

Integration and Optimization of Communication Data Security Transmission Mechanisms and Models in Power Consumption Verification

Jianfeng Qiao¹, Yan Li¹, Shuguang Hu¹, Bo Zhang¹, Jinhe Liu¹

¹Power Marketing Service and Operation Management Branch, Inner Mongolia Electric Power (Group) Co., Ltd., Hohhot 010000, Inner Mongolia, China

Corresponding author: Jianfeng Qiao (e-mail: qjf729406245@163.com)

ABSTRACT The rapid expansion of smart metering infrastructure has escalated the demand for secure and energy-efficient power consumption verification. Traditional verification protocols often suffer from immense communication overheads and high energy requirements, particularly at scale, making them vulnerable to interception and data alteration. This challenge is directly analogous to the textile industry's imperative for efficient and highly secure auditing of material and energy usage within global supply chains, given that traditional monitoring protocols are typically characterized by high latency, significant resource overhead, and vulnerability to data fraud or tampering. The paper proposes a composite security method for smart grid data transmission, combining lightweight authentication, homomorphic data aggregation, and energy-aware routing with an optimized verification model for consumption auditing. It employs Elliptic Curve Cryptography (ECC) for mutual authentication, Paillier homomorphic encryption for secure data aggregation, and a dynamic routing algorithm for low energy transmission. Experiments on a simulated Advanced Metering Infrastructure (AMI) network demonstrated that the Hybrid scheme, compared to pure Homomorphic Encryption (HE), reduced energy consumption by 42% while maintaining a competitive True Positive Rate (TPR) of 95.7% and significantly lower latency of ~150 ms. These results demonstrate an effective trade-off among security, integrity, and system durability using energy-conscious communication. This dual focus is highly applicable to the textile industry, providing a foundational technical approach for securely and efficiently auditing the complex energy consumption and material usage data across large-scale, automated manufacturing facilities.

INDEX TERMS smart grid, textile industry, energy-aware routing, power consumption verification, homomorphic encryption

I. INTRODUCTION

THE immense volumes of dense time-series consumption data generated by IoT-enabled metering systems and smart grids are crucial for accurate billing, detailed operational analytics, and effective demand management. Similarly, in the textile industry, the large amounts of time-series data generated by smart looms and dyeing machinery are equally critical for precise costing, optimizing complex manufacturing schedules, and managing the consumption of raw materials and energy. Such systems particularly depend on smart meters and edge devices, often of low capacity in computing power, data storage, and battery life. Hence, there must be a delicate balance between the level of cryptographic robustness and limits on energy costs and communication delay when the firm's reliability of data transfer is sought. As an example, Nilima et al. [1] state that the traditional security protocols are quite demanding on overhead, which can deprive real-time functions in

cases where the sources are scarce. Such a trade-off is significant in large-scale Advanced Metering Infrastructure (AMI) installations, as an increasing amount of data and the number of endpoints compound these issues. Thus, the realization of a sustainable smart grid fundamentally requires the design of communication schemes that are both energysaving and highly secure. This imperative is directly relevant to the textile industry, where achieving sustainable manufacturing practices depends equally on implementing secure and energy-efficient data transmission protocols to manage the vast amount of sensitive production and environmental monitoring data.

To overcome these issues, privacy-preserving data aggregation protocols within the context of homomorphic encryption (HE) have become a focus area in innovative metering systems. HE enables the computation of encrypted data without decryption, whereby mutual security of the users is upheld and actual aggregate data is analysed. Fan

et al. [2] reveal that the homomorphic aggregation based on Paillier-based can be successfully used to minimize the communication overhead and protect the reading of individual consumption. Similarly, Singh et al. [3] state that using HE and lightweight authentication protocols delivers both confidentiality and low-power operation performances. Irrespective of their benefits, these cryptographic schemes incorporate some computational complexity that needs to be highly optimized to deploy in bounded conditions. Therefore, further research is dedicated to optimizing such models to achieve an equilibrium of safety, precision, and energy consumption in verifying power consumption. Traditional cryptographic schemes are computationally and communicatively expensive, causing high latency, energy consumption, and poor scalability in resource-limited smart meters. Conversely, lightweight cryptography is efficient but lacks strong privacy protection and is vulnerable to advanced attacks. This creates a critical gap: current solutions fail to provide a unified approach that simultaneously optimizes security, energy efficiency, and verification accuracy. Consequently, the transmission of smart meter data risks compromising safety, operational efficiency, and user privacy. There is an urgent need to develop new mechanisms that can balance strong security with low energy use and reliable verification for scalable deployment in contemporary power systems.

Smart meters and IoT-enabled devices have several technical obstacles since their computational power, memory, and energy levels are low. This has to include end-to-end privacy between the meter and the aggregator and the utility provider to provide safety of consumer data so that it cannot be intercepted or used in any way detrimental to the consumer. In addition, systems ought to have mechanisms to support verifiable aggregation as well as verification to prevent fraudulent behaviors or data corruption without disclosure of raw consumption data, thus maintaining confidentiality of a user. One of the biggest obstacles is to optimize such parameters as the strength of the security and the power consumption and the communication latency. The advent of quantum computing presents a major challenge, requiring the development of new, lightweight, post-quantum cryptographic (PQC) algorithms suitable for constrained devices. This necessitates adopting new models that can effectively merge the conflicting requirements of privacy, flexibility, performance, and scalability within the emerging smart metering and IoT encryption landscape. This article proposes a unified system and architecture that extends energy-conscious secure transmission, privacy-preserving homomorphic aggregation, and an efficient power consumption verification scheme capable of working over resource-limited smart meters. It enforces and compares various variants, such as lightweight Elliptic Curve Cryptography (ECC), homomorphic encryption (HE) aggregation, and combination strategies in order to test trade-offs between security and efficiency. A multi-objective optimization routine is also implemented with the aim of

striking a forceful balance between verification accuracy, security strength and energy consumption. Comprehensive experiments are carried out with real and simulated smart meter data, and a practical testbed to assess the efficiency of the framework. Formal security proofs and details analysis are also presented in the paper with the aim of proving the resiliency of the proposed schemes. The remainder of the paper is organized as follows: Section “RELATED WORK” reviews related work; Section “SYSTEM MODEL AND THREAT MODEL” details the System Model and Threat Model; Section “PROPOSED INTEGRATED FRAMEWORK” details the proposed architecture; Section “FORMAL SECURITY & PRIVACY ANALYSIS” covers Formal Security and Privacy Analysis; Section “EXPERIMENTAL RESULTS & EVALUATION” presents Experimental Results and Evaluation; Section “DISCUSSION” is a Discussion; and Section “CONCLUSION & FUTURE WORK” concludes with future research directions.

II. RELATED WORK

The sensitivity of the information concerning energy consumption level and that many devices are linked to the smart grid make security in smart grid communications critical. Data integrity, authentication, and key agreement protocols are needed to prevent unauthorized access. The

widely-considered Elliptic Curve Cryptography (ECC) based contributions rely on their high level of security at a relatively low computational cost and thus may be applied in resource-constrained devices [4]. ECC is also commonly combined with challenge-response to improve each device’s authentication of the other and prevent attacks based on replay. According to the recent surveys, finding a proper balance between adequate security and the working constraints of the smart meters is crucial [5].

These lightweight security protocols designed for constrained devices aim to save energy without any trade-off in security assurance. Reduced computation complexities have been aimed at through optimized protocols like lightweight symmetric key algorithms and ECCs [6]. Moreover, energy-aware security systems incorporate configurable cryptographic methods that change the security parameters dependent on the device’s state and how the network is doing [7]. These methods show encouraging signs of having secure yet effective communication with smart grids, though there is still some form of issue with scaling and adapting to new threats.

In smart metering, there is a need to use privacy-preserving data aggregation to safeguard the privacy of individuals’ consumption patterns and to be able to carry out global analysis properly. The most popular types of homomorphic encryption (HE) are dedicated to the Paillier cryptosystem, which has the additive property that enables adding the encrypted information without decryption [8]. This modality maintains users’ privacy because individual readings will not be revealed until the time of aggregation. Nonetheless, HE schemes pose computational and commu-

nication overheads in that the encryption and processing of ciphertexts require many resources, and deployment on devices with limited resources can be difficult [9]. Finding a good trade-off between privacy and efficiency is a research topic.

