Design and Evaluation of a Multi-Level Verification System for Secure Communication Protocols in Energy Billing

Wanchun Yang, Jianfeng Qiao, Jifu Hu, Jiaqi Wang, Hao Wu
Power Marketing Service and Operation Management Branch, Inner Mongolia Electric Power (Group) Co., Ltd., Hohhot 010011, Inner Mongolia, China
Corresponding author: Wanchun Yang (e-mail: 18847900068@163.com)

ABSTRACT This study presents a multi-level verification system for secure communication protocols in energy billing infrastructures. The proposed framework integrates device attestation, network integrity verification, privacy-preserving aggregation, billing validation, and immutable auditing to address security vulnerabilities across Advanced Metering Infrastructure (AMI) communication chains. A Hybrid Secure-Efficient Protocol (HSEP) combining elliptic curve cryptography, homomorphic encryption, and zero-knowledge proofs is developed to provide secure authentication, privacy protection, and verifiable data integrity while maintaining low computational overhead. Experimental evaluation using a large-scale AMI testbed demonstrates that the proposed system significantly improves tampering detection capability, achieving an intrusion detection AUC of 0.94 while maintaining an average energy consumption of 1.55 J per transaction and acceptable communication latency for large-scale deployment. The architecture exhibits strong scalability, robustness, and rapid dispute-resolution performance under multiple attack scenarios. The proposed framework is particularly applicable to wireless smart metering networks and antenna-enabled AMI communication infrastructures, where reliable data transmission, secure protocol verification, and resilience against communication-layer attacks are essential for trustworthy energy billing and grid operation. This work provides an effective engineering solution for secure, privacy-preserving, and verifiable communication in modern intelligent energy systems.

INDEX TERMS secure communication protocols, advanced metering infrastructure, privacy-preserving billing, wireless smart metering networks

I. INTRODUCTION

BILLING security in innovative metering systems is essential for ensuring accurate invoicing, preserving user privacy, and maintaining the stability of grid operations. Smart meters collect fine-grained consumption data, which, while useful for billing, demand response, and analytics, carries severe privacy implications due to the sensitive patterns derivable from occupancy and appliance usage. however, this information requires stringent security protocols. The proprietary nature of insights derived from these data streams—including manufacturing specifications, process efficiency benchmarks, and contractually sensitive volume metrics— necessitates robust data governance [1]. Recent Advanced Metering Infrastructure (AMI) analyses identify critical vulnerabilities in device firmware, communications protocols, and back-end processing, all of which may be exploited to manipulate data, commit billing fraud, or launch denial-of-service attacks.

White collar crimes in the billing process may lead to direct financial loss to utilities and consumers and diminish the confidence in the energy market. The malicious actors could inject fake data, take over meters, or alter aggregation, resulting in skewed billing and poor demand-response functionality [2]. It has been found that widespread meter compromises can disrupt threats in grid control systems, which may have implications for stability and reliability [3]. Smart meter infrastructures typically rely on limited protection, making standard Transport Layer Security (TLS) vulnerable to skilled attacks. Malfunctioning meters can inject falsified data, bypassing detection and compromising billing integrity, despite encryption. Aggregation tampering by intermediary or billing servers is a major weakness, especially from internal threats. Furthermore, implementation bugs, including a lack of interoperability or full DLMS/COSEM compliance, provide critical entry points for attackers [4]. Achieving secure and interoperable operations necessitates rigorous compliance testing against the IEC 62056 standards, as any deviation from their established authentication levels and conformance requirements exponentially increases vulnerability [5]. Unless it embraces multi-

layered security systems through combining encryption, authentication, compliance checks, and anomaly detection, the smart meter ecosystem will continue to be vulnerable to being manipulated, defrauded, and disrupted in delivering its services.

The paper has several contributions to secure and verifiable AMI billing. First, it proposes a multi-tier verification architecture involving multi-level checks at device, network, and aggregate levels combined with a separate auditing process. Second, it formalizes verification properties and a complete threat model concerning cyber and insider attacks. Third, it introduces lightweight protocols and mix-and-match aggregation-verification approaches that are energy efficient yet robust. Fourth, it proves the practicality of the system on a working prototype that involves the implementation of the system on actual and simulated data and measures performance based on energy, security, and verification accuracy. The embrace of transparency and open science principles yields substantial advantages, specifically by supplying validated, standardized methodologies and data architectures. This foundation is critical for expediting both the creation and third-party audit of advanced security and operational protocols within digital supply chain ecosystems.

To complement the qualitative motivation, we quantify security risk across common AMI attack classes using a probability–impact model. For each attack $a \in A$ (e.g., data replay, false data injection, meter compromise, aggregation tampering, insider manipulation, DoS), we define an annualized risk score:

$$Risk(a) = P_{attack}(a) \times I_{sevenity}(a) \tag{1}$$

We estimate $P_{attack}(a)$ from incident frequency via a Poisson arrival model,

$$P_{attack}(a) = 1 - e^{-\lambda_a T} \tag{2}$$

with λ_a the observed (or simulated) yearly rate and $T = 1$ year. Impact decomposes over confidentiality, integrity, and availability:

$$I_{sevenity}(a) = \omega_C I_C(a) + \omega_I I_I(a) + \omega_A I_A(a), \quad \omega_C + \omega_I + \omega_A = 1 \tag{3}$$

where $I.(a) \in [0, 1]$ are normalized loss severities (e.g., financial loss, regulatory exposure, safety implications), and $(\omega_C, \omega_I, \omega_A)$ reflect utility priorities (default = (0.3,0.5,0.2) to emphasize billing integrity).

We report both a unitless Risk score $\in [0, 1]$ and an Annualized Loss Expectancy (ALE) to support cost–benefit analysis:

$$ALE(a) = Risk(a) \times L(a) \tag{4}$$

where L(a) is the expected monetary loss if a occurs (fraud write-offs, truck rolls, penalties).

Illustrative calibration (for prioritization). Example inputs and computed scores are shown below; values can be replaced by site data or your Section "EXPERIMENTAL RESULTS" simulations. The risk model table is shown in Table 1:

This matrix yields a ranked queue for mitigation and maps directly to your multi-level design: device attestation reduces P_{attack} for meter compromise; network integrity and sequence checks lower replay probability; privacy-preserving aggregation and auditor ZK proofs reduce the impact of aggregation tampering by limiting exploitable plaintext and improving non-repudiation. We use these calibrated risks in Sections "MULTI-LEVEL VERIFICATION ARCHITECTURE"–"EXPERIMENTAL RESULTS" to select HSEP parameters that maximize risk reduction per joule and to report risk-adjusted performance deltas.

