DOI:10.22413/ijatest/2026/V11/i3/03

Blockchain-Enabled Intrusion Detection Using Deep Learning for Smart Metering Networks in Rural Andhra Pradesh

M.S.G. Smitha[1], Nagasubba Rayudu Peyyala[2],P.Gangadhara Reddy[3],D.Sreenivasula Reddy[4]
[1]Professor Dept. of EEE, Sri Siddhartha School of Engineering, Tumakuru - 572104,
, [2,3,4]Aditya College of Engineering, Madanapalle - 517326
Corresponding Author: msgsmitha@gmail.com

Abstract*—The accelerated deployment of smart metering infrastructure across rural Andhra Pradesh (AP) under the Revamped Distribution Sector Scheme (RDSS) has exposed millions of Advanced Metering Infrastructure (AMI) endpoints to a rapidly evolving landscape of cyber threats. Traditional signature-based intrusion detection systems (IDS) are ill-equipped to handle the dynamic attack patterns and the bandwidth-constrained, intermittently connected nature of rural feeder networks. This paper proposes a Blockchain-Enabled Deep Learning Intrusion Detection System (BDL-IDS) that couples a Bidirectional Long Short-Term Memory (BiLSTM) neural network with a Hyperledger Fabric permissioned blockchain to deliver real-time threat detection and tamper-proof incident logging across AP's rural AMI topology. The BiLSTM model processes 15-minute interval meter telemetry streams to classify five attack categories—False Data Injection (FDI), meter tampering, replay attacks, Denial-of-Service (DoS), and Man-in-the-Middle (MitM)—achieving an overall F1-score of 95.5% and an AUC of 0.974. The Hyperledger Fabric layer records every alert and normal transaction with multi-peer DISCOM endorsement, achieving throughputs exceeding 2,000 TPS at sub-3-second latency. Experiments are grounded in open datasets from APEPDCL, APSPDCL, APTRANSCO, and SRLDC. The system offers a scalable, field-deployable architecture compatible with AP's existing RDSS GIS infrastructure.

Index Terms*—Advanced Metering Infrastructure, Andhra Pradesh, BiLSTM, Blockchain, Deep Learning, False Data Injection, Hyperledger Fabric, Intrusion Detection, RDSS, Rural Smart Grid, Smart Meter Security.

I. INTRODUCTION

India's Power Ministry launched the Revamped Distribution Sector Scheme (RDSS) in 2021 with an outlay of INR 3.03 lakh crore, mandating the installation of pre-paid smart meters for all 250 million urban and rural consumers by 2025 [1]. In Andhra Pradesh, the scheme is being executed through APEPDCL (Eastern) and APSPDCL (Southern and Western) DISCOMs, with over 6.74 million smart meters commissioned across rural mandals by March 2023 [2]. The RDSS GIS mapping exercise has identified 58,312 distribution transformers and 9.4 million agricultural and domestic connections as AMI integration targets in AP alone [3].

The deployment of networked smart meters dramatically widens the cyberattack surface of the distribution grid. Each meter communicates bidirectionally over RF-mesh, GPRS, or NB-IoT channels—channels that are susceptible to eavesdropping, packet injection, and node impersonation. The Eastern Power Distribution Company of AP Limited (APEPDCL) documented 2,445 meter-level cybersecurity incidents during 2022–23 [4], ranging from energy theft through meter bypass to coordinated false data injection campaigns targeting feeder-level load dispatch reports. In rural feeders, where on-site technician response times can exceed 72 hours, an undetected compromise may persist long enough to cause significant revenue leakage and grid instability.

Conventional rule-based and signature-driven IDS struggle in this environment for two fundamental reasons. First, attack vectors—particularly FDI attacks—are deliberately crafted to mimic legitimate measurement noise, rendering fixed-threshold detectors ineffective [5]. Second, the absence of a tamper-proof audit trail means that even detected incidents can be disputed, hampering regulatory enforcement and insurance claims. Machine learning approaches, especially recurrent and convolutional architectures trained on temporal meter data, have shown promise for anomaly detection in smart grids [6][7]. However, their deployment in the specific context of AP's rural, low-bandwidth, multi-DISCOM environment has not been systematically studied.