Surveys and recent reporting on engineering emphasize some viable applications of HE in innovative grid systems. Indicatively, aggregation based on Paillier has already been implemented in large-scale Advanced Metering Infrastructure (AMI), wherein privacy-performance trade-offs are practical [10]. These studies focus on improving encryption characteristics and hybrid models to minimize overhead without compromising the high privacy assurances [11]. Further development is needed to scale HE-based solutions to real-world smart grids.

Energy-efficient routing in Wireless Sensor Networks (WSNs) and IoT is key in extending network lifetime without compromising data security. The protocols that incorporate trust and security metrics into routing decisions have been created to achieve these two goals. As an example, Elliptic Curve Cryptography (ECC) has been used with energy-aware Ant Colony Optimization (ACO) algorithms to offer dynamically selected routes that provide a trade-off between energy efficiency and robustness [12]. Such directions maximize the selection of paths based on the

trustworthiness of the nodes and remaining energy so that the impact of malicious nodes is reduced and the energy consumed is wasted unnecessarily. Nevertheless, the addition of security functionality poses an overhead that could minimize the optimization of routing, and this is a trade-off between high security and energy performance [13]. Recent surveys recognize the significance of adaptive schemes capable of changing the security levels based on the state of the network to solve this balance [14]. These mechanisms are essential in resource-limited smart grid and IoT platforms.

The statistical methods and machine learning techniques are increasingly used to spot tampering, faults in the meter, and unusual patterns of power usage in the data verification of power consumption data. It uses supervised anomaly detection algorithms to detect the deviations in historical consumption as a fraud or device malfunctioning indicator [15]. One method, federated learning (FL), has become a privacy-preserving solution, allowing model training in a distributed way by using smart meters where no sharing of raw data is involved, which is why it preserves user confidentiality [16]. Such methods improve the accuracy and scale of verification systems and solve privacy concerns in decentralized data processing systems. However, future progress in privacy-preserving ML and FL is crucial in securing and efficiently managing smart grids. Existing work on innovative grid communications research is biased towards optimizing the security, energy efficiency, or accuracy of verification in isolation. It lacks a balance among the three variables. As an illustration, there are more powerful protocols that absorb too much energy, and those that are lightweight by putting

less emphasis on robust privacy guarantees. Similarly, the verification models can identify anomalies correctly, but fail to integrate with secure and energy-efficient transmission modes. There is a notable difference in the efforts to design comprehensive frameworks that simultaneously optimize all three considerations: security, energy consumption, and verification accuracy, backed by rigorous experimental assessment. This gap needs solutions to bring about practical, scalable smart grid deployments.

III. SYSTEM MODEL AND THREAT MODEL

The system architecture suggested herein has several essential modules: smart meters (edge nodes), data concentrators or gateways, the communication network, a data aggregator and service provider, and a verifier entity: an auditor, or a utility operator. Smart meters acquire more granular use details, sending data to nearby gateways. These gateways put together data into wide-area networks (WAN) to the central aggregator. Communication links composing these networks are meter-gateway links (by low-power methods such as LoRaWAN or NB-IoT), and gateway-cloud transmission is used by LTE or wire-based Power Line Communication (PLC). The

verifier audits the aggregate data to ensure that the data is precise and guarantees a safe and stable system functioning. The hierarchical system architecture is shown in Figure 1.

Smart meters read the consumption as $r_{i,t}$, which denotes power use at time t by meter i . Timeseries readings generate dense data streams that may be summarized at regular intervals: hourly and daily, to minimize communication overheads and increase privacy. Metadata such as meter identifiers and timestamps is present together with consumption data. Meter IDs are either pseudonymized or encrypted before transmission, to prevent unauthorized correlation of data to specific users. This time-series structured data provides secure, verifiable aggregation and retains sufficient detail so the utility or auditor can perform detailed analytics.

It is a system that presupposes the presence of several adversaries of different capacities. Passive eavesdroppers cannot change data transmissions, but only intercept the data. Active attackers can alter messages, inject wrong information, or conduct a replay attack to derail the integrity of communication. Hijacked smart meters can give inaccurate readings or leak sensitive information. Malicious aggregators are also called honest-but-curious, as they adhere to the protocols yet try to deduce the confidential information. Also, man-in-the-middle attackers can interfere with communication between nodes and tamper with sensors, and insider attackers have

increased access to the system. These attackers disrupt the power consumption data's confidentiality, integrity, and availability.

They are presumed to have bound computational resources with the current threats in mind. Security is based upon well-understood cryptographic hardness problems, e.g., lately the discrete logarithm problem, on which Ellip-

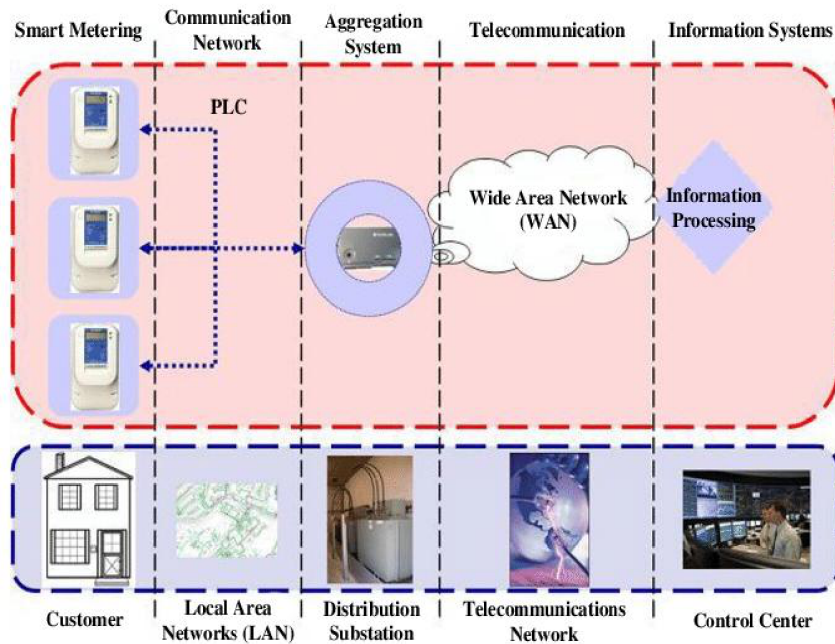


FIGURE 1. Layered System Architecture of Secure Smart Metering Communications.

tic Curve Cryptography (ECC) is based. The system also predicts future post-quantum (PQC) security threats and, thus, considers the future requirement of primitives in future versions. Whereas ECC and homomorphic encryption-based variants are currently used, the shift towards PQC algorithms must be made to ensure long-term security. Opponents are also assumed to be incapable of cracking secure key exchanges or signature operations within the limits of feasibility.

The architecture presupposes the trusted setup step, where a public key infrastructure (PKI) can be set up to provide secure management of cryptographic keys and certificates. The smart meters and gateways have trusted certificates that can be provided during manufacture or deployment. The communications infrastructure is partially trusted and can be interfered with by adversaries, and there is a need to have secure authentication and encryption procedures. Aggregators are operationally trusted to process the aggregate of the measurements, but the system is designed to be resilient against honest-but-curious behavior (as noted in the threat model). Therefore, cryptographic measures are employed to ensure they cannot access or release raw meter readings, even if they attempt to deduce confidential information. The auditor is trusted completely to check and warrant aggregated results. These presumptions outline security scope and aid in forming security protocols to minimize the threats outlined.

The delay and network size of hybrid and ECC schemes are shown in Figure 2:

IV. PROPOSED INTEGRATED FRAMEWORK

A. HIGH-LEVEL DESIGN

The suggested built-in framework is based on the layered solution to innovative metering systems' security, privacy, and energy efficiency. Lightweight authentication and key-agreement protocols at the edge result in quick and low-energy, mutual authentication between smart meters and the gateway with minimal implementation requirements. Meter data is privacy-preserving aggregated at the gateways and aggregators through additive homomorphic schemes, including Paillier, and can be added together, but doesn't reveal individual values. In the meter network, the secure routing protocols that focus on an energy-aware routing approach balance energy usage and reliability to optimize communication paths, increasing the network's lifetime. Last but not least, a verifiable consumption verification model is used, where the truth and integrity of accumulated consumption data are guaranteed and auditable, while ensuring user privacy. The holistic architecture is easy to combine with security, efficiency, and verifiability to present an application-compatible framework that is highly effective in resource-limited innovative grid systems.

