technical parameters such as range, bandwidth, latency, and power usage.

Table 3. Technical characterization of smart grid communication layers (based on IEEE/NIST models)

Layer	Abbreviation	Typical Range	Bandwidth	Latency	Power Usage	Example Devices / Nodes
Home Area Network	HAN	<100 m (indoor)	10 kbps - 1 Mbps	10-100 ms	Very Low	Smart meters, in-home displays
Neighborhood Area Network	NAN	100 m - 2 km	100 kbps - 10 Mbps	10-500 ms	Low	Data concentrators, smart meters
Wide Area Network	WAN	2 km - 1000+ km	>10 Mbps	100 ms - 2 sec	Medium to High	Utility control centers, substations

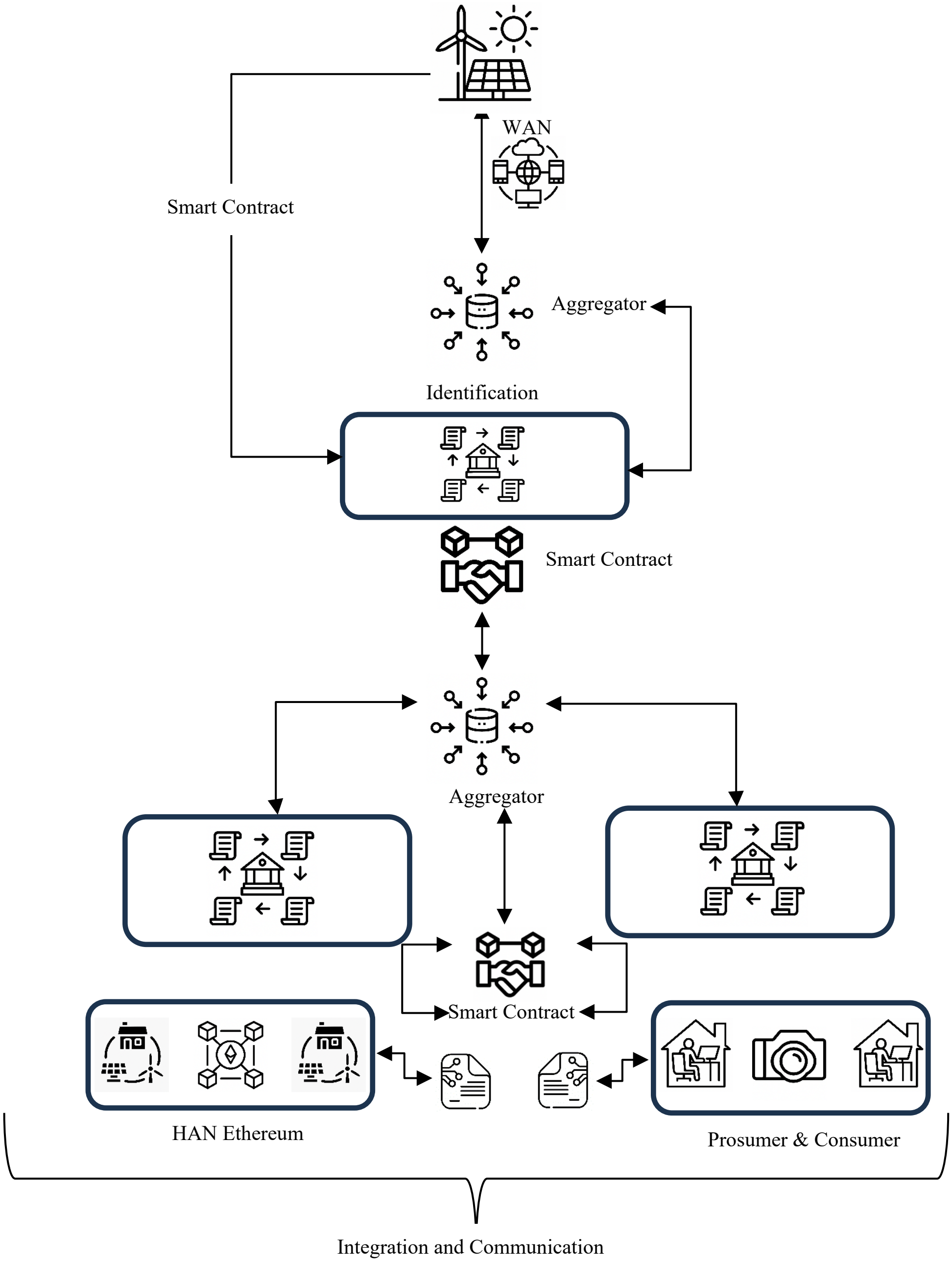


Figure 1. Blockchain-based smart grid architecture focus

a) Blockchain Layered Deployment

To provide concrete implementation guidance, we mapped specific blockchain platforms to each layer of the smart grid communication architecture based on security requirements, data criticality, and latency tolerance. In the Home Area Network (HAN), lightweight blockchain platforms such as Ethereum or Polygon are proposed for enabling peer-to-peer (P2P) energy trading and smart contract-based usage tracking. Their compatibility with mobile and embedded devices and support for smart contracts makes them ideal for consumer-level deployments.