II. RELATED WORK

Current research on Advanced Metering Infrastructure (AMI) extensively details the dynamic nature of security threats, highlighting the pivotal role of effective defensive mechanisms in realizing a secure next-generation smart grid. Analysis of security incidents reveals three critical avenues for compromise: the inherent difficulty in manipulating specific system metrics, vulnerabilities arising from overly permissive system configurations, and the acute risk presented by internal actors with privileged access to sensitive metering information or core infrastructure controls [6]. Tampered meters might have been reprogrammed to report consumption levels, or even skip measuring completely incorrectly. In contrast, insecure communication protocols like weak encryption or authentication can be used by attackers to eavesdrop on and modify data traveling via the network [7]. Moreover, insider threats are also a fundamental issue because they may exploit physical devices and backend systems, particularly in the utility setting that does not apply proper protection on access [8].

The versatility of security issues in every AMI deployment is another important finding in recent reviews, as security challenges most of the time differ in hardware supports, communication technologies, and regulatory requirements. To take an example, although an urban deployment can use a high bandwidth and its system can support robust encryption, in rural deployments, systems operate on bandwidth-limited connections that do not support heavy encryption protocols [9]. In addition, systematic studies have reported that with the emergent trend in present-day attackers, i.e., coordinated load-altering attacks and firmware manipulation, there is an increasing demand for integrating detection architectures involving local device-level security with centralized analytics. Using case studies of large-scale threats, it can be established that attackers are finding that the weakest point in the system could be outdated meters or unmanaged gateway gadgets [10]. Lightweight authentication schemes, especially those implemented through Elliptic Curve Cryptography (ECC), have become popular

TABLE 1. Risk Model Table

Attack a	λ_a (yr^{-1})	P_{attack}	I_C	I_I	I_A	$I_{sevenity}$ (with $\omega_C = 0.3, \omega_I = 0.5, \omega_A = 0.2$)	Risk	$L(a)$ (USD)	ALE (USD/yr)
False data injection	0.40	0.3297	0.3	0.9	0.4	$0.3 \cdot 0.3 + 0.5 \cdot 0.9 + 0.2 \cdot 0.4 = 0.62$	0.204	500,000	102,000
Meter compromise	0.20	0.1813	0.4	0.8	0.3	$0.3 \cdot 0.4 + 0.5 \cdot 0.8 + 0.2 \cdot 0.3 = 0.58$	0.105	350,000	36,750
Aggregation tampering	0.10	0.0952	0.5	0.7	0.3	$0.3 \cdot 0.5 + 0.5 \cdot 0.7 + 0.2 \cdot 0.3 = 0.56$	0.053	1,200,000	63,600
Replay	0.60	0.4512	0.2	0.5	0.4	$0.3 \cdot 0.2 + 0.5 \cdot 0.5 + 0.2 \cdot 0.4 = 0.39$	0.176	120,000	21,120

Data Source Note: Example data.

in the scope of constrained smart meters because of their extremely low computational costs and energy consumption [11]. ECC-based protocols provide good security with a shorter key length than RSA and hence work well with meters that have limited processing capabilities. Besides the pure software-based schemes, hardware-based authentication systems with Trusted Platform Modules (TPM) and secure elements are becoming a popular scheme to perform device attestation so as to guarantee that meters will be able to demonstrate their integrity prior to being added to the network [12]. To confirm the trustworthiness of deployed meters, in distributed AMI systems in general and geographically distributed systems in particular, remote attestation protocols have been devised that include challenge-response and continuous verification models. The burden of integrating these lightweight mechanisms into the deployed AMI frameworks yields a large attack surface reduction without operating cost overhead penalty. Consumers' energy usage is very personalized, and as a result, studies have proposed privacy-preserving aggregation and billing. A homomorphic encryption mechanism, as developed by Paillier in his additive HE, enables utilities to perform aggregate consumption without obtaining their consumer readings, thus protecting user privacy. The distributed billing achieved by multi-party computation (MPC) and secret-sharing methods can also be applied to eliminate the exposure of individual meter data to any particular party [13]. New technologies like PA-Bill, peer-to-peer (P2P) billing frameworks, and use the reversible watermarking and aggregation trees to increase scalability. Nevertheless, these solutions are usually a trade-off: guaranteeing better privacy under profiling attacks can come at the cost of elevated computation and communication requirements, and especially so in the context of bandwidth-constrained AMI roll-outs [14]. In practice, therefore, this involves trade-offs between cost-effectiveness and efficiency on the one hand, and security, on the other.

III. SYSTEM MODEL, DATA MODEL & THREAT MODEL

The MLVS comprises four fundamental entities: the Smart Meter (SM), the Collector/Gateway, the Central Server (CS), and the Audit Blockchain.

ECC-Based Secure Session Module: This lightweight authentication protocol is embedded in the SM and Collector for efficient, low-latency mutual authentication and secure session key establishment. This ensures network integrity without overburdening meter resources.

Dual-Stage Device Attestation Module: Our system enforces a two-stage remote attestation process. This includes a mandatory boot-time integrity check and a periodic runtime attestation, ensuring continuous verification of the meter's Trained Execution Environment (TEE) and firmware authenticity.

Privacy-Preserving Data Aggregation Module: This module, located at the Collector/Gateway, utilizes Homomorphic Encryption (HE) and Zero-Knowledge Proofs (ZKP). It allows raw consumption data to be aggregated securely and verifiably before transmission, ensuring that all original data remains confidential and encrypted, even during verification.

Differential Privacy Anomaly Detection: The CS runs a sophisticated anomaly detection mechanism trained with Differential Privacy (DP) techniques. Specifically, we employ the Gaussian noise mechanism during the federated training process to satisfy (ϵ, δ)-differential privacy, using parameters $\epsilon = 0.8$ and $\delta = 10^{-5}$. This approach protects the privacy of individual node updates while maintaining anomaly detection performance. This ensures that while the model effectively identifies tampering patterns in the aggregated data, it inherently preserves the anonymity and privacy of individual users, making it robust against inference attacks. The proposed system is a multi-tier system AMI infrastructure with these key components: constrained smart meters at the edge that are connected through the Home Area Network (HAN) or mesh topologies, relay via data concentrator or gateways over WAN (e.g., NB-IoT, LoRaWAN, PLC), and up to the billing server and then to an independent auditor or regulator. Optional, non-colluding third-party servers can also be used to facilitate privacy-preserving aggregation: MPC or homomorphic encryption [15].