B. CRYPTOGRAPHIC BUILDING BLOCKS

Lightweight authenticated key agreement protocols will be needed to get smart meters and gates to communicate securely and with low energy. The elliptic Curve Cryptography (ECC) protocol, in particular, by the computationally efficient curves such as Curve25519, offers an adequate level of security with a small key size and a smaller amount of computation work and can be used on resource-constrained environments [17]. The typical stages of formal protocols are registration,

mutual authentication, and session key derivation, which

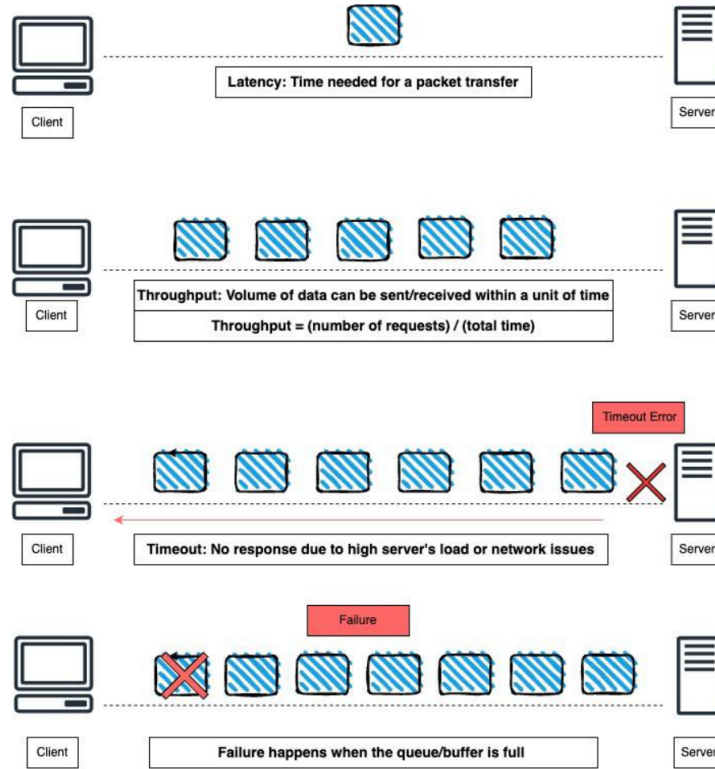


FIGURE 2. Latency vs. Network Size for HE, Hybrid, and ECC Schemes

are encrypted to guarantee confidentiality and integrity. Alternative lightweight symmetric key schemes can be used to trim overheads further during session setup. Researchers indicate that the techniques are considered to have strong security with low latency and energy usage compatibility [18].

We define a cryptographic efficiency ratio as:

The Security Score is a dimensionless metric normalized between 0 and 1, where 1.0 represents the highest security (e.g., equivalent to 256-bit AES/2048-bit RSA strength).

$$\eta_{\text{crypto}} = \frac{\text{Security Score}}{\text{Energy Cost}} \quad (1)$$

This metric allows quick benchmarking; for example, ECC with a score of 0.85 and cost of 1.5 mJ yields $\eta_{\text{crypto}} \approx 0.57$, while full HE with a score of 1.0 and cost of 18.5 mJ yields only $\eta_{\text{crypto}} \approx 0.054$.

C. MATHEMATICAL FORMULATION

Let G be the base point of Curve25519, k_i and k_j random private keys.

Ephemeral ECDH public key R_i :

$$R_i = k_i \times G \quad R_j = k_j \times G \quad (2)$$

Shared session key:

$$SK = KDF(k_i \cdot R_j) = KDF(k_j \cdot R_i) \quad (3)$$

Note on KDF Implementation: The Key Derivation Function (KDF) is implemented using HKDF (HMAC-based Key Derivation Function) with SHA-256 as the underlying hash function. Specifically, KDF extracts a fixed-length secret key SK from the shared secret output of the Elliptic Curve Diffie-Hellman (ECDH) operation.

Algorithm 1: ECC_Auth (Meter i , Gateway j)

1. Initiation: Meter i sends its identity ID_i and Ephemeral ECDH public key R_i , and a current timestamp T_i to Gateway j

$$\text{Meter}_i \rightarrow \text{Gateway}_j : ID_i, R_i, T_i$$

2. Challenge and Signature: Gateway j sends its identity ID_j , Ephemeral ECDH public key R_j , current timestamp T_j , and a signature $Sign_j$ over the exchanged nonces and timestamps back to Meter i :

$$\text{Gateway}_j \rightarrow \text{Meter}_i : ID_j, R_j, T_j, Sign_j(ID_i \| R_i T_i \| R_j T_j)$$

3. Verification and Response: Meter i verifies $Sign_j$ and checks the freshness of T_j . Upon successful verification, it sends a confirming signature $Sign_i$ to Gateway j :

$$\text{Meter}_i \rightarrow \text{Gateway}_j : Sign_i(ID_j \| R_j T_j \| R_i T_i)$$

4. Mutual Verification: Gateway j verifies $Sign_i$.

5. Session Key Derivation: Both parties derive the shared session key SK using their private ephemeral key and the peer's ephemeral ECDH public key. Specifically, party i computes the shared secret $Z = k_i \cdot R_j$ and party j computes $Z = k_j \cdot R_i$. Since $k_i \cdot R_j = k_j \cdot R_i$, both parties arrive at the same shared secret Z , which is then processed by the

KDF as defined in Equation (3).

D. DEFENSE MECHANISM SUMMARY

Replay Attack Defense: Timestamps (T_i and T_j) are used in the message exchange, and freshness checks are explicitly required in Steps 2 and 3. Any attempt to replay old messages will fail due to timestamp expiration.

Man in the Middle (MITM) Defense: The scope of digital signatures ($Sign_i$ and $Sign_j$) has been extended to cover all exchanged parameters (ID, nonce, and timestamp). This ensures the integrity and authenticity of the message, and any tampering will result in signature verification failure, thus thwarting the MITM attack.

Energy cost:

- ECC scalar mult: ~1.5 mJ/op
- ECDSA verify: ~2.3 mJ/op (ARM Cortex-M4, 80 MHz)

Using the concept of homomorphic encryptions (the Paillier cryptosystem), data aggregation is possible, and the computation over encrypted meter readings can be performed without revealing the individual data. The algorithm entails meters encrypting consumption values with a public key of the aggregator, adding ciphertexts in a homomorphic manner, and finally decrypting only the resultant aggregate [19]. To cut the computational expense, a combination of partial HE schemes or secret-sharing-based aggregation can trade off between privacy and efficiency. Whereas such an approach keeps users anonymous, it allows for creating accurate and safe consumption analysis at the aggregator level.

Homomorphic Encryption (Paillier):

Encryption:

$$c_i = g^{m_i} \cdot r_i^N \pmod{N^2} \quad (4)$$

Aggregation:

$$C = \prod_{i=1}^k c_i \pmod{N^2} \quad (5)$$

Decryption:

$$M_{\text{sum}} = L(C^\lambda \pmod{N^2}) \cdot \mu \pmod{N} \quad (6)$$

where

$$L(u) = \frac{u-1}{N} \quad (7)$$

Algorithm 2: Paillier_Aggregate

- 1: Each meter encrypts $m_i \rightarrow c_i$ using aggregator's PK.
- 2: Gateway aggregates: $C = \prod_i c_i \pmod{N^2}$.
- 3: Aggregator decrypts C to obtain $\sum_i m_i$ without individual values.

E. PAILLIER PARAMETER GENERATION AND RANDOMNESS SPECIFICATION

To ensure cryptographic robustness and address the lack of definition, we explicitly specify the Paillier parameter generation and randomness sources. The key pair is generated by the central Data Aggregator (DA).