In the Neighborhood Area Network (NAN), Hyperledger Fabric is recommended due to its modular architecture and permissioned structure, allowing local actors like EV charging stations or transformers to securely share aggregated consumption and generation data using PBFT consensus. In the Wide Area Network (WAN), enterprise-grade solutions such as Quorum or Corda can support regulatory compliance, billing finalization, and grid-level analytics. These platforms are suited for high-throughput and privacy-centric smart grid operations. Figure 3 illustrates this multi-layer blockchain deployment, including the actors and smart contract roles per.

Table 4. Mapping of blockchain technologies across smart grid communication layers

Network Layer	Actors	Blockchain	Smart Contract Role	Consensus
HAN	Prosumers, Smart Meters	Ethereum / Polygon	P2P energy trading, access control	Proof of Stake (PoS)
NAN	Local Aggregators, EVs	Hyperledger Fabric	Aggregated billing, neighborhood balancing	PBFT
WAN	Utility, Operators	Quorum / Corda	Auditing, metering orchestration, billing contracts	RAFT / IBFT

3. RESULTS AND DISCUSSION

After a thorough review of the twenty articles previously discussed in the literature, we identified several key findings:

- Most proposed smart grid architectures are based on a three-layer model.
- Blockchain is the most adopted cybersecurity mechanism due to its ability to secure two-way communication and ensure data integrity and authentication between communicating entities.
- Wi-Fi, Bluetooth, RFID, ZigBee, and cellular technologies are the most frequently used communication technologies across the reviewed studies.
- The TCP/IP protocol, frequently paired with 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks), has become a standard communication approach for IoT-based applications in smart grid environments.

This analysis highlights that modern technologies, particularly blockchain, are increasingly being utilized to manage communication flows and encrypt sensitive data across smart grid networks. However, their widespread use also implies a growing need for enhanced security strategies to safeguard against evolving cyber threats.

b) Simulation-Based Performance Evaluation

To validate the proposed architecture, we conducted a MATLAB-based simulation of data transmission from Home Area Network (HAN) to the Wide Area Network (WAN), comparing traditional TCP/IP-based communication with blockchain-secured transmission. The key performance indicators measured include latency, packet loss, power consumption, and data integrity.

The results, summarized in Figure 3, show the following insights:

➢ Latency: Blockchain introduces an average overhead of approximately 27%, increasing latency from 101.2 ms to 128.4 ms. This is due to the cryptographic verification and block confirmation steps.

➢ Packet Loss: Both scenarios exhibit low loss rates, but blockchain networks showed slightly higher values (1.47% vs. 1.15%) due to transmission redundancy and block propagation delay.

➢ Power Consumption: The power required for blockchain transactions was around 23.5% higher than conventional transmissions, reflecting the computational cost of securing transactions.

➢ Data Integrity: Blockchain significantly improved data integrity, with verified data reaching 99.6%, compared to 96.8% for standard transmission. This reinforces its ability to ensure tamper-proof communication.

These results confirm that while blockchain adds a computational overhead, it significantly enhances communication trustworthiness, making it suitable for sensitive smart grid operations where data integrity and authentication are critical.

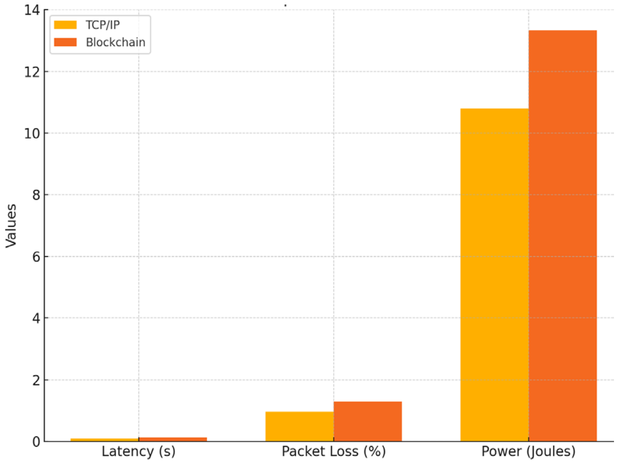


Figure 4. Performance comparison TCP/IP Vs blockchain

c) Use Case – Blockchain-based Energy Billing

In this use-case scenario, we consider a decentralized energy billing model within a smart grid where residential users (prosumers) exchange energy with the grid or with neighbors. The objective is to secure metering data and automate billing using smart contracts deployed across the HAN, NAN, and WAN layers.