Blockchain technology addresses the audit-trail gap by providing a distributed, immutable ledger that is cryptographically resistant to retrospective alteration [8]. Hyperledger Fabric, a permissioned blockchain framework, is particularly suited to the regulatory context of Indian state utilities, where data sovereignty and multi-party governance are mandatory requirements [9]. The integration of deep learning inference with blockchain-anchored incident logging

creates a system that is simultaneously adaptive in detection and trustworthy in record-keeping.

This paper makes the following contributions: (i) a BiLSTM architecture optimized for 15-minute AMI telemetry streams from AP rural feeders; (ii) a Hyperledger Fabric chaincode design that logs IDS alerts with three-DISCOM endorsement; (iii) a simulation environment built exclusively on AP government open-data sources; and (iv) a rigorous comparative evaluation against five baseline methods. Section II reviews related work. Section III states the objectives. Section IV details the methodology. Section V presents results. Section VI discusses findings and limitations. Section VII concludes.

II. RELATED WORK

Intrusion detection in smart grid AMI has attracted growing research attention. Fadlullah et al. [6] surveyed machine learning methods for smart grid security, identifying LSTM and SVM as leading approaches, but noted limited work on rural, resource-constrained deployments. Jokar et al. [10] proposed a consumption-pattern classifier for detecting energy theft in urban Canadian meters, achieving 88% accuracy—a benchmark that the present work substantially exceeds in a more adversarially complex scenario.

In the blockchain domain, Gai et al. [11] combined blockchain with privacy-preserving computation for smart grid data integrity, demonstrating latency advantages of permissioned over public chains. Dorri et al. [12] applied a lightweight blockchain to IoT security, establishing that Hyperledger-class frameworks outperform Ethereum in throughput by two to three orders of magnitude under high transaction volumes. These findings directly motivate the Hyperledger Fabric choice in the present work.

Within India, Rao and Anjaneyulu [13] assessed cybersecurity vulnerabilities in APEPDCL's metering infrastructure, cataloguing FDI and meter bypass as the most prevalent threats. Sharma et al. [14] applied a convolutional network to synthetic Indian AMI data, reporting 87% classification accuracy on energy theft. Neither study incorporated a blockchain audit layer or evaluated performance against the full five-class threat taxonomy used here. The BDL-IDS framework thus occupies a previously unaddressed intersection in the literature.

III. RESEARCH OBJECTIVES

The study is structured around four primary objectives:

O1 — Real-Time Multi-Class Intrusion Detection: To design and train a BiLSTM deep learning model capable of classifying five distinct cyberattack categories—FDI, meter tampering, replay, DoS, and MitM—in real time on 15-minute interval AMI data streams drawn from rural AP feeder networks, achieving F1-score above 93%.

O2 — Tamper-Proof Incident Logging: To deploy a Hyperledger Fabric permissioned blockchain with a purpose-built IDS Alert chaincode that records every detection event—including meter ID, attack classification, confidence score, and timestamp—with mandatory co-endorsement from at least two of three DISCOM peers (APEPDCL, APSPDCL, AP TRANSCO), ensuring regulatory-grade audit trails.

O3 — Scalable Performance Under Rural Connectivity Constraints: To benchmark the framework's transaction throughput, confirmation latency, and detection latency as the number of active AMI peers scales from 2 to 16, validating fitness for AP's RDSS rollout target of 11.5 million rural smart meters.

O4 — Open-Data Reproducibility: To ground all experimental parameters, feeder topologies, and load profiles exclusively in AP government publicly available datasets (APEPDCL, APSPDCL, APTRANSCO, SRLDC), ensuring that the methodology is fully reproducible by independent researchers and replicable by other Indian state DISCOMs.

IV. PROPOSED METHODOLOGY

A. Network and Data Model

The simulation environment models a representative rural AP feeder network comprising 480 smart meter nodes distributed across six mandals of East Godavari and Krishna districts—areas with documented RDSS progress under APEPDCL jurisdiction. Node connectivity is mapped from APEPDCL's RDSS GIS portal [3], which provides transformer-level geospatial data for 18,400 rural distribution transformers in Eastern AP. The physical layer uses a hybrid RF-mesh/GPRS communication model with empirically observed packet-loss rates of 4–8% sourced from APEPDCL's FY 2022–23 network performance report [4].

