RADemics

Homomorphic Encryption and AI-Based Intrusion Detection for Cyber-Resilient IoT-Connected Smart Power Systems

Neha Agrawal, N. Saranya
Maharaja Agrasen Institute of Technology,
Karpagam College of Engineering

10. Homomorphic Encryption and AI-Based Intrusion Detection for Cyber-Resilient IoT-Connected Smart Power Systems

[1]Neha Agrawal, Associate Professor, Department of Information Technology, Maharaja Agrasen Institute of Technology, New Delhi, India. nehaagrawal@mait.ac.in

[2]N. Saranya, Assistant Professor, Department of Artificial Intelligence and Data Science, Karpagam College of Engineering, Coimbatore, Tamil Nadu, India, saranyababumecse@gmail.com

Abstract

The integration of homomorphic encryption (HE) within IoT-connected smart grid systems presents a promising solution for ensuring data privacy and security, particularly in environments where sensitive energy data was transmitted and processed. The computational overhead of HE has hindered its widespread adoption, especially in resource-constrained devices within the grid. This chapter explores the synergies between HE and emerging technologies, such as edge and fog computing, lightweight cryptography, and hardware acceleration, to enhance the efficiency and feasibility of real-time encrypted data processing in smart grids. A detailed analysis of computational challenges and optimization strategies was presented, focusing on reducing the latency and energy consumption associated with HE operations. Case studies and experimental evaluations highlight successful implementations of hardware-accelerated HE in smart grid applications, demonstrating significant improvements in system performance and scalability. The chapter also examines the comparative advantages of HE over traditional encryption techniques, emphasizing its potential for securing critical infrastructure while maintaining privacy in decentralized power networks. Overall, this work provides a comprehensive framework for overcoming the challenges of HE implementation in smart grids and paves the way for future advancements in cyber-resilient, privacy-preserving energy management systems.

Keywords: Homomorphic encryption, smart grids, edge computing, lightweight cryptography, hardware acceleration, data privacy.

Introduction

The integration of homomorphic encryption (HE) in IoT-connected smart grid systems represents a significant advancement in the realm of data security and privacy [1,2]. With the growing adoption of smart grids, which rely heavily on interconnected devices such as smart meters, sensors, and controllers, ensuring the confidentiality of sensitive energy data has become a critical concern. Traditional encryption techniques typically require decryption before data can be processed, which poses significant privacy risks [3]. Homomorphic encryption, allows computations to be performed directly on encrypted data, enabling privacy-preserving analytics without exposing the underlying sensitive information [4]. This capability was especially

important in environments like smart grids, where data transmission occurs over potentially insecure networks [5]. HE faces challenges such as high computational complexity and increased resource demands, making its real-time application in smart grids a topic of considerable research [6].

As smart grid systems become increasingly complex, the need for robust security mechanisms grows, particularly when dealing with the vast amounts of data generated by IoT devices [7]. The real-time nature of smart grid operations further complicates this challenge. Secure and timely data processing was required to make decisions related to grid optimization, load balancing, demand response, and fault detection [8]. Homomorphic encryption, while offering unparalleled privacy protection, introduces significant computational overhead due to the complex arithmetic operations involved. This complexity limits its practical application, particularly in resource-constrained IoT devices embedded in the grid infrastructure [9,10]. Therefore, a key focus of ongoing research was to optimize HE to reduce its computational burden without compromising its security features [11].

The development of efficient solutions to mitigate the computational challenges of HE was essential to enable its widespread adoption in smart grids. One promising approach was the integration of edge and fog computing technologies with HE [12,13]. By leveraging edge computing, data can be processed closer to the source, reducing the need for data transmission to centralized cloud servers. This not only reduces latency but also minimizes the communication overhead and energy consumption typically associated with cloud-based computations [14]. Fog computing, which extends cloud capabilities to the edge of the network, offers additional flexibility by enabling distributed processing across a network of localized nodes. This combination of edge and fog computing with HE can significantly enhance the performance of smart grid applications, enabling real-time data processing while maintaining robust security and privacy protections [15].

To edge and fog computing, hardware acceleration was another critical strategy for addressing the computational overhead of HE in smart grids [16]. Specialized hardware, such as Field Programmable Gate Arrays (FPGAs), Graphics Processing Units (GPUs), and Application-Specific Integrated Circuits (ASICs), can be utilized to accelerate the key operations involved in HE, such as encryption, decryption, and homomorphic computation [17]. These hardware accelerators are designed to handle parallel computations efficiently, reducing the time required to process encrypted data. Experimental evaluations of hardware-accelerated HE have shown promising results, with significant improvements in computational efficiency and energy consumption [18,20]. By offloading the computationally intensive operations of HE to dedicated hardware, it becomes possible to support real-time processing requirements in smart grid applications, such as real-time anomaly detection, dynamic load forecasting, and secure energy trading [21].