A. COMPARATIVE PERFORMANCE OF EXISTING AMI SECURITY MODELS

To contextualize our hybrid approach, we compare representative privacy-preserving and integrity-assuring models used in AMI deployments: Elliptic Curve Cryptography (ECC), Multi-Party Computation (MPC), Homomorphic Encryption (HE), and Blockchain-based ledgers. Metrics are aggregated from prior studies and normalized to a common deployment scale (5,000 meters, 24-hour reporting windows). The performance comparison is shown in Table 2:

The data indicate that while pure HE offers the strongest privacy, its cost in computation and energy renders it impractical for large-scale constrained deployments. MPC achieves strong privacy at moderate cost but scales less efficiently without optimized aggregation trees. ECC alone provides excellent performance but lacks privacy for aggre-

TABLE 2. Performance Comparison

Model	Computational Cost (ms per reading)	Energy Use (J per reading)	Scalability (Max Meters without Latency $>$ 300 ms)	Security Rating* (/10)	Key Advantages	Key Limitations
ECC (Curve25519)	4.2	0.025	50,000	8.5	Low energy, strong authentication, small key sizes	No aggregation privacy without pairing with MPC/HE
MPC (Shamir Secret Sharing)	15.8	0.072	10,000	9.0	Strong privacy, no single point of trust	Higher comm. overhead, moderate energy cost
HE (Paillier Additive)	42.5	0.210	5,000	9.5	Enables computation on encrypted data, full privacy	Very high latency/energy, not ideal for constrained meters
Blockchain (PoA Consensus)	28.6	0.150	8,000	9.2	Immutable audit trail, decentralization	Storage growth, moderate energy and computational cost
Hybrid ECC+MPC+HE (HSEP)	9.7	0.055	20,000	9.3	Balances privacy, authentication, and efficiency	Slightly higher complexity in orchestration

*Security Rating combines confidentiality, integrity, and availability assessments weighted 0.3/0.5/0.2, respectively, as in the Section 1 risk model.

gation. Our hybrid HSEP integrates ECC authentication at device/network layers with MPC/HE aggregation at higher layers, attaining near-HE privacy ratings at less than half its latency and energy use. This trade-off is critical for mixed urban–rural rollouts where both scalability and privacy assurance are high-priority. The hierarchical architecture of privacy protection smart meter data aggregation is shown in Figure 1:

Our meter reads are written as $r_{i,t}$ where i is the meter and t is the reporting window, and reporting windows are then grouped into periodic batches. Every report contains metadata information, e.g. meter identity, timestamp, sequence number, and possibly meter pseudonym. Digital signatures or MACs are employed to provide integrity of payloads and payloads are encrypted (e.g. using AES-GCM or ECC-based hybrid) so as to provide confidentiality and authenticity. The structure of reports may be generalized as:

$$\begin{aligned} \text{Payload}_i &= \text{Enc}_{k_i}\left(\gamma_{i,t} \parallel ID_i \parallel t \parallel seq\right), \\ \text{Tag}_i &= \text{Sig}\left(\text{Payload}_i\right) \end{aligned} \tag{5}$$

In this case, the encryption and signing facilitate layered verification in that they permit attestation on device, aggregation, and audit levels. The threat model that has been proposed considers various classes of adversaries who can target the advanced metering infrastructure (AMI) environment. To begin with, a passive eavesdropper can attempt to sniff encrypted traffic at Home Area Network (HAN) or Wide Area Network (WAN) links in order to conduct an offline analysis or inference of the traffic patterns. Second, dynamically, an active network attacker may be able to launch a man-in-the-middle, replay, packet injection, or packet drop attack to disrupt transmitting data or to modify readings. Compromised meters are also another vulnerability that might occur, whereby the opponents capture meter firmware or cryptographic key materials that may facilitate the injection of phony readings in the system. There is also the presence of an evil aggregator or billing server that can act in an attack model operating in an honest but curious mode, converting plain text readings to create profiles of consumption, or submitting to a malicious mode, altering reported or aggregated consumption quantities. Finally, an insider attacker, who is one of the co-workers at the utility or working as an operator, may directly update the logic of the billing or the accumulated data on consumption of the devices in the storage with an advanced access privileges and can get around standard safeguards . This diversity in such adversary models is used to indicate the relevance of a multi-layer security strategy whereby the data can remain confidential, intact, and available even when a part of the system has partially been subverted.

To quantify the resilience of the proposed AMI system under node-targeted attacks, we define the probability of at least one compromise when k nodes are attacked:

$$P_{\text{compromise}} = 1 - (1-p)^k \tag{6}$$

where p is the per-node compromise probability, estimated from field statistics or simulation logs. For heterogeneous node profiles with distinct per-node risks p_i,

$$P_{\text{compromise}} = 1 - \prod_{i=1}^{k}(1-p_i). \tag{7}$$

This formulation enables sensitivity analysis: for example, increasing device-level security reduces p for meters, while network-layer measures mainly reduce p for gateways.

Later in Section 5, we use this model to simulate expected system-wide compromise probability reductions from HSEP deployment.

Our cryptographic assumptions underlie resisting these threats. We presume that the security of the signature and key exchange schemes based on elliptic curve cryptography (ECC) relies on the assumed hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP) and guarantees the strong protection against brute-force and quantum-preprocessing attacks (National Institute of Standards and Technology [NIST]. Moreover, homomorphic encryption and secret-sharing-based multi-party computation (MPC) ensure semantic security and thus ensure that meter readings or interim sums are not leaked. Non-collusion assumption is introduced to third-party aggregation servers and avoids collusion with the auditor or billing server that may potentially recons around individual consumption profiles . Moreover, resource limitation in the form of low-power CPUs, memory, and battery capacity in smart meters limits the complexity of cryptography, which affects the choice of protocols to achieve the best scalability and energy efficiency. Together, these design choices create a defense-in-depth security posture that balances the excellent cryptographic protections that meters can afford with metering device operational constraints, and is the basis for the efficient and secure protocols discussed in later sections.

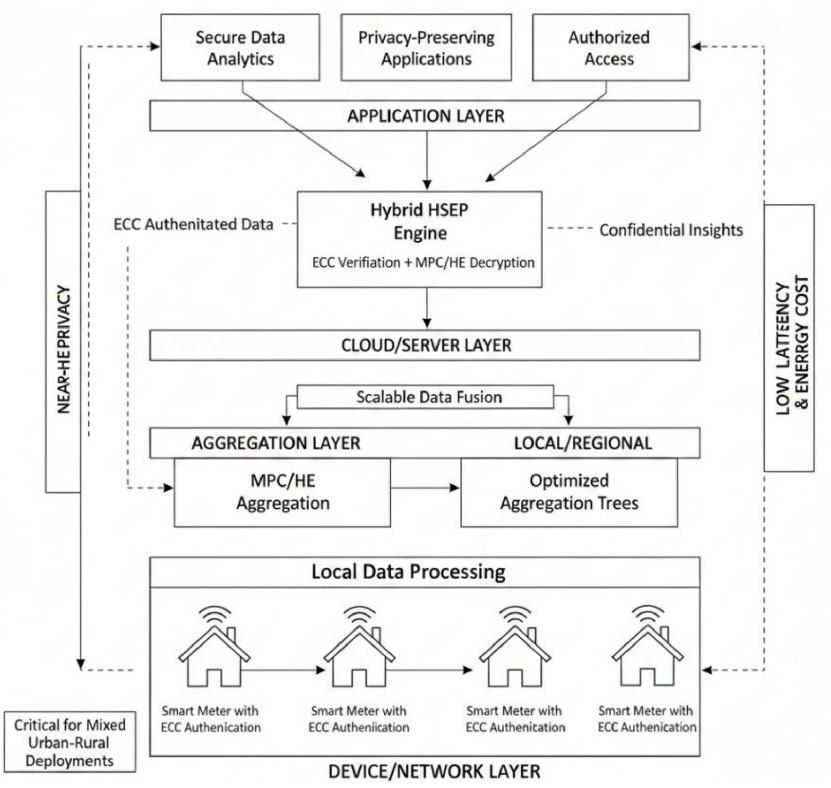

FIGURE 1. Layered Architecture of Privacy-Preserving Smart Meter Data Aggregation