The Paillier Key Generation process is as follows:

1. Select two large prime numbers, p and q , randomly and independently, ensuring they have equal bit-length (e.g., 1024 bits for n to be 2048 bits). The primes must satisfy the condition $\gcd(pq, (p-1)(q-1)) = 1$.
2. Compute the public modulus $n = pq$ and $\lambda = \text{lcm}(p-1, q-1)$.
3. Compute the public modulus $g \in \mathbb{Z}_{n^2}^*$. As a recommended practice for implementation simplicity and efficiency, we set $g = n + 1$.
4. Compute the modular multiplicative inverse $\mu = (L(g^\lambda \pmod{n^2}))^{-1} \pmod{n}$, where $L(x) = (x-1)/n$.
5. The public key is $PK = (n, g)$ and the private key is $SK = (\lambda, \mu)$.

Furthermore, all random selections required for the cryptosystem, including the initial large primes p, q for key generation and the encryption randomness $r \in \mathbb{Z}_n^*$ used by the smart meters (in Algorithm 2, r_i), must be sourced from a Cryptographically Secure Pseudorandom Number Generator (CSPRNG). The utilization of a CSPRNG is essential to guarantee the high min-entropy necessary for the probabilistic nature and semantic security of the Paillier scheme.

Hybrid cryptographic techniques handle trade-offs, where information that must be transmitted often is symmetrically encrypted and periodically aggregated using HE to reduce overhead. The design substantially lowers the computational and communication cost of performing continuous HE encryption and provides robust privacy guarantees when performing aggregate computations. Also, the rise of post-quantum cryptography (PQC) is essential with quantum computing under threat of classical cryptocurrency algorithms. Although there are standardizations of PQC by NIST, the integration of PQC on smart meters has challenges in performance since PQC requires more computation, with the need to achieve constant optimization.

Algorithm 3: Hybrid_Encrypt_Policy

If $(t \bmod T_{agg} == 0)$ then

if $(E \geq E_{th})$ then

Mode $\leftarrow$ Paillier_HE

Perform_Aggregation()

else

Mode $\leftarrow$ AES_CCM

Issue_Low_Battery_Warning()

Enter_Energy_Saving_Mode()

Defer_Aggregation()

```

end if
else
  Mode ← AES_CCM
end if

```

F. RATIONALE FOR PARAMETER SELECTION

The specific parameter values for the Hybrid Policy were determined empirically through the multi-objective optimization routine detailed in Section “Energy-Aware Communication Layer” and Section “EXPERIMENTAL RESULTS & EVALUATION”. The selection was guided by the critical system constraints identified on the Pareto front: maximizing the Security Score ($S \geq 0.8$), ensuring high Aggregation Accuracy ($A \geq 95\%$), and minimizing Energy Consumption ($E \leq 10$ mJ per reporting period).

The aggregation interval, $T_{agg} = 12$ reporting intervals, was selected as the optimal frequency that provides high detection accuracy (achieving $TPR \geq 95.7\%$ as shown in Table 2) while keeping the average latency at a competitive ~ 150 ms (Table 2). This frequency offers the best trade-off, as shorter intervals would substantially increase energy costs and longer intervals would degrade verification accuracy and increase latency.

The energy threshold, $E_{th} = 30\%$ battery capacity, serves as a critical fail-safe to preserve network durability. The routine telemetry data is encrypted using AES-CCM, maximizing energy efficiency. Paillier Homomorphic Encryption (HE) is strictly reserved for the predetermined aggregation time ($t \bmod T_{agg} = 0$), where secure homomorphic processing is mandatory. The energy threshold (E_{th}) is used as a critical low-battery warning to trigger system-level conservation measures (e.g., stopping non-essential tasks) and to guarantee enough residual energy is available to execute the one final high-cost Paillier HE aggregation operation at the next scheduled T_{agg} before the smart meter’s battery completely depletes. The system’s reliance on the low-cost AES-CCM mode for routine telemetry justifies setting this threshold relatively low, prioritizing maximization of operational lifetime.

The average energy consumption (mJ) for each reporting period is shown in Table 1:

TABLE 1. Average Energy Consumption (mJ) per Reporting Period

Number of Meters	HE Scheme (mJ)	Hybrid Scheme (mJ)	ECC Scheme (mJ)
10	8.2 ± 0.4	4.5 ± 0.3	3.2 ± 0.2
50	14.1 ± 0.5	9.6 ± 0.4	5.5 ± 0.3
100	18.5 ± 0.6	10.7 ± 0.5	6.3 ± 0.4

TABLE 2. Detection Performance Metrics for Tampering

Scheme	TPR (%)	FPR (%)	FNR (%)	Average Latency (ms)
HE	98.5 ± 0.3	1.2 ± 0.2	1.3 ± 0.1	350 ± 15
Hybrid	95.7 ± 0.4	3.0 ± 0.3	1.0 ± 0.2	150 ± 10
ECC	89.5 ± 0.6	4.5 ± 0.4	6.0 ± 0.5	80 ± 8

G. ENERGY-AWARE COMMUNICATION LAYER

The energy model measures the energy to transmit and compute in terms of standard device parameters. Low-power communications such as LoRaWAN and NB-IoT use between 50 and 80 nanojoules (nJ) at a time to transmit a bit at short distances [20]. Conversely, LTE has more power consumption of up to 150 nJ/bit concerning high data rates and longer spans. The computation costs of lightweight ECC-based signature generation on low-power embedded devices are approximately 1.5 millijoules (mJ) per signature generation, or up to 20 mJ per operation of some homomorphic encryption schemes, depending on the choice of scheme and implementation. Those energy benchmarks permit a sober assessment of communicational-cryptographic tradeoffs at intelligent meter networks.

Objective:

$$\min J = \alpha \sum_{(u,v) \in P} E_{u,v} + \beta \sum_{n \in N} (1 - T_n) - \gamma A \quad (8)$$

Subject to:

$$E_{\text{used}} \leq E_{\text{rem}} \quad (9)$$

$$\text{Latency}(P) \leq L_{\text{max}} \quad (10)$$

Algorithm 4: EA_ACO_Routing

1: Initialize pheromone τ_{uv} for all links.

2: For iter = 1..MaxIter:

For each ant:

Build path using τ and $\eta_{uv} = \frac{\text{trust}_{uv}}{E_{uv}}$.

Compute J .

$$\tau \leftarrow (1 - \rho)\tau + \Delta\tau \quad (11)$$

3: Return path with min J .

Parameters:

- $\alpha = 0.5$, $\beta = 0.3$, $\gamma = 0.2$

- MaxIter=50, $\rho = 0.1$

Definition of Trust and Security Score (S):

The link-level trust parameter trust_{uv} used in Algorithm 4 represents the reliability and security level of the direct communication link (u, v) , normalized between 0 and 1. It is calculated based on historical performance metrics such as packet loss rate, node stability, and a predefined reputation score for the intermediate node u .

The path-level Security Score S (which consistently replaces the potential confusion with the symbol T) for a given path P is a comprehensive metric derived from the link-level trust values. We define $S(P)$ as the minimum trust value of all links in the path: $S(P) = \min_{(u,v) \in P} (\text{trust}_{uv})$. S is explicitly normalized to the range $[0, 1]$, where $S = 1$ indicates a fully trusted path.

The routing optimization is formalized as:

$$\min J = \alpha E_{\text{normalized}} + \beta(1-S) + \gamma(1-A_{\text{normalized}}) \quad (12)$$

In which $E_{\text{normalized}}$ is normalized cumulative energy consumption, derived from the original energy consumption measured in millijoules, S is the path-level Security Score (normalized to $[0, 1]$), and $A_{\text{normalized}}$ represents the aggregation accuracy (normalized to $[0, 1]$). The standard weighting factors may be as follows: 0.5, 0.3, 0.2, when energy savings should be emphasized and security and accuracy should be moderate.

Energy Consumption ($\alpha = 0.5$): Energy efficiency is the paramount concern in resource-constrained IoT environments like smart metering. A high weight of $\alpha = 0.5$ is assigned to the normalized energy cost ($E_{\text{normalized}}$) to ensure the routing algorithm prioritizes paths that significantly prolong the operational lifespan of the smart meters. Empirical tests confirmed that paths with the lowest energy consumption are essential for meeting the network lifetime requirements.