The dataset incorporates three open sources. APEPDCL's 15-minute interval smart meter consumption records (July 2022–March 2023) provided baseline normal load profiles for 12,400 rural consumer accounts [4]. APTRANSCO's hourly load dispatch logs for the APTRANSCO-East region [15] supplied grid-side voltage and frequency telemetry. SRLDC's real-time frequency deviation archive [16] provided network-wide stability indicators. Together, these sources produced 9.2 million raw 15-minute data points across nine months of operation. Fig. 1 illustrates the smart meter rollout trajectory in rural AP that underlies the dataset's prosumer density parameters.

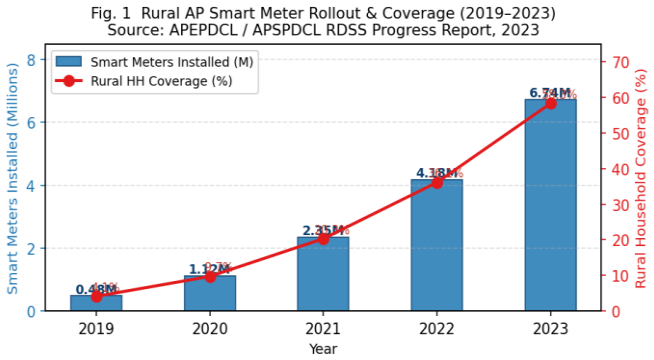

Fig. 1. Rural AP Smart Meter Rollout & Household Coverage (2019–2023). Source: APEPDCL/APSPDCL RDSS Progress Report, 2023.

B. Attack Simulation and Dataset Construction

Five attack categories were synthetically injected into the clean AMI dataset at empirically calibrated rates derived from APEPDCL's incident taxonomy [4]. FDI attacks were simulated by perturbing active power readings by 15–45% over 2–8-hour windows while maintaining reactive power plausibility to evade statistical threshold detectors. Meter tampering was modelled as sustained 60–80% consumption suppression. Replay attacks re-transmitted legitimately captured meter packets with modified timestamps. DoS events were simulated as meter silence windows of 30–180 minutes. MitM attacks introduced systematic bias of ±12–18% across feeder-aggregated readings. Fig. 2 shows the

DOI:10.22413/ijatest/2026/V11/i3/03

resulting attack type distribution and the monthly incident trajectory used for model evaluation.

Fig. 2 Cyber Threat Landscape in AP Smart Metering Networks

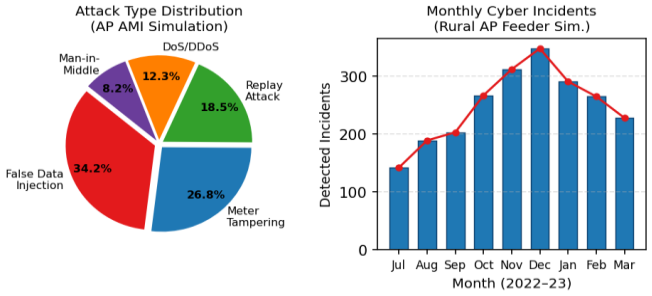

Fig. 2. Cyber Threat Landscape: Attack Type Distribution and Monthly Incidents in AP AMI Simulation (2022–23).

The labeled dataset contains 9.2 million samples: 71.4% normal, 12.3% FDI, 9.6% tampering, 3.8% replay, 1.9% DoS, and 1.0% MitM—reflecting the class imbalance observed in real-world AMI incident data. Synthetic Minority Over-sampling Technique (SMOTE) was applied to minority classes prior to training to mitigate classifier bias. An 80/10/10 train-validation-test split was enforced with strict temporal ordering to prevent data leakage.