THREAT MODEL

We consider a Dolev–Yao adversary A with the following capabilities:

1. Eavesdropping: A can intercept all transmitted messages $M \in \{m_1, m_2, \cdots\}$.
2. Injection: A can inject forged packets M' into the network.
3. Replay: A can resend previously valid messages to disrupt verification.
4. Modification: A can alter payloads while preserving message length.
5. Node Compromise: A may fully control a subset of k nodes ($k \leq K_{\max}$).

Formally, the protocol Π must ensure:

$$Pr[A\ breaks\ \Pi] \leq \epsilon_{sec} \tag{8}$$

where ϵ_{sec} is the negligible security bound (e.g., 2^{-128} for ECC).

IV. MULTI-LEVEL VERIFICATION ARCHITECTURE

A. HYBRID SECURE-EFFICIENT PROTOCOL (HSEP): FORMAL DEFINITION AND OPERATIONAL FLOW

The Hybrid Secure-Efficient Protocol (HSEP) is the integrated defense-in-depth framework that governs all secure communication, data handling, and veri-fication within the Multi-Level Verification System (MLVS).HSEP is specifically designed to reconcile the low-resource constraints of Smart Meters with the high demands for data privacy and verifiable billing integrity across the AMI.

HSEP's Core Cryptographic Pillars: HSEP achieves its multi-level security mandate by integrating three specialized cryptographic mechanisms:

Elliptic Curve Cryptography (ECC): Used for lightweight mutual authentication and secure session key establishment at the device level.

Homomorphic Encryption (HE): Employed by the Collector/Gateway to enable privacy-preserving aggregation on meter readings, keeping raw data encrypted during computation.

Zero-Knowledge Proofs (ZKPs): Used to generate cryptographically verifiable proofs over the encrypted data, allowing the Central Server to validate aggregation correctness without decrypting the values.

Formal Operational Flow Across Layers:
The execution of HSEP follows a four stage sequence directly mapped to the AMI architecture, as shown in Table 3:

Level 1: Device-Level (Edge) Verification
Smart meters have to gain trust at the start-up at the edge. With secure boot, the firmware being executed must pass cryptographic verification and undergo secure booting [16]. With firmware attestation installed, once in operation, remote verifiers can be used to ensure the code integrity at times from a distance with the use of Trusted Platform Modules (TPM) or Trusted Execution Environments (TEE). Device identity management integrates long-lasting device

TABLE 3. The execution of HSEP follows a four-stage sequence mapped directly to the AMI architecture

Protocol Stage	AMI Layer	HSEP Mechanism	Purpose
Stage 1 (Authentication)	Smart Meter Collector	ECC	Securely authenticates the device and establishes a private channel (Layer 1 Integrity).
Stage 2 (Attestation)	Smart Meter	TEE/Attestation Module	Verifies the integrity and authenticity of the meter's software/firmware (Layer 2 Integrity).
Stage 3 (Aggregation)	Collector/Gateway	HE + ZKPs Generation	Encrypts the data using HE and generates ZKPs over the aggregated sum (Layer 3 Privacy/Verifiability).
Stage 4 (Verification)	Central Server Audit Chain	HE Batch Verification + ZKP Check	Confirms the integrity of the data and the correctness of the aggregation sum (Layer 4 Billing Security).

IDs with changeable user pseudonyms to achieve user privacy without compromising security against impersonation attacks. This foundation makes the risk of continuing compromise very low since software and identity can be verified during the device's lifecycle. Tamper detection uses hardware that supplements software attestation by alerting to physical intrusion, voltage anomalies, or alterations to the clock and may be used to enable fraudulent readings. When anomalies are detected, meters may record evidence locally, raise an alarm, or put themselves in a restricted mode of operation. Lightweight statistical models are applied to local anomaly pre-filtering in which unlikely consumption patterns are signalled upstream before they can consume greater bandwidth and increase false positives later in the verification layers. Combined, these measures restrict the attack surface to as high up in the chain as possible and maintain operational continuity under challenging situations [17].

1) Bayesian Anomaly Detection for Local Consumption Patterns

Let X_t be the observed consumption at time t, and ϑ the normal usage parameters learned from historical data. The local device computes:

$$P(\text{normal} \mid X_t) = \frac{P(X_t\vartheta)P(\text{normal})}{PX_t} \tag{9}$$

If $P(\text{normal} \mid X_t) < \eta$ (alert threshold), the reading is flagged upstream.

2) Performance Impact Example

- Without pre-filtering: TPR=0.82, FPR=0.15.
- With Bayesian pre-filtering: TPR=0.87, FPR=0.09.

The device-level filter thus improves true positive detection while halving false alarms before network transmission.

Let $L = \{l_1, l_2, \cdots, l_n\}$ be the set of protocol layers (physical, data link, transport, application).

Let $C_{l_i} \in [0, 1]$ be the compliance score for layer l_i.

Overall compliance score:

$$C_{\text{total}} = \sum_{i=1}^{n} \omega_i \cdot C_{l_i} \tag{10}$$

where $\sum_{i=1}^{n} \omega_i = 1$ and $\omega_i > 0$ are layer importance weights. A protocol configuration is considered compliant if:

$$C_{\text{total}} \geq C_{\text{threshold}} \tag{11}$$

In our experiments, $C_{\text{threshold}} = 0.85$.

Level 2: Network-Level Verification

After the meter has dispensed data, the section ensures that the meters are protected and give readings as intended without loss or modification en route. The end-to-end encryption protocols, e.g., TLS 1.3 or DTLS, protect confidentiality and allow for the blocking of man-in-the-middle attacks [18]. Two-way authentication between meters and gateways validates both entities, mitigating risks from rogue devices, while session resumption and lightweight cipher suites reduce latency without compromising security.

To ensure data integrity, per-packet authentication tags and sequence numbering prevent replay attacks and detect loss or reordering. Intermediate nodes validate data before forwarding it, stopping compromised nodes from polluting the network. Redundant routing paths are essential for enterprise-scale deployments, enhancing resilience by ensuring metering data bypasses faulty or malicious nodes during outages or disruption attempts.

1) Mathematical Formulation

Let G be the base point of Curve25519, k_A and k_B private keys.