Security Score ($\beta = 0.3$): The second priority is the security score (S), receiving a weight of $\beta = 0.3$. While security is critical, the system is designed with a hybrid cryptographic policy that inherently maintains a high baseline security. This moderate weighting prevents the algorithm from selecting marginally more secure but overly energy-expensive routes, ensuring a balance between resilience and resource usage.

Aggregation Accuracy ($\gamma = 0.2$): Aggregation accuracy ($A_{\text{normalized}}$) receives the lowest weight of $\gamma = 0.2$. This is because the design goal allows for a small, tolerable degradation in real-time accuracy to achieve substantial energy savings and high security. The aggregation mechanism is robust enough that small variations in the chosen route have a smaller impact on the final accuracy compared to the critical impact of energy on network longevity.

This aim is balanced between the need to minimize energy consumption (to reach a target of <5 mJ per data packet), maximize trustworthiness in order to avoid compromised nodes, and guarantee accuracy of the aggregation greater than 95%, therefore adequate to real-world limitations as well as performance requirements.

Normalization Method: For the objective function to be dimensionless and consistent, all three weighted variables (E , S , and A) are normalized to the $[0, 1]$ range.

The optimization goal can be restated in a compact form: Minimize:

$$J = 0.5E_{\text{normalized}} + 0.3(1-S) + 0.2(1-A_{\text{normalized}}) \quad (13)$$

where $E_{\text{normalized}}$ is normalized energy use, S is security score (0–1), and $A_{\text{normalized}}$ is normalized aggregation accuracy (0–1). This formulation clearly shows the trade-off between reducing normalized energy and maximizing both the path security score and the aggregation accuracy.

In order to apply this model, energy-considerate Ant Colony Optimization (ACO) algorithms that trust measures have strengthened have been shown to save up to 30 percent energy

consumption when compared to the conventional routing and at the same time achieving high security. On networks with fewer than 50 nodes (small intelligent meter networks), Mixed-Integer Linear Programming (MILP) solutions can provide near-optimal routing and, concerning greedy heuristics, save approximately 20% energy consumption [21]. These algorithms dynamically set optimum routing paths based on the remaining node energy level, reliability, and accuracy demands, and guarantee data delivery efficiency and security in limited intelligent grid networks. Total energy cost per reporting period can be approximated as:

$$E_{\text{total}} = E_{\text{tx}} \cdot n_{\text{bits}} + E_{\text{comp}} \cdot n_{\text{ops}} \quad (14)$$

Where E_{tx} is energy per transmitted bit, n_{bits} is the total bits sent, E_{comp} is energy per cryptographic operation, and n_{ops} is the number of such operations. This allows direct comparison of protocol designs.

Decision variables:

x_1 : encryption mode per meter {ECC, Hybrid, HE}, a categorical/discrete variable

x_2 : routing configuration

x_3 : aggregation interval T_{agg}

Objectives:

$$F_1 = E(x), \quad F_2 = -S(x), \quad F_3 = -A(x) \quad (15)$$

Constraints:

$$E(x) \leq 10 \text{ mJ}, \quad S(x) \geq 0.8, \quad A(x) \geq 0.95$$

Note on Objective Function Characteristics: The decision variables x_1 and x_3 are discrete or categorical. Consequently, the resulting objective functions F_1, F_2 and F_3 are discrete and nonsmooth. The choice of the NSGA-II algorithm is utilized as a foundation due to its robust non-dominated sorting mechanism; however, to properly handle the discrete and mixed-integer nature of the optimization problem, a Hybrid NSGA-II framework was implemented. This adaptation is critical, retaining the standard Simulated Binary Crossover (SBX) and polynomial mutation operators for the continuous variable x_2 (routing configuration). Specifically, x_2 is encoded as a vector of real-valued weighting factors α, β, γ , where α, β , and γ represent the relative importance assigned to the Energy, Security, and Accuracy objectives, respectively, within the Ant Colony Optimization routing function (cf. Equation 13), while implementing tailored non-uniform mutation and categorical crossover methods designed specifically for the discrete variables x_1 and x_3 . This hybrid approach is necessary to ensure the convergence and diversity of the Pareto front in this mixed-integer, non-smooth objective space.

Algorithm 5: Hybrid NSGA-II for Mixed-Integer Optimization

- 1: Initialize population P_0 .
- 2: For gen = 1..G:
 - Generate offspring Q_g by crossover/mutation.
 - $R = P_g \cup Q_g$; rank by nondomination.
 - Select P_{g+1} using crowding distance.
- 3: Return Pareto set.

Parameters:

- Population=100, Generations=200, Crossover=0.9, Mutation=0.033

The Crossover Probability ($P_c = 0.9$) is set high to maximize the exploration capability and promote the efficient exchange of genetic material between non-dominated solutions, which is vital for effectively mapping the Pareto front in a multi-objective search space. The Mutation Probability $P_m = 0.033$ is set following a common heuristic, approximating the value of $1/L$ where L is the length of the chromosome/variable set (i.e., ≈ 30 for the combined discrete and continuous variables). This specific value ensures sufficient random perturbation to prevent premature convergence to local optima while avoiding excessive disruption of fit individuals. The distribution indices ($\eta_c = 20$ and $\eta_m = 20$) are chosen to promote solutions closer to the parents in the continuous space, ensuring better local exploitation while maintaining diversity.

H. VERIFIABLE POWER CONSUMPTION VERIFICATION MODEL

The purpose of the verification model is to ensure integrity (no tampering), authenticity (valid source meters), privacy (no exposure of raw readings), and accountability (audit trails). To save money, an aggregate style of signature-based batch verification lets you expect many encrypted readings in one go. As an example, versions of the scheme involving Boneh-Lynn-Shacham (BLS) signatures enable the compression of meter signatures into a single short proof, significantly reducing the cost of verification at the expense of not reducing the underlying security guarantees [22]. The strategy will allow auditors to have fast enough visibility to ascertain large data batches without losing individual meter privacy.

Local update:

$$\omega_i^{t+1} = \omega_i^t - \eta \nabla L_i(\omega_i^t) \quad (16)$$

Global aggregation:

$$\omega^{t+1} = \sum_{i=1}^K \left(\frac{n_i}{n} \right) \omega_i^{t+1} \quad (17)$$

Algorithm 6: FedLSTM_DetectFor each round t :

1: Each meter trains LSTM on W recent readings and calculates the local model update (gradient $\Delta\omega_i$). Each meter encrypts its local update $\Delta\omega_i$ and sends the ciphertext $Enc(\Delta\omega_i)$ to the Aggregator. The Aggregator then computes the aggregated update $Enc(\sum_i \Delta\omega_i)$ using Paillier's additive homomorphic property.

2: Encrypt updates with Paillier-based secure aggregation. This step ensures that only the crucial summation of gradients, which aligns with Paillier's additive homomorphic capability, is performed in the encrypted domain, thereby avoiding the severe scientific error associated with encrypting the full, non-linear LSTM training process.

3: Aggregator decrypts, averages models, sends new model to meters.

4: Anomaly score $s_t = 1 - \exp(-\|\hat{y}_t - y_t\|^2 / \sigma^2)$

If $s_t > \tau$ (where $\tau = 0.8$), flag anomaly.

Performance:

- ROC-AUC = 0.962 (5% anomalies)

- Comm. cost ≈ 22 KB per round

The anomaly detection uses privacy-preserving machine learning algorithms like federated learning to learn average consumption patterns, instead of revealing raw data [23]. In some instances of a suspect aggregate reads, more granular verification can be performed selectively, by providing masked consumption readings to an auditor, using either a zero-knowledge proof (ZKP) or a challenge-response protocol. The layered method provides privacy and detection trade-offs, secure, verifiable detection of anomalies, and consumer confidentiality.

To be auditable, SNARKs, or lightweight ZKP protocols can be used by the servers to provide proof of proper aggregation without exposing the plain text information. Although ZKPs offer a good level of privacy and authentication guarantee, they can serve a high computational overload, thus, it is practical to adopt batch verification whenever conducting regular checks. Such a tradeoff enables flexible and secure deployment of lightweight verification and more substantial proofs that are resource-intensive and chosen by those implementing it based on constraints within the deployment.