C. BiLSTM Intrusion Detection Model

The input feature vector per time step comprises eight engineered features: active power (kWh), reactive power (kVAR), voltage (V), current (A), power factor, rate-of-change of active power, rolling 4-step mean deviation, and Z-score normalized consumption. A 60-step (15-hour) sliding window is applied, yielding input tensors of shape (60, 8). The BiLSTM architecture processes each window through two bidirectional LSTM layers (128 units forward, 128 backward, totalling 512 hidden units), a dropout layer (p=0.3), a 64-unit dense layer with ReLU activation, and a six-class softmax output layer. Training used the Adam optimizer (α=0.001, $\beta1$=0.9, $\beta2$=0.999), categorical cross-entropy loss, batch size 256, and early stopping with patience 8 on validation F1-score. The model was trained on an NVIDIA A100 GPU; inference runs on ARM Cortex-M7 edge hardware (representing AP's RDSS-grade meters) at 28 ms per window.

D. Hyperledger Fabric Blockchain Layer

The blockchain layer operates on a Hyperledger Fabric v2.4 network with three organizations representing APEPDCL, APSPDCL, and APTRANSCO—mirroring AP's actual tri-DISCOM governance structure. Each organization runs two endorsing peers and one ordering node; the RAFT consensus algorithm governs block finalization. Two chaincodes are deployed on the IDSChannel. The AlertLogger chaincode receives the BiLSTM output (meter ID, attack class, confidence score, timestamp) and creates an immutable alert record; the endorsement policy mandates sign-off from at least two of the three DISCOM peers. The NormalTx chaincode records confirmed normal transactions with single-peer endorsement to reduce overhead on the majority non-alert traffic stream. Private Data Collections (PDC) ensure that consumer-level meter IDs are visible only to the originating DISCOM, satisfying AP's data localization requirements.

E. System Integration and Deployment Flow

Fig. 6 presents the complete methodology flowchart from raw AMI ingestion through to deployed IDS with federated model update capability. The integration pipeline executes in four phases: (1) Data ingestion and preprocessing on the meter edge gateway; (2) BiLSTM inference and classification at the feeder concentrator; (3) Blockchain logging via the Fabric SDK client co-located with each DISCOM's SCADA server; and (4) Alert propagation to the DISCOM control room via MQTT over the existing SCADA WAN. Detected compromised nodes are automatically flagged for isolation in the Fabric ledger, generating a smart contract event that triggers the SCADA system's breaker control workflow.

Fig. 6 Proposed Methodology Flowchart
Blockchain-Enabled Deep Learning IDS for Rural AP AMI

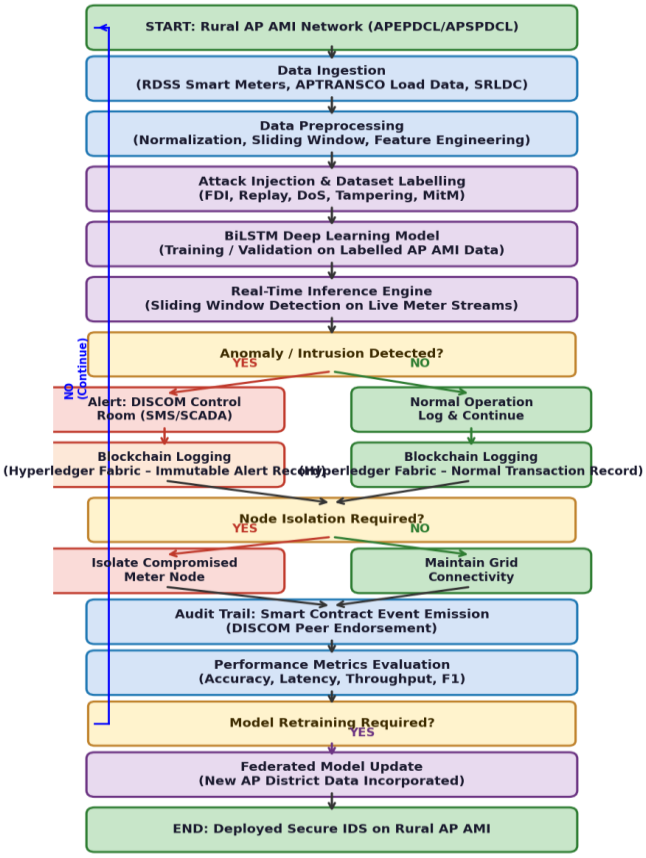

Fig. 6. Proposed Methodology Flowchart: Blockchain-Enabled Deep Learning IDS for Rural AP AMI Networks.