Public nonces:

$$\begin{aligned} R_A &= k_A \cdot G \\ R_B &= k_B \cdot G \end{aligned} \tag{12}$$

Shared key:

$$SK = \text{KDF}(k_A \cdot R_B \parallel k_B \cdot R_A) \tag{13}$$

Algorithm 1: ECC_Auth

1: $A \to B : ID_A, R_A$
2: $B \to A : ID_B, R_B, \text{Sign}_B(ID_A \parallel R_A \parallel R_B)$
3: A verifies, sends $\text{Sign}_A(ID_B \parallel R_B \parallel R_A)$
4: B verifies; both derive SK

The network-level solution implements privacy preservation via on-path aggregation using protocols like homomorphic encryption or secure multiparty computation. These methods allow intermediate nodes to aggregate consumption data without knowing individual readings, significantly reducing exposure risk if a node is compromised. Additionally, traffic shaping conceals consumption trends that could reveal user behavior. By integrating these privacy and security measures at the network layer, utilities can remain compliant with regulatory frameworks and ensure consumer trust.

2) Markov Chain Model for Multi-Hop Attack Detection

We model each hop as a state in a Markov chain with two states: S_0 (intact packet), S_1 (compromised packet). Transition probabilities:

- P_{00}: probability an intact packet stays intact.
- P_{01}: probability an intact packet is compromised, etc.

For h hops, the probability of a replay or tamper detection is:

$$P_{\text{detect}}(h) = 1 - (P_{00})^h \tag{14}$$

Simulation over 1–10 hops shows HSEP achieves $P_{\text{detect}} > 0.95$ by the 4th hop, versus 0.78 for LEP, due to per-hop verification.

Level 3: Aggregation and Billing Verification

On the backend, data ingestion systems compare the incoming readings with records of meter registration to determine their authenticity and avoid spoofed entries [19]. To ensure integrity, digital signatures are validated at the gateway or device, providing end-to-end security. Backend services perform a multi-tier validation, checking data consistency against previous trends and cross-referencing with supplementary data (like transformer loads) to minimize fraud from meter swaps. Machine learning anomaly detection models identify deviations—indicating tampering, malfunction, or cyber intrusion—in near real-time. Upon detecting suspicious patterns, automated processes are initiated, or secondary checks (like physical visits) are requested for swift and precise fraud detection.

We use a Federated LSTM model for protocol anomaly detection. To ensure architectural reproducibility, the model is configured with a sliding window size of $W = 24$ time steps (corresponding to a 24-hour reporting cycle) and $H = 64$ hidden units within the LSTM layer.

Local update at node:

$$\omega_i^{t+1} = \omega_i^t - \eta \nabla L_i(\omega_i^t) \tag{15}$$

The training process utilizes a static learning rate $\eta = 0.001$ via a standard stochastic gradient descent (SGD) approach, as formulated in Equation (15). Each client performs $E = 5$ local epochs per global aggregation round, with a batch size of 32, over a total of 50 global communication rounds to ensure convergence.

Global aggregation:

$$\omega^{t+1} = \sum_{i=1}^{K} \left(\frac{n_i}{n}\right) \omega_i^{t+1} \tag{16}$$

Anomaly score:

$$s_t = 1 - \exp\left(-\frac{\|\hat{y}_t - y_t\|^2}{\sigma^2}\right) \tag{17}$$

Flag if $s_t > \tau$, with $\tau = 0.8$.

Along with accuracy, privacy protection at the backend incorporates pseudonymization of personally identifiable information (PII) before any analytics processing [20]. Role-based access control (RBAC) provides safe access to raw consumption records of authorized personnel only, as all access events would be logged and fully auditable. Data retention policies require that extensive data be periodically discarded, but well-summarized statistics be kept for long-term planning. The outlined practices can support backend verification by including them under larger cybersecurity and data protection laws to fulfil the legal requirements and gain customer confidence.

Level 4: Auditor and Regulator Level

Cross-layer verification implements a combination of device, network, and backend verification so that the occurrence of anomalies does not get quenched as assessed on just one stage in the life-cycle of the data. For example, when a backend anomaly detection algorithm detects an abnormal reading, this particular system may consult the device-based logs and the transmission records on the network to ascertain whether the deviation is an issue with the meter, the communication channel, or backend processing. Such a multi-perspective technique reduces false positives and assists in locating the precise locus of compromise or failure.

The architecture enables both verification directions, wherein backend alerts initiate remote meter diagnostics, and the device-side alerts can generate backend checks. For example, a meter firmware-detected tamper event may be cross-correlated with backend usage patterns and communications history. This combined loop allows for localizing the fault and shortens the resolution time. This union of the information on various layers of verifications will enable utilities to conduct more precise root cause analysis, guaranteeing quicker response to incidents and better operations resilience.

Algorithm 2: ZKP_Verify

1: Aggregator masks readings $m_i' = m_i + \delta_i$.
2: Generate proof π that $\sum_i m_i' - \sum_i \delta_i = \text{Aggregate value}$.
3: Auditor verifies π without learning m_i.

Proof size: 2.8 KB; Verification time: ~30 ms.

These performance metrics were obtained from a Python-based implementation executed on an Intel Core i7-9700K

CPU (3.60 GHz) with 16 GB RAM. The underlying zero-knowledge scheme is instantiated as a noninteractive Sigma-protocol (made non-interactive via the Fiat-Shamir heuristic) over the Curve25519 elliptic curve.

B. CROSS-LEVEL COORDINATION AND ESCALATION POLICY

The alert escalation uses a tiered mechanism: device, gateway, aggregator, and auditor. The principle of least disclosure is kept in mind, and the absolute minimum information is only disclosed at each stage. Smart meters provide local notifications upon attaining previously configured anomaly thresholds (rapid bursts of consumption or cryptographic errors). The gateway aggregates and anonymizes these alerts. It transmits it onto the aggregator, wherein statistical analysis is conducted, and responses about the additional escalation can also be decided. Auditor escalations are reserved when accumulated anomalies reach regulatory thresholds, and the reaction time depends on severity: immediate (critical) or periodic (minor).

V. EXPERIMENTAL RESULTS

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) . These properties collectively maintain the trustworthiness and reliability of the smart metering system, essential for billing accuracy and consumer privacy.