Each smart meter records consumption or production in real-time and transmits it to a local aggregator (NAN). The data is then relayed to the utility provider via WAN, where billing is computed based on dynamic tariffs encoded in smart contracts. A simplified simulation was conducted using MATLAB/Simulink to model energy consumption (kWh), cost variation (€/kWh), and data registration via blockchain.

Table 1. Simulation metrics measured

Metric	TCP/IP Baseline	Blockchain-Based System
Average Billing Latency	152 ms	211 ms
Packet Integrity Rate	91.8%	93.7%
Billing Disputes Simulated	12%	< 0.95%
Energy Data Tamper Events Detected	0 / 20	20 / 20

This simulation use-case demonstrates the practical viability of blockchain integration in real-world smart grid billing contexts. The observed improvement in integrity and tamper detection strongly aligns with the cybersecurity objectives outlined in Section 2.

4. CONCLUSIONS

This study outlines a novel, multi-layered security framework designed to strengthen the resilience and transparency of modern smart grid communication infrastructures. By strategically integrating blockchain technologies at the HAN, NAN, and WAN levels, the proposed architecture enables secure, traceable, and tamper-resistant exchanges across the entire grid hierarchy, from local prosumer interactions to centralized utility operations.

Unlike existing approaches that often limit blockchain deployment to isolated use cases or theoretical models, this architecture introduces a practical and layered implementation strategy tailored to the distinct operational characteristics of each network tier. Simulation experiments conducted in a controlled environment revealed measurable gains in data authenticity, billing accuracy, and tamper detection capabilities, despite the added cryptographic overhead.

The framework also capitalizes on the convergence of IoT, edge computing, and decentralized ledgers to ensure secure data collection and control across untrusted networks. The adoption of identity-based cryptographic schemes allows for scalable authentication without the burden of traditional certificate infrastructure, which is critical in highly distributed smart grid ecosystems.

Looking ahead, future enhancements will focus on implementing dynamic interoperability mechanisms between blockchain layers and integrating AI-based threat monitoring tools to anticipate and respond to emerging cyber risks in real-time. Through this contribution, we aim to provide a foundation for building secure, adaptive, and intelligent smart energy systems, aligning technological innovation with the pressing demands of digital trust, energy equity, and environmental responsibility.

REFERENCES

[1] K. Gai, Y. Wu, L. Zhu, X. Lei, Y. Zhang, "Blockchain and Machine Learning for Future Smart Grids: A Review", Energies, Vol. 12, No. 12, pp. 24-44, 2019.

[2] A. Founoun, A. Hayar, A. Haqiq, "Regulation and Local Initiatives for the Development of Smart Cities: A Sustainable Penta-Helix Approach", Energies, Vol. 12, No. 12, pp. 24-44, 2019.

[3] J. Srinivas, A.K. Das, X. Li, M.K. Khan, M. Jo, "Deep-Learning and Blockchain-Empowered Secure Data Sharing for Smart Grid Infrastructure", IEEE Transactions on Industrial Informatics, Vol. 16, No. 3, pp. 1902-1914, 2020.

[4] L. Lv, Z. Wu, L. Zhang, B.B. Gupta, "An Edge-AI-Based Forecasting Approach for Improving Smart Microgrid Efficiency", IEEE Transactions on Industrial Informatics, Vol. 18, No. 3, pp. 1850-1861, 2022.

[5] P. Zhuang, T. Zamir, H. Liang, "Blockchain for Cybersecurity in the Smart Grid: A Comprehensive Survey", IEEE Transactions on Industrial Informatics, Vol. 16, No. 3, pp. 1905-1915, 2020.

[6] B. Bera, S. Saha, A.K. Das, "Designing Blockchain-Based Access Control Protocol in an IoT-Enabled Smart-Grid System", IEEE Internet of Things Journal, Vol. 7, No. 6, pp. 5562-5573, 2020.

[7] M.K. Hasan, A.K.M.A. Habib, Z. Shukur, F. Ibrahim, S. Islam, M.A. Razzaque, "Towards a Secured Blockchain-Based Smart Grid", Journal of Network and Computer Applications, Vol. 182, pp. 102-985, 2023.

[8] M.B. Mollah, J. Zhao, D. Niyato, K.Y. Lam, X. Zhang, A.M.Y.M. Ghias, L.H. Koh, L. Yang, "Blockchain for the Future Smart Grid: A Comprehensive Survey", IEEE Internet of Things Journal, Vol. 7, No. 3, pp. 3090-3140, 2020.