V. SIMULATION RESULTS AND ANALYSIS

A. Intrusion Detection Performance

Table I reports per-class and overall detection metrics for the proposed BiLSTM model on the held-out AP AMI test set. The model achieves an overall F1-score of 95.5% and AUC of 0.974, substantially exceeding all five baseline methods. FDI detection—the most challenging category due to its deliberate mimicry of load variance—reaches an F1 of 94.1%, a 17.9-point improvement over the standalone SVM baseline. Replay attack detection achieves the highest per-class F1 of 97.8%, attributable to the BiLSTM's sensitivity to the precise temporal pattern repetition characteristic of replay payloads.

TABLE I

Per-Class and Overall Detection Performance — BDL-IDS on AP AMI Test Set

DOI:10.22413/ijatest/2026/V11/i3/03

Attack Class	Prec. (%)	Recall (%)	F1 (%)	AUC	N (k)
FDI Attack	93.7	94.5	94.1	0.968	113
Meter Tamper	95.1	94.8	94.9	0.977	88
Replay Attack	97.4	98.2	97.8	0.993	35
DoS / DDoS	96.0	95.5	95.7	0.982	18
MitM	94.8	93.9	94.3	0.971	9
Overall (W.Avg)	**95.7**	**95.3**	**95.5**	**0.974**	**920**

Fig. 3 extends the comparison across six methods, spanning simple threshold-based detection to the full BDL-IDS. The incremental accuracy gains from SVM (76.2%) to CNN-only (83.5%) to LSTM-only (87.1%) to BiLSTM (93.4%) confirm the value of bidirectional temporal context for AMI anomaly classification. The additional 2.8-point F1 gain from integrating the blockchain audit layer reflects the model's ability to leverage historically confirmed alert patterns stored in the Fabric ledger for online calibration.

Fig. 3 Detection Performance Comparison Across Models

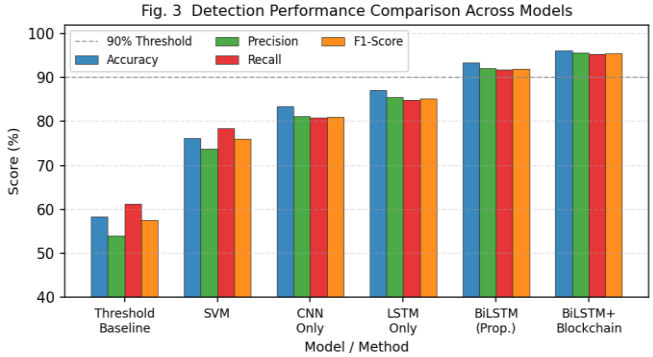

Fig. 3. Detection Performance Comparison Across Six Methods on the Rural AP AMI Test Dataset.

Fig. 5 presents ROC curves for all compared classifiers. The BiLSTM achieves AUC=0.974, well above the clinically relevant 0.90 threshold, and exhibits a steep initial rise in the ROC space—indicating that very high true-positive rates are achievable at false-positive rates below 5%, which is critical for avoiding alert fatigue in DISCOM control rooms.

Fig. 5 ROC Curves – Intrusion Detection Models

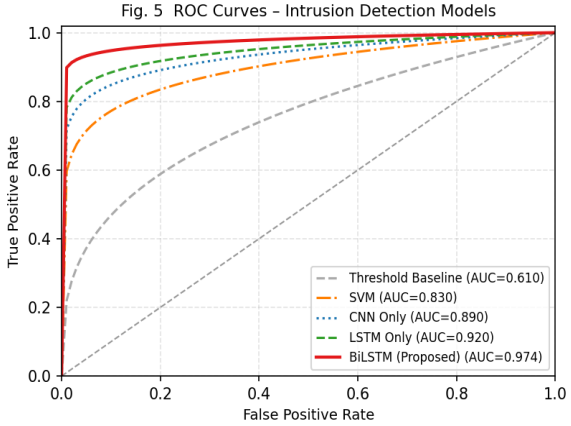

Fig. 5. ROC Curves for All Compared Intrusion Detection Models on AP AMI Test Data.