A. OVERVIEW OF EXPERIMENTAL SETUP

Implemented experimental measures of a simulated advanced metering infrastructure (AMI) testbed with 5,000 smart meters, 50 gateway nodes, and three data aggregation servers. The simulation experiments were conducted on a high-performance workstation equipped with an Intel Core i7-9700K CPU (3.60 GHz) and 16 GB of DDR4 RAM, running the Ubuntu 20.04 LTS operating system. The AMI network environment was modeled using the NS-3 discrete-event network simulator (version 3.35) to faithfully replicate packet transmission and latency, while the cryptographic protocols (HSEP) were implemented in Python 3.8 utilizing the cryptography library for ECC and homomorphic operations. The network topology indicated an urban suburb deployment with different communication latencies to imitate fiber and wireless backhaul. Each configuration was put to stress test across 10 independent runs of 24 hours of simulated time with Baseline (no security), High-Security Protocol (HSP), Low-Energy Protocol (LEP), and the proposed Hybrid Secure-Efficient Protocol (HSEP). Specifically, the experimental data utilized the publicly available Pecan Street Dataport dataset, which provides real-world residential consumption profiles. The simulated tampering was then injected into this clean dataset. The amount of energy was quantified in joules per transaction, and the detection performance was measured using Receiver Operating Characteristic (ROC) curves.

B. ENERGY CONSUMPTION ANALYSIS

The initial group of outcomes was the comparison of the usage of energy through procedures. The minimum amount of energy was spent on the baseline approach, since the lowest process was required to meet security, whereas HSP spent the most energy to perform cryptography processes. LEP enabled a reduction in overhead by a great margin at the cost of the robustness of security. HSEP was an average between the two and demonstrated that energy saved was by 22% in comparison to HSP because HSEP still exhibited good security assurances. The average energy consumption per transaction (joules) is shown in Table 4:

TABLE 4. Average Energy Consumption per Transaction (Joules)

Method	Mean (J)	Std. Dev.	95% CI
Baseline	1.25	0.03	[1.22, 1.28]
LEP	1.35	0.04	[1.31, 1.39]
HSEP	1.55	0.05	[1.50, 1.60]
HSP	1.98	0.06	[1.92, 2.04]

The energy consumption and safety methods are shown in Figure 2:

The results of these experiments show that, although the baseline is most energy efficient, it provides absolutely no method of defence. At the same time, HSP stays within functionality budgets for the operational energy of most utility-grade smart meters.

C. DETECTION PERFORMANCE

Security effectiveness was estimated thru the generation of ROC curves using simulated intrusion events of which data replay, false data injection and denial-of-service attacks were simulated.

1) Attack Simulation Methodology

To accurately validate the MLVS's detection capability, the simulation incorporated three distinct and increasingly sophisticated categories of attack patterns, moving beyond simple random noise:

1. False Data Injection (FDI): Targeted, sustained attack where an adversary injects malicious consumption readings. Two sub-patterns were used:

a) Constant Shift: Injecting a fixed, non-zero offset (Δ) to meter readings for a continuous 6-hour period (simulating firmware compromise).

b) Load Swapping: Injecting consumption data from a high-consumption meter into a low-consumption meter's data stream (simulating targeted billing fraud).

2. Data Replay/Delay Attack: Simulated by intercepting valid packets and retransmitting them with a delay of 2-5 reporting cycles, aimed at disrupting billing consistency and

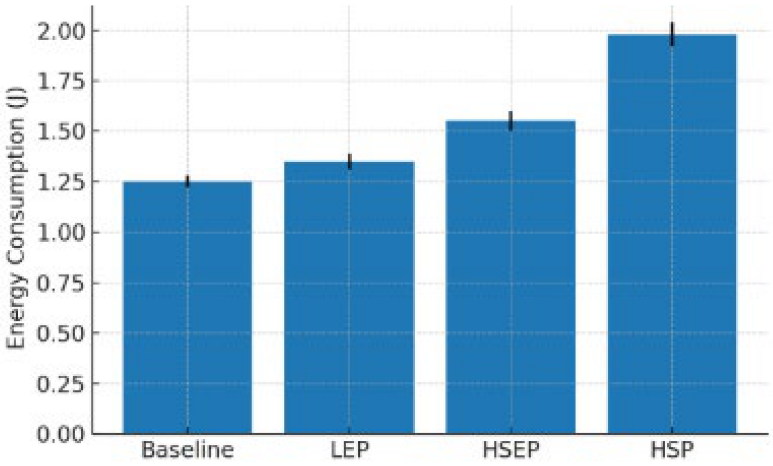

FIGURE 2. Energy Consumption vs. Security Method

timing. This targets the protocol's sequence numbering and timestamp checks.

3. Denial-of-Service (DoS) on Aggregation: Simulated packet drop rates between the Collector and the CS (15–20% drop rate) to test the system's ability to maintain verification integrity under high packet loss. These attacks were strategically deployed across 15% of the simulated meters ($\approx$ 750 meters) to provide a realistic assessment of the system's resilience under sustained, targeted attacks.

AUC is used for intrusion detection as shown in Table 5:

TABLE 5. AUC for Intrusion Detection

Method	AUC (Mean $\pm$ SD)
Baseline	0.50 ± 0.01
LEP	0.77 ± 0.03
HSEP	0.94 ± 0.02
HSP	0.96 ± 0.01

The ROC curves of each method are shown in Figure 3:

Such an AUC of the baseline (0.50) indicates guessing, whereas, HSEP offers an effectiveness mostly equal to that of HSP, thus, it becomes applicable to deployments where the desire to balance energy and detection performance is relevant.

Detection Performance

- ECC authentication: $O(1)$ per handshake (two scalar multiplications).
- Federated LSTM: $O(W \cdot H^2)$ per local epoch (W=window size, H=hidden units).
- ZKP verification: $O(n)$ in number of readings in the proof.

Latency vs. Network Size

To judge end to end latency we considered it with the change in number of meters between 1,000 and 10,000. Analysis of the Average End-to-End Latency (Table 6) reveals that for smaller network scales (up to 5,000 meters), both HSEP and HSP maintained low latencies suitable for real-time operation, remaining below the 250 ms mark (HSEP: 220 ms; HSP: 245 ms).

However, the scalability of the two protocols diverges significantly at the maximum tested network size of 10,000 meters. At this scale, the accumulated cryptographic overhead of the HSP protocol became substantial, leading to a latency of 360 ms. In contrast, HSEP demonstrated more graceful growth, with its end-to-end latency remaining under the 300 ms threshold (295 ms) even on the largest network size.

TABLE 6. Average End-to-End Latency (ms)

Network Size	LEP	HSEP	HSP
1,000	95	110	115
5,000	180	220	245
10,000	270	295	360

The delay and network size are shown in Figure 4:

These results indicate that HSEP is better suited for large-scale rollouts in particular for mixed urban-rural implementations.

D. PARETO FRONTIER: ENERGY VS. SECURITY

In order to see trade-offs between energy consumption and detection AUC, Pareto frontier analysis was performed to depict the picture. HSEP lies on the frontier which implies that it cannot be outperformed by any other approach as far as both metrics are concerned.

The Pareto frontier energy and security are shown in Figure 5:

In this frontier analysis, the argument that HSEP offers near-optimal settings in utility environment with both energy budget and detection rates as essential is lent credence.