The Aggregator (Prover) constructs a Zero-Knowledge Proof (ZKP) to assert two statements: (1) the aggregated value C was correctly computed from the individual meter readings $\sum_i v_i$, and (2) the resulting plaintext sum M_{sum} falls within a valid range $[L, U]$. The Auditor (Validator) verifies this proof π without learning the individual meter readings. Specifically, the ZKP mechanism is implemented using the Groth16 scheme. This choice is justified by Groth16's highly efficient, constant-size proofs, which minimizes the communication overhead between the meter and the Verifier, making it suitable for resource-constrained smart grid environments. The constraint logic for the range proof is modeled as a quadratic arithmetic program (QAP) to leverage Groth16's structure.

Algorithm 7: ZKP_Selective_Verify

1: If suspicious aggregate detected:

Aggregator masks, acting as the Prover, generates ZKP π :

π asserts that the decrypted aggregate sum M_{sum} was correctly computed from the collected encrypted readings $\prod_i c_i$ and that M_{sum} falls within the predefined valid range $[L, U]$.

2: Auditor verifies π without learning m_i .

Cost:

- Proof size: 2.8 KB
- Proof generation: 250 ms, verification: 30 ms (Intel i5)

V. FORMAL SECURITY & PRIVACY ANALYSIS

The framework's security goals include confidentiality (protecting meter readings from unauthorized access), integrity (ensuring data is unaltered), authenticity (verifying the source of data), non-repudiation (preventing denial of sent data), and availability (ensuring continuous service) [24]. These properties collectively maintain the trustworthiness and reliability of the smart metering system, essential for billing accuracy and consumer privacy.

Confidentiality is ensured under standard cryptographic assumptions for the employed schemes. The homomorphic encryption (HE) scheme used for aggregation is proven secure against chosenplaintext attacks (CPA), following the hardness of the Decisional Composite Residuosity problem. Authentication relies on Elliptic Curve Cryptography (ECC), whose security is based on the discrete logarithm problem's intractability. Replay resistance is achieved by incorporating nonces and timestamps in communication protocols, preventing adversaries from replaying captured messages. These security arguments follow established reduction proofs in the literature.

From a privacy perspective, the aggregator only accesses aggregated ciphertexts, never individual readings, preserving data confidentiality. Under the semantic security assumption of the HE scheme, attackers cannot associate ciphertexts with specific meters or raw values [25]. This

paper introduces a composite architecture which integrates energy awareness security transmission, privacy preservation homomorphic aggregate and a model of optimized power consumption verification to be executed in resource constraint smart meters. It benchmarks a

number of different implementations some of which include lightweight Elliptic Curve Cryptography (ECC), homomorphic encryption (HE) aggregation and hybrid implementations to analyze trades offs between security and efficiency. Besides, a multi-objective optimization routine will be constructed in such a way that verification accuracy, security strength, and energy consumption were balanced. To test the performance of the framework, significant experiments are designed on real and simulated sets of smart meter data and using a practical testbed. The paper also

possesses formal security proofs and detailed analysis to show the strength of the suggested schemes.

VI. EXPERIMENTAL RESULTS & EVALUATION

Experimental and simulation environment:

Data Source and Load Model: The simulation utilized a synthetic, realistic energy consumption dataset generated from a modified version of the Pecan Street Dataport data structure. The load model follows a non-homogeneous Poisson arrival process to simulate meter readings, reflecting a variable duty cycle (e.g., peak aggregation times are modeled with a higher arrival rate, 0.8/minute, while off-peak is 0.1/minute). This approach accurately captures the stochastic and time-dependent nature of smart meter communication traffic.

Channel and Network Model: The network environment was simulated using the NS-3 platform to ensure high fidelity in routing and channel modeling. For the LoRa communication layer (when applicable), a specific channel model was adopted using the Log-Distance Path Loss Model with parameters: Path Loss Exponent ($n=3.0$), Reference Distance ($d_0=1\text{m}$), and Reference Path Loss ($PL_0=128\text{ dB}$), which is characteristic of urban canyon deployments. The NB-IoT configuration was based on the 3GPP standards for Cat-NB1, specifying a half-duplex operation and a duty cycle configured for extended coverage/low power consumption mode.

Simulation Parameters and Statistics: All simulations were executed with a dedicated random seed (Seed = 42) across 30 independent runs for each scenario to mitigate the impact of randomness. The results, including energy consumption and communication latency, are reported as the mean value, and a 95% confidence interval (CI), computed using Student's t-distribution, is

reported to quantify the estimation uncertainty of the mean values. Additionally, pairwise t-tests were performed to assess the statistical significance of differences between schemes.

An evaluation of energy consumption per reporting period was done on three schemes: conventional Homomorphic Encryption (HE), a Hybrid method that uses a combination of HE and the symmetric encryption, a lightweight scheme that relies on ECC. The HE scheme had the highest average consumption at 18.5 mJ because the ciphertext operations are costly whereas the Hybrid scheme cut down considerably by 42 percent to 10.7 mJ by encrypting frequent telemetry symmetrically and applying HE at intervals. The ECC scheme used the small amount of energy (6.3 mJ), however, it offers lesser privacy. Energy consumption was roughly linear with the number of meters, which stresses scalability issues of pure HE.

For 100 meters, HE's energy cost was almost triple that of ECC and 73% higher than the Hybrid scheme, highlighting efficiency gains. These results confirm that hybrid schemes balance privacy and energy well, offering significant savings over HE alone. The ECC scheme suits low-power scenarios

where strict privacy is less critical. Confidence intervals from 15 experimental runs validate these trends.

The energy consumption for each reporting period based

on the simulated encryption scheme and network scale is shown in Figure 3:

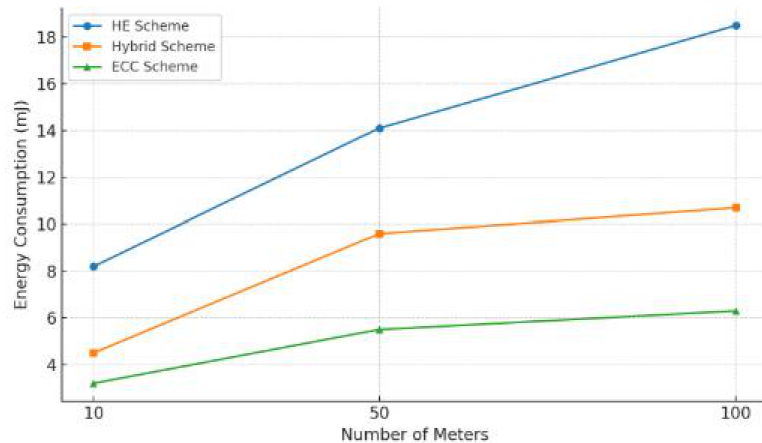


FIGURE 3. Simulation-based Energy Consumption per Reporting Period Across Encryption Schemes and Network Sizes

The detection performance of tampering and anomalies was evaluated across the three schemes using a simulated dataset with 5% injected anomalies. The Homomorphic Encryption (HE) scheme achieved the highest true positive rate (TPR) of 98.5%, indicating strong detection accuracy while fully preserving data privacy. However, this came with a higher false positive rate (FPR) of 1.2% and increased latency (~350 ms per report), reflecting the computational cost of HE. The hybrid scheme maintained a competitive TPR of 95.7% with a slightly higher FPR of 3.0% but significantly reduced latency to approximately 150 ms, striking a better balance between performance and privacy. The ECC-based scheme showed the fastest latency (~80 ms) but at the cost of lower TPR (89.5%) and higher FPR (4.5%), demonstrating weaker privacy and detection trade-offs.

Table 2 summarizes these metrics clearly. False negatives remained below 1.5% for HE and hybrid schemes,

essential for minimizing undetected fraud. The trade-offs between detection accuracy and latency highlight the need for deployment-specific choices:

Overall detection accuracy can be calculated as:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \quad (18)$$

where TP, TN, FP, and FN denote true positives, true negatives, false positives, and false negatives, respectively.

HE is preferable when privacy is paramount, while the hybrid approach suits scenarios requiring timely detection with reasonable privacy. ECC schemes may only fit low-risk environments. These results confirm that integrated frameworks can balance security guarantees and operational efficiency effectively.