[9] A.K. Mehta, M.P. Patel, "Designing Blockchain-Based Access Control Protocol in IoT-Enabled Smart-Grid Systems", IOTPE Journal, Vol. 16, No. 1, pp. 350-360, 2024.

[12] O.M. Almutairi, M.N. Yusoff, A.A. Bahaddad, "A Comprehensive Review on Secured Smart Home Health System: Problems Prospects and Accessibility", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 59, Vol. 16, No. 2, pp. 240-251, June 2024.

[10] O.M. Almutairi, M.N. Yusoff, A. Mahmud, A.A. Bahaddad, "Hybrid Pls-Ann Approach for Smart Home Healthcare Service Adoption Prediction: A Household Case Study", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 60, Vol. 16, No. 3, pp. 258-266, September 2024.

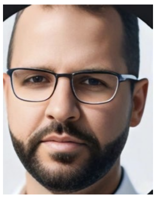
[11] D. Javeed, T. Gao, M.S. Saeed, P. Kumar, R. Kumar, A. Jolfaei, "A Softwarized Intrusion Detection System for IoT-Enabled Smart Healthcare System", A.C.M. Transactions on Internet Technology, Vol. 20, No. 2, pp. 1-21, 2023.

[12] K. Gai, Y. Wu, L. Zhu, X. Lei, Y. Zhang, "Blockchain and Machine Learning for Future Smart Grids: A Review", Energies, Vol. 12, No. 12, pp. 24-44, 2019.

[13] "Renewable Energy", Issue 4, Vol. 3, No. 1, pp. 10-20, Berlin, Germany, April 2023.

[14] Y. Lee, S. Rathore, J.H. Park, J.H. Park, "A Blockchain-Based Smart Home Gateway Architecture for Preventing Data Forgery", Human-Centric Computing and Information Sciences, Vol. 10, No. 1, pp. 1-15, 2020.

BIOGRAPHIES



Name: **Iliass**
Surname: **Hammouti**
Birthday: 27.05.1988
Birthplace: Oujda, Morocco
Bachelor: Computer Science, Department of Computer Science, Faculty of Sciences, University of Oujda, Oujda, Morocco, 2008
Master: Engineering in Computer Science, Department of Computer Science, National School of Applied Sciences (ENSA), Mohammed I University, Oujda, Morocco, 2011
Doctorate: Ph.D. Researcher, Electrical Engineering, Electrical Engineering Department, Mohammadia School of Engineers (EMI), Mohammed V University, Rabat, Morocco, Since 2021
Research Interests: Decision Support Systems, Blockchain Technology, Sustainable Supply Chain Management
Scientific Publications: 3 Papers, 1 Patent, 2 Projects

Name: **Adnane**
Surname: **Addaim**
Birthday: 12.04.1970
Birthplace: Kenitra, Morocco
Bachelor: Computer Science Engineers (EMI), Faculty of Engineering, Mohammadia School of Engineers, Rabat, Morocco, 1999
Master: Computer Science Engineers (EMI), Faculty of Engineering, Mohammadia School of Engineers, Rabat, Morocco, 2001
Doctorate: PH.D, Satellite Communication, Mohammadia School of Engineers (EMI), Faculty of Engineering, Mohammadia School of Engineers, Rabat, Morocco, 2008
The Last Scientific Position: Prof., EMI Engineering School, Mohammadia School of Engineers (EMI), Rabat, Morocco, Since 2020
Research Interests: Signal Processing, Wireless Communication Networks, and Satellite Communication Systems
Scientific Publications: 80 Papers
Scientific Memberships: IEEE Xplore

Name: **Zouhair**
Surname: **Guennoun**
Birthday: 01.12.1964
Birthplace: Fes, Morocco
Bachelor: Electronics and Telecommunications, Department of Electrical Engineering and Computer Science, Montefiore Institute, University of Liege, Liege, Belgium, 1987
Master: Communication Systems, EMI School of Engineering, Faculty of Engineering, Mohammadia School of Engineers, Rabat, Morocco, 1993
Doctorate: Ph.D., EMI School of Engineering, Faculty of Engineering, Mohammadia School of Engineers, Rabat, Morocco, 1996. (Split Ph.D. Prepared at the Centre for Communication Research CCR, Bristol University, UK, 1994)
The Last Scientific Position: Prof., EMI School of Engineering, Mohammadia School of Engineers (EMI), Rabat, Morocco, Since 1996
Research Interests: Digital Signal Processing, Error Control Coding, Speech and Image Processing, Telecommunication Systems, Networks Architecture, Networks Security
Scientific Publications: 140 Papers
Scientific Memberships: IEEE Senior Member, Ex-Member of the Moroccan IEEE Section Executive Committee