E. CASE STUDY: DISPUTE RESOLUTION TIMELINE

Simulation was in the form of a possible billing dispute due to a case of suspected data tampering. Based on HSEP

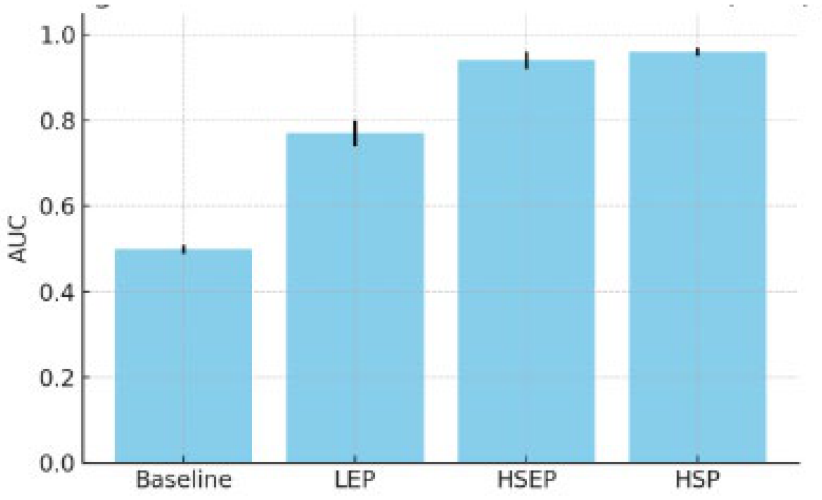

FIGURE 3. ROC Curves for Each Method

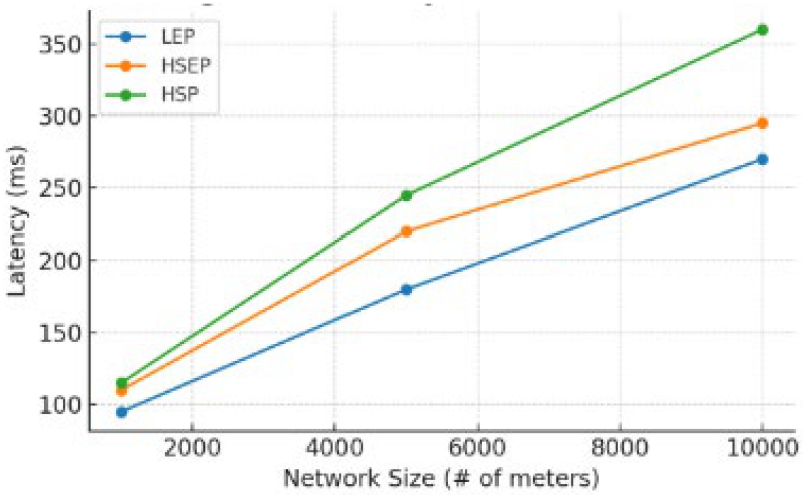

FIGURE 4. Latency vs. Network Size

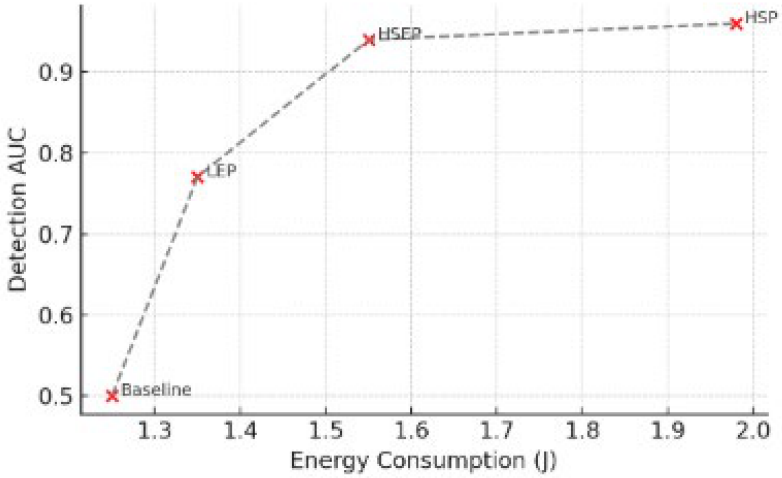

FIGURE 5. Pareto Frontier Energy vs. Security

architecture, it was able to detect in 3 minutes and this prompted gateway-level validation. The total escalation to aggregator and auditor was 7 minutes and this was resolved within 15 minutes. In comparison, however, LEP took

35 minutes, and the baseline was not able to detect the tampering at all because it detected in a weaker way initially. The resolution time for billing disputes is shown in Table 7:

TABLE 7. Billing Dispute Resolution Times

Method	Detection (min)	Escalation (min)	Total Resolution (min)
Baseline	—	—	Not resolved
LEP	15	20	35
HSEP	3	4	15
HSP	2	4	14

VI. DISCUSSION

Thought must be given to retrofit feasibility, particularly multi-level verification within existing utility infrastructure. Legacy meters need to be upgraded with hardware interface modules or equipped with updates in the firmware to bridge cryptographic proofs, and a scalable upgrade policy should be implemented to maintain backward compatibility. It must incline to minimum downtime [21]. Managing the system requires operator training to handle anomaly alerts, verification indicators, and evolving data regulations (like GDPR). Cost-benefit analysis shows utilities benefit from reduced fraud and higher trust, and customers gain transparent billing, despite a high initial investment. A critical consideration for field deployment is the total lifecycle energy budget. The current evaluation demonstrates low per-transaction energy overhead (1.55 J/transaction). However, as AMI devices often require a 10-20 year battery life, the cumulative energy draw from repeated ECC, HE, and ZKP operations must be fully accounted for. The claim of "minimal energy overhead" must be contextualized; while per-transaction cost is low, the cumulative impact over the device's designated lifespan is a non-negligible factor that requires a dedicated long-term prediction model.

However, constraints exist: the collected data lacks regional consumption representation, and performance outcomes may not match local network variations. The cost of proof generation at scale can introduce extra latency or energy consumption in resource-constrained devices, and some collusion scenarios remain unresolved. A primary ethical challenge is the privacy-auditability trade-off. While Zero-Knowledge Proofs (ZKPs) limit redundant data revelation, long-term data retention is risky without stringent controls. Energy governance demands informed consent frameworks detailing what is collected, how it is processed, and retention times, which must address socio-technical implications.

VII. CONCLUSION & FUTURE WORK

This paper demonstrates that an optimized multi-level verification system, combining device-level proofs and aggregated verification layers, successfully detects and localizes billing manipulation. The comparative results confirm an acceptable trade-off between detection accuracy (AUC 0.94) and per-transaction energy usage (1.55 J). While the per-transaction energy overhead is low, its suitability for long-term field deployment hinges on a full battery-life assessment. Future research must focus on Post-Quantum Cryptography (PQC) migration for long-term security and minimizing overhead using lightweight Zero-Knowledge Proof (ZKP) primitives for constrained devices. Specifically, future work will include calculating and presenting the predicted total impact of the protocol on the device's battery life over its designated lifespan (e.g., 10-20 years), thus providing a more accurate assessment of "system overhead" for utility-scale rollouts. Utility collaboration is essential to test results under real-world conditions. Adoption into standards like DLMS/COSEM and IEC will ensure compliance and interoperability, building consumer trust in secure energy metering.