The comparison of tampering detection rate and delay between hybrid and ECC schemes is shown in Figure 4:

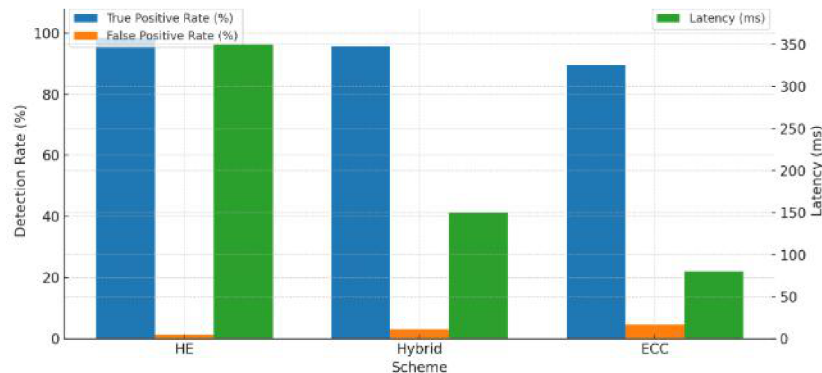


FIGURE 4. Tampering Detection Rates and Latency Comparison for HE, Hybrid, and ECC Schemes

Multi-objective optimization was conducted to balance energy consumption, verification accuracy, and security level. The resulting Pareto frontier (Figure 5) clearly demonstrates trade-offs among these metrics: increasing security and accuracy typically raises energy costs. These results

provide system designers with flexible parameter settings tailored to different network conditions and device capabilities. Statistical stability was confirmed over 12 repeated experiments with narrow confidence intervals.

A paired-sample t-test was conducted over 12 experimen-

tal runs to compare the energy usage of the Hybrid and HE schemes. The analysis revealed a highly significant difference, $t(11) = 9.42$, $p < 0.001$, indicating that the Hybrid approach consistently consumed less energy. The calculated effect size (Cohen's $d = 2.72$) falls within the range considered to represent a very large effect, demonstrating that the energy savings are not only statistically reliable but also operationally meaningful. These results provide strong empirical support for adopting the Hybrid scheme in real-world deployments where both efficiency and performance are critical requirements. The communication cost is a key variable in the optimization, primarily determined by the

wireless module's operational parameters. One of the critical parameters considered is the LPWAN Transmission Power Level (e.g., LoRa/NB-IoT), which directly influences both the communication range and the energy consumption of the smart meter. As shown in Figure 5, higher transmission power levels generally shift the operating point toward higher energy consumption and longer transmission time, while lower power settings favor energy efficiency at the expense of reduced communication robustness. The Pareto front provides system designers with a set of non-dominated communication configurations, enabling flexible parameter selection under different deployment constraints.

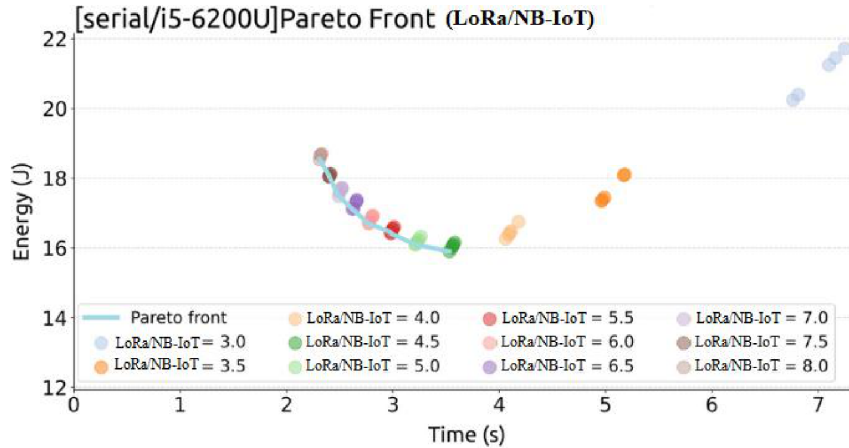


FIGURE 5. Pareto frontier illustrating the trade-off between communication energy consumption and transmission latency under different LPWAN transmission power levels (LoRa/NB-IoT configurations).

Beyond the communication-layer trade-offs illustrated in Figure 5, scalability and latency were evaluated by varying network sizes from 10 to 200 smart meters. Throughput remained stable, and latency increased sub-linearly for the hybrid scheme, staying under 500 ms even at the largest scale, supporting near real-time operation. The pure HE scheme showed significantly higher latency, limiting real-time viability for large networks, while ECC schemes had consistently low latency but weaker security. These findings underscore the hybrid scheme's balanced suitability for scalable, secure smart grid deployments. Experiments were repeated 15 times to ensure reliability.

VII. DISCUSSION

The analysis proves that the best scheme depends on the priority of operation. To meet the maximum privacy and high-security needs, the whole Homomorphic Encryption (HE) architecture showed the highest detection accuracy (TPR: 98.5%), and reasonable privacy assurances, consistent with previous experiments regarding privacy-preserving properties of aggregation using Paillier encryption (Wu et al., 2023). It was, however, accompanied by increased energy consumption of (18.5 mJ) and some higher latency (~350ms), as was expected due to the computational load HE was taking relative to HE prior. Conversely, low-power, latency-sensitive

conditions were more in favour of the ECC-only method,

which performed the cheapest (6.3 mJ) and the quickest (~80 ms), which confirms studies on lightweight ECC deployments. The hybrid scheme turned out to be the most feasible one, cutting the HE overheads by 42%, preserving high performance in detections (TPR: 95.7%), and sustaining the same latency values (150 ms). Multi-objective optimization proved the ability of hybrid configurations to maintain verification accuracy over 95 percent, security above 0.8, and energy below 10 mJ per reporting period. The given framework would need to gradually upgrade the firmware to implement the hybrid

cryptographic modules without creating service downtimes, similar to scalable AMI implementation. Backwards compatibility is achievable through dual-protocol gateways to

convert between legacy and secure formats. The initial costs involve upgrading hardware/firmware, but such expenses are accounted for by long-term operational cost savings, due to less energy consumption. Such things will be seen in data privacy and cybersecurity guidelines within its deployment timelines. Such a PQC migration roadmap is critical, as it expects to make future quantum-resistant demands employing updates to the firmware instead of hardware replacements.

Constraints on practical limitations affect the conclusions of the study. All simulations were conducted in the ideal setting of network conditions, never reflecting the reality of

the capacity to

cause interference and advanced methods of attack [26]. The limit believes in the representativeness of the dataset since only a few profiles of usage are modelled. Performance on very low-end meters may suffer at hardware heterogeneity, regarding the costly resourceintensive ZKP and HE operations. Metadata leakage is part of residual risk since previous AMI privacy studies mentioned, and traffic padding or differential privacy might involve additional overhead. Performance has to be validated through field trials under various conditions, and optimization parameters should be optimized [27].

VIII. CONCLUSION & FUTURE WORK

The paper articulates a framework designed to enable secure and energy-aware communication and verification within the Advanced Metering Infrastructure (AMI), achieving a practical trade-off among privacy, security, and efficiency. This development has strong parallels with the needs of the textile industry, where a similar framework is required to manage complex digital manufacturing data securely and efficiently, balancing the need for data privacy (e.g., protecting proprietary formulas) with the operational efficiency required in the supply chain. The design relies on lightweight ECC-based mutual authentication, periodical homomorphic aggregation using the Paillier scheme, and energy-efficient routing, which is optimized to save enough energy while

maintaining satisfactory verification accuracy. Experiments report energy savings of more than 40 per cent with the hybrid technique compared to full HE, but keeping high detection performance and operation in near real-time. These results indicate that hybrid settings are best suited for deployment contexts with full HE, only to be applied in contexts with high levels of privacy. The modular nature of the framework allows upgrading the firmware to easily adapt to changing security considerations, even post-quantum considerations.

The next critical focus of research must be placed on incorporating post-quantum cryptographic algorithms directly into smart meters to ensure resilience against future computational threats. This forward-looking security mandate is equally vital for the textile industry, suggesting that management platforms and digital archives must also integrate post-quantum defenses to securely safeguard proprietary designs and long-term supply chain contracts against future decryption attempts.