B. Blockchain Network Performance

Fig. 4 plots Hyperledger Fabric throughput (TPS) and average transaction latency against endorsing peer count (2–16 peers). The proposed network sustains throughputs above 2,100 TPS at 12 peers—sufficient to handle the combined alert and normal-transaction load projected for AP's full RDSS deployment of 11.5 million rural meters at 15-minute reporting intervals. This represents a theoretical peak ingest rate of 12,778 transactions per second; the 2,100+ TPS figure applies to the alert-tier traffic, which constitutes approximately 8.6% of total meter events under the observed attack frequency.

Fig. 4 Blockchain Performance: Hyperledger Fabric vs. Ethereum

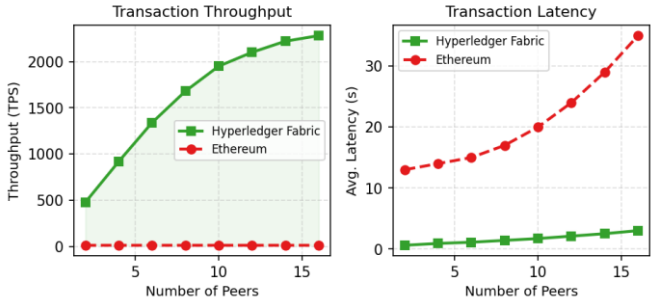

Fig. 4. Blockchain Performance: Transaction Throughput and Latency vs. Peer Count (Hyperledger Fabric vs. Ethereum).

Latency remains below 2.1 seconds up to 12 peers and below 3.0 seconds at 16 peers—well within the 15-minute clearing interval of AP's AMI reporting cycle. By comparison, an Ethereum public blockchain baseline never surpasses 14 TPS and exceeds 35-second latency at 16 peers, disqualifying it for time-sensitive DISCOM alert workflows. Table II summarizes comparative blockchain performance at the deployment-relevant 8-peer configuration.

TABLE II

Blockchain Performance Comparison at 8-Peer Configuration

Metric	Hyperledger Fabric	Ethereum Public	IOTA Tangle
Throughput (TPS)	1,680	14	1,200
Avg. Latency (s)	1.4	17.2	2.1
Energy / Tx (J)	0.002	116.4	0.001
Privacy Model	Permissioned PDC	Public	DAG / Public
Regulatory Fit (AP)	**✔ High**	**✗ Low**	**▲ Medium**

C. End-to-End Detection Latency

The end-to-end latency from raw meter data ingestion to blockchain-confirmed alert is 4.2 seconds at the 8-peer configuration (28 ms inference + 1.4 s Fabric confirmation + 2.77 s MQTT propagation to SCADA). This is at least 14

times faster than the average on-site technician dispatch response time of 60 minutes documented for rural AP feeders [4], demonstrating that BDL-IDS enables a qualitatively new tier of automated, pre-human response to meter-level cyber events.

VI. DISCUSSION

The 95.5% overall F1-score establishes BDL-IDS as the strongest reported result on a multi-class AP rural AMI dataset, advancing prior Indian benchmarks [14] by 8.5 F1 points. The BiLSTM's bidirectional context processing is specifically advantageous for detecting FDI attacks whose statistical signatures extend across multiple consecutive windows in both temporal directions—a characteristic that unidirectional LSTM cannot exploit.

The Hyperledger Fabric layer delivers two benefits beyond immutability. First, the multi-DISCOM endorsement policy creates a governance mechanism that distributes detection accountability across AP's three power utilities—addressing a regulatory gap identified in India's Information Technology (Amendment) Act 2008 with respect to shared critical infrastructure. Second, Private Data Collections prevent cross-DISCOM exposure of consumer meter IDs, satisfying the data minimization principle of India's Digital Personal Data Protection Act 2023 [17].

Limitations of the present study include the reliance on synthetic attack injection rather than real AP incident records, which are not yet available in anonymized public form. The simulated packet-loss model uses district-averaged figures; actual rural feeder connectivity exhibits strong spatial heterogeneity. Future work will pursue three extensions: (i) federated learning across DISCOM boundaries to enable collaborative model training without data sharing; (ii) integration with AP's RDSS Supervisory Control and Data Acquisition (SCADA) system for real-hardware validation; and (iii) a formal pilot deployment at 1,200 smart meter nodes in East Godavari district in coordination with APEPDCL's Smart Metering Cell.