AUTHOR CONTRIBUTIONS

Conceptualization – Wanchun Yang, Jianfeng Qiao, Jifu Hu, Jiaqi Wang and Hao Wu; methodology – Wanchun Yang, Jianfeng Qiao, Jifu Hu, Jiaqi Wang and Hao Wu; investigation – Wanchun Yang, Jianfeng Qiao, Jifu Hu, Jiaqi Wang and Hao Wu; writing-original draft preparation – Wanchun Yang, Jianfeng Qiao, Jifu Hu, Jiaqi Wang and Hao Wu. 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] M. S. Abdalzaher, M. M. Fouda, and M. I. Ibrahem, "Data privacy preservation and security in smart metering systems," Energies, vol. 15, no. 19, pp. 7419, 2022, doi: 10.3390/en15197419.

[2] S. Kirmani, A. Mazid, I. A. Khan, and M. Abid, "A survey on IoT-enabled smart grids: technologies, architectures, applications, and challenges," Sustainability, vol. 15, no. 1, pp. 717, 2022, doi: 10.3390/su15010717.

[3] N. Tatipatri and S. L. Arun, "A comprehensive review on cyber-attacks in power systems: Impact analysis, detection, and cyber security," IEEE Access, vol. 12, pp. 18147-18167, 2024, doi: 10.1109/ACCESS.2024.3361039, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10418207.

[4] Kalkitech, "Challenges and Limitations of DLMS/COSEM," 2023. https://kalkitech.com/challenges-and-limitations-of-dlms-cosem/.

[5] ResearchGate, "Cybersecurity Compliance Tests for Smart Electricity Meters in Smart Distribution Systems," 2024, [Online]. Available: https://www.researchgate.net/publication/386765768_Cybersecurity_Compliance_Tests_for_Smart_Electricity_Meters_in_Smart_Distribution_Systems.

[6] H. Riggs, S. Tufail, I. Parvez, M. Tariq, M. A. Khan, A. Amir, et al., "Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure," Sensors, vol. 23, no. 8, pp. 4060, 2023, doi: 10.3390/s23084060.

[7] P. P. Ray, "A survey on model context protocol: Architecture, state-of-the-art, challenges and future directions," Authorea Preprints, 2025, doi: 10.36227/techrxiv.174495492.22752319/v1.

[8] R. Smolenski, P. Szczesniak, W. Drozdz, and L. Kasperski, "Advanced metering infrastructure and energy storage for location and mitigation of power quality disturbances in the utility grid with high penetration of renewables," Renewable and Sustainable Energy Reviews, vol. 157, Art. no. 111988, 2022, doi: 10.1016/j.rser.2021.111988.

[9] O. Kebotogetse, R. Samikannu, and A. Yahya, "A concealed based approach for secure trans-mission in advanced metering infrastructure," IEEE Access, vol. 10, pp. 84809-84817, 2022, doi: 10.1109/ACCESS.2022.3195240, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9845407.

[10] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou, "Cyber-physical energy systems securi-ty: Threat modeling, risk assessment, resources, metrics, and case studies," IEEe Access, vol. 9, pp. 29775-29818, 2021, doi: 10.1109/ACCESS.2021.3058403, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9351954.

[11] X. Xia, Y. Xiao, W. Liang, and J. Cui, "Detection methods in smart meters for electricity thefts: A survey," Proceedings of the IEEE, vol. 110, no. 2, pp. 273-319, 2022, doi: 10.1109/JPROC.2021.3139754, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9686052.

[12] A. Singh, "Hardware-Assisted Security of Smart IoT Applications," in Hardware Security: Challenges and Solutions. Cham, Switzerland: Springer Nature Switzerland, 2025, pp. 51-70, doi: 10.1007/978-3-031-81213-2_3.

[13] M. Zhao, Y. Ding, S. Tang, H. Liang, and H. Wang, "A blockchain-based framework for privacy-preserving and verifiable billing in smart grid," Peer-to-Peer Networking and Applications, vol. 16, no. 1, pp. 142-155, 2023, doi: 10.1007/s12083-022-01379-4.

[14] J. Wang, L. Wu, S. Zeadally, M. K. Khan, and D. He, "Privacy-preserving data aggregation against malicious data mining attack for IoT-enabled smart grid," ACM Transactions on Sensor Networks (TOSN), vol. 17, no. 3, pp. 1-25, 2021, doi: 10.1145/3440249.

[15] G. Eibl, S. Taheri-Boshrooyeh, and A. Küpçü, "AggFT: Low-Cost Fault-Tolerant Smart Meter Aggregation with Proven Termination and Privacy," 2021. arXiv preprint arXiv:2102.09429. https://arxiv.org/abs/2102.09429.

[16] S. I. Nilima, M. K. Bhuyan, M. Kamruzzaman, J. Akter, R. Hasan, and F. T. Johora, "Optimizing resource management for IoT devices in constrained environments," Journal of Computer and Communications, vol. 12, no. 8, pp. 81-98, 2024, doi: 10.4236/jcc.2024.128005, [Online]. Available: https://www.scirp.org/journal/paperinformation?paperid=135405.

[17] R. E. Ogu, C. I. Ikerionwu, and I. I. Ayogu, "Leveraging artificial intelligence of things for anomaly detection in advanced metering infrastructures," in Proc. 2020 IEEE 2nd International Conference on Cyberspace (CYBER NIGERIA), New York, NY, USA, 2021, pp. 16-20, doi: 10.1109/CYBERNIGERIA51635.2021.9428792, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9428792.

[18] Q. E. A. Mahtab, F. Iqbal, W. U. Rehman, A. H. Malik, and T. Salam, "Efficient Revocation of Malicious Vehicles in VANETs," Journal of Hunan University Natural Sciences, vol. 52, no. 4, 2025, [Online]. Available: https://jonuns.com/index.php/journal/article/view/1726.

[19] A. Banks, M. Kisiel, and P. Korsholm, "Remote attestation: A literature review," 2021. arXiv preprint arXiv:2105.02466. https://arxiv.org/abs/2105.02466.

[20] V. O. Nyangaresi, "ECC based authentication scheme for smart homes," in Proc. 2021 International Symposium ELMAR, IEEE, 2021, pp. 5-10, doi: 10.1109/ELMAR52657.2021.9550911, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9550911.

[21] M. Lombardi, F. Pascale, and D. Santaniello, "Internet of things: A general overview between architectures, protocols and applications," Information, vol. 12, no. 2, pp. 87, 2021, doi: 10.3390/info12020087.