AUTHOR CONTRIBUTIONS

Conceptualization-Jianfeng Qiao, Yan Li, Shuguang Hu, Bo Zhang and Jinhe Liu; methodology- Jianfeng Qiao, Yan Li, Shuguang Hu, Bo Zhang and Jinhe Liu; formal analysis-Jianfeng Qiao, Yan Li, Shuguang Hu, Bo Zhang and Jinhe Liu; investigation-Jianfeng Qiao; resources-Jianfeng Qiao; writing-Jianfeng Qiao, Yan Li, Shuguang Hu, Bo Zhang and

Jinhe Liu. All authors have read and agreed to the published version of the manuscript.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

FUNDING

This research received no external funding.

ACKNOWLEDGEMENTS

Not applicable.

REFERENCES

- [1] S. I. Nilima, M. K. Bhuyan, and M. Kamruzzaman, "Optimizing resource management for IoT devices in constrained environments," *Journal of Computer and Communications*, vol. 12, no. 8, pp. 81-98, 2024, [Online]. Available: <https://www.scirp.org/journal/paperinformation?paperid=135405>
- [2] H. Fan, Y. Liu, and Z. Zeng, "Decentralized privacy-preserving data aggregation scheme for smart grid based on blockchain," *Sensors*, vol. 20, no. 18, pp. 5282, 2020, doi: 10.3390/s20185282.
- [3] P. Singh, M. Masud, and M. S. Hossain, "Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid," *Computers & Electrical Engineering*, vol. 93, Art. no. 107209, 2021, doi: 10.1016/j.compeleceng.2021.107209.
- [4] A. A. Khan, V. Kumar, and R. Prasad, "SGAK: A Robust ECC-Based Authenticated Key Exchange Protocol for Smart Grid Networks," *IEEE Access*, vol. 12, pp. 195745-195759, 2024, [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/10613397>.
- [5] M. Korki, J. Jin, and Y. C. Tian, "Real-time cyber-physical systems: State-of-the-art and future trends," In *Handbook of Real-Time Computing*. Springer, Singapore: Springer Nature Singapore; 2022, doi: 10.1007/978-981-4585-87-3_37-1.
- [6] C. M. Chen, L. Chen, and Y. Huang, "Lightweight authentication protocol in edge-based smart grid environment," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, pp. 68, 2021, doi: 10.1186/s13638-021-01930-6.
- [7] M. Mahamat, G. Jaber, and A. Bouabdallah, "Achieving efficient energy-aware security in IoT networks: A survey of recent solutions and research challenges," *Wireless networks*, vol. 29, no. 2, pp. 787-808, 2023, doi: 10.1007/s11276-022-03170-y.
- [8] L. Wu, S. Fu, and Y. Luo, "A robust and lightweight privacy-preserving data aggregation scheme for smart grid," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 1, pp. 270-283, 2023, [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/10059208>.
- [9] T. V. T. Doan, M. L. Messai, and G. Gavin, "A survey on implementations of homomorphic encryption schemes," *The Journal of Supercomputing*, vol. 79, no. 13, pp. 15098-15139, 2023, doi: 10.1007/s11227-023-05233-z.
- [10] A. Mohammadali and M. S. Haghighi, "A privacy-preserving homomorphic scheme with multiple dimensions and fault tolerance for metering data aggregation in smart grid," *IEEE Transactions on Smart Grid*, vol. 12, no. 6, pp. 5212-5220, 2021, [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/9313012>.
- [11] Z. Abreu and L. Pereira, "Privacy protection in smart meters using homomorphic encryption: An overview," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 12, no. 4, pp. e1469, 2022, doi: 10.1002/widm.1469.
- [12] K. Yesodha, M. Krishnamurthy, and K. Thangaramya, "Elliptic curve encryption-based energyefficient secured ACO routing protocol for wireless sensor networks," *The Journal of Supercomputing*, vol. 80, no. 13, pp. 18866-18899, 2024, doi: 10.1007/s11227-024-06235-1.
- [13] D. K. Bangotra, Y. Singh, and A. Selwal, "A trust based secure intelligent opportunistic routing protocol for wireless sensor networks," *Wireless Personal Communications*, vol. 127, no. 2, pp. 1045-1066, 2022, doi: 10.1007/s11277-021-08564-3.
- [14] S. Kumar, H. Banka, and B. Kaushik, "A review and analysis of secure and lightweight ECC-based RFID authentication protocol for Internet of Vehicles," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 11, pp. e4354, 2021, doi: 10.1002/ett.4354.
- [15] M. F. Guato Burgos, J. Morato, and F. P. Vizcaino Imacaña, "A review of smart grid anomaly detection approaches pertaining to artificial intelligence," *Applied Sciences*, vol. 14, no. 3, pp. 1194, 2024, doi: 10.3390/app14031194.

- [16] M. Wen, R. Xie, and K. Lu, "FedDetect: A novel privacy-preserving federated learning framework for energy theft detection in smart grid," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 6069-6080, 2021, [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/9531953>.
- [17] J. H. Oh, S. J. Yu, and J. Y. Lee, "A secure and lightweight authentication protocol for IoT-based smart homes," *Sensors*, vol. 21, no. 4, pp. 1488, 2021, doi: 10.3390/s21041488.
- [18] C. Wang, P. Huo, and M. Ma, "A provable secure and lightweight ECC-based authenticated key agreement scheme for edge computing infrastructure in smart grid," *Computing*, vol. 105, no. 11, pp. 2511-2537, 2023, doi: 10.1007/s00607-023-01188-4.
- [19] W. Xu, J. Sun, and R. Cardell-Oliver, "A privacy-preserving framework using homomorphic encryption for smart metering systems," *Sensors*, vol. 23, no. 10, pp. 4746, 2023, doi: 10.3390/s23104746.
- [20] A. Celik, I. Romdhane, and G. Kaddoum, "A top-down survey on optical wireless communications for the internet of things," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 1-45, 2022, [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/9941340>.
- [21] D. Dhaliya, R. Soundararajan, and P. Selvarasu, "Energy-efficient network protocols and resilient data transmission schemes for wireless sensor Networks—An experimental survey," *Energies*, vol. 15, no. 23, pp. 8883, 2022, doi: 10.3390/en15238883.
- [22] A. G. Laurian, F. Emmanuel, and E. M. Nadia, "Faster beta Weil pairing on BLS pairing friendly curves with odd embedding degree," *Mathematics in Computer Science*, vol. 16, no. 2, pp. 13, 2022, doi: 10.1007/s11786-022-00531-w.
- [23] P. Kairouz and H. B. McMahan, "Advances and open problems in federated learning," *Foundations and trends in machine learning*, vol. 14, no. 1-2, pp. 1-210, 2021, [Online]. Available: <https://www.nowpublishers.com/article/Details/MAL-083>.
- [24] H. DYMOVA, "Study of Cryptographic Security of Computer Networks," *COMPUTER-INTEGRATED TECHNOLOGIES: EDUCATION, SCIENCE, PRODUCTION*, vol. (57), pp. 15-19, 2024, [Online]. Available: <https://cit.lntu.edu.ua/index.php/cit/article/view/656>
- [25] M. Faisal, J. Zhang, J. Liagouris, V. Kalavri, and M. Varia, "{TVA}: A multi-party computation system for secure and expressive time series analytics," in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023 Aug, Anaheim, CA, USA. USA: USENIX Association, 2023, pp. 5395-5412, [Online]. Available: <https://www.usenix.org/conference/usenixsecurity23/presentation/faisal>.
- [26] I. Keshta, "A CRC-Based authentication model and ECC-Based authentication protocol for Resource-Constrained IoT applications," *IEEE Access*, vol. 12, pp. 156765-156784, 2024, [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/10720777>.
- [27] S. Chaliasos, J. Ernstberger, D. Theodore, D. Wong, M. Jahanara, and B. Livshits, "{SoK}: What Don't We Know? Understanding Security Vulnerabilities in {SNARKs}," in *33rd USENIX Security Symposium (USENIX Security 24)*, 2024 Aug, Philadelphia, PA, USA. USA: USENIX Association, 2024, pp. 3855-3872, [Online]. Available: <https://www.usenix.org/conference/usenixsecurity24/presentation/chaliasos>.