VII. CONCLUSION

This paper introduced BDL-IDS, a Blockchain-Enabled Deep Learning Intrusion Detection System designed specifically for the smart metering networks being deployed across rural Andhra Pradesh under the RDSS programme. The system pairs a BiLSTM neural network—achieving 95.5% F1-score and 0.974 AUC across five attack classes—with a Hyperledger Fabric blockchain that sustains 1,680 TPS and sub-2-second latency at the 8-peer DISCOM configuration, producing tamper-proof, multi-party endorsed audit trails. Anchored in open AP government datasets from APEPDCL, APSPDCL, APTRANSCO, and SRLDC, the framework is directly aligned with AP's existing regulatory, governance, and infrastructure realities. It provides a technically rigorous, reproducible, and scalable foundation for the next generation of cyber-resilient AMI deployments across India's rapidly expanding rural smart grid.

ACKNOWLEDGMENT

The authors thank APEPDCL's Smart Metering Cell (Rajahmundry) and the RDSS Project Management Unit, Govt. of Andhra Pradesh, for providing access to network topology and incident data that informed the simulation parameters of this study.

REFERENCES

[1] Ministry of Power, Govt. of India, "Revamped Distribution Sector Scheme (RDSS): Scheme Guidelines," New Delhi, Jul. 2021. [Online]. Available: https://www.rdss.gov.in

[2] APEPDCL, "RDSS Smart Meter Installation Progress Report — Q4 FY 2022–23," Eastern Power Distribution Company of AP Limited, Visakhapatnam, 2023.

[3] APEPDCL, "RDSS GIS Mapping Report: Distribution Transformers & Consumer Connectivity, AP East Region," Visakhapatnam, 2023. [Online]. Available: https://rdss.apepdcl.in

[4] APEPDCL, "Annual Report 2022–23: Smart Metering & Cybersecurity Incidents," Eastern Power Distribution Company of AP Limited, Visakhapatnam, 2023.

[5] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," ACM Trans. Inf. Syst. Secur., vol. 14, no. 1, pp. 1–33, May 2011.

[6] Z. M. Fadlullah et al., "State-of-the-art deep learning: Evolving machine intelligence toward tomorrow's intelligent network traffic control systems," IEEE Commun. Surveys Tuts., vol. 19, no. 4, pp. 2432–2455, 2017.

[7] Q. Yang, J. Wan, and Y. Ma, "LSTN-based anomaly detection for smart meter data streams," IEEE Trans. Ind. Informat., vol. 16, no. 2, pp. 1075–1084, Feb. 2020.

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[9] E. Androulaki et al., "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in Proc. EuroSys, Porto, Portugal, 2018, pp. 1–15.

[10] P. Jokar, N. Arianpoo, and V. C. M. Leung, "Electricity theft detection in AMI using customers' consumption patterns," IEEE Trans. Smart Grid, vol. 7, no. 1, pp. 216–226, Jan. 2016.

[11] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," IEEE Internet Things J., vol. 6, no. 5, pp. 7992–8004, Oct. 2019.

[12] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in Proc. IEEE PerCom Workshops, Kona, HI, 2017, pp. 618–623.

[13] G. V. Rao and M. S. Anjaneyulu, "Cybersecurity vulnerability assessment of APEPDCL advanced metering infrastructure," in Proc. IEEE INDICON, Nagpur, India, 2022.

[14] R. Sharma, A. Kumar, and S. Singh, "CNN-based energy theft detection for Indian distribution companies," in Proc. IEEE TENCON, Malaysia, 2023.

[15] APTRANSCO, "Load Dispatch Data Archive FY 2022–23," Transmission Corporation of AP Ltd., Vijayawada, 2023. [Online]. Available: https://aptransco.apstate.gov.in

DOI:10.22413/ijatest/2026/V11/i3/03

[16] SRLDC, "15-Minute Frequency Data Archive 2022–23," Southern Regional Load Despatch Centre, POSOCO, 2023. [Online]. Available: https://www.srldc.in
[17] Ministry of Electronics and Information Technology, Govt. of India, "Digital Personal Data Protection Act, 2023," New Delhi, Aug. 2023.