ISSN 2277-2685
IJESR/April-June. 2025/ Vol-15/Issue-2/848-854
K Satish *et. al.,* / International Journal of Engineering & Science Research

Sending Smart Meter Data to the Head-End System over a 4G Cellular Network

K Durga Rao[1], Dr. Gautam Moni Patro[2], K Satish[3], M Somesh[4], G Sai Siddu[5]

[1,2]Assistant Professor, Associate Professor Department of Electrical and Electronics Engineering, Avanthi Institute of Engineering & Technology, Tamaram, Makavarapalem, Anakapalle – 531113, Andhra Pradesh, India

[3,4,5]UG Student, Department of Electrical and Electronics Engineering, Avanthi Institute of Engineering & Technology, Tamaram, Makavarapalem, Anakapalle – 531113, Andhra Pradesh, India

Abstract

This paper presents a smart-metering data communication system that uses 4G cellular connectivity to link Data Concentrator Units (DCUs) with a Head-End System (HES). Traditional meter-data communication methods often suffer from latency, limited coverage and reliability issues; integrating a 4G module into the DCU improves the speed, accuracy and security of data transfer. Each DCU, built on a Rugged Board (i.MX6UL) single-board computer, aggregates readings from multiple smart meters over UART/RF and forwards them, through a Network Interface Card and a 4G module, to an MQTT broker that feeds the HES and, ultimately, utility billing and grid-management systems. Lightweight protocols such as MQTT, together with TLS/IPsec encryption, mutual authentication and a private Access Point Name (APN), keep the link secure and bandwidth-efficient over a wide-area cellular network. The system was validated through unit, integration, system and user-acceptance testing, and a structured deployment plan and set of key performance metrics (signal strength, throughput, latency, packet loss, device uptime) support ongoing operation. The resulting architecture gives utilities real-time, wide-area visibility into energy consumption without depending on fixed physical infrastructure.

Index Terms— *Data Concentrator Unit (DCU), Head-End System (HES), 4G LTE, smart meter, MQTT, DLMS/COSEM, network security, cellular communication.*

I. INTRODUCTION

Traditional energy-data communication methods often suffer from latency, limited coverage and reliability issues. This work integrates 4G cellular connectivity into the smart-metering data path to improve the speed, accuracy and security of data transfer between smart-metering components. At the core of the system is the interaction between the Data Concentrator Unit (DCU), which aggregates data from multiple smart meters, and the Head-End System (HES), which receives, processes and analyses that data for utility decision-making. Reliable, real-time communication between these components lets utility providers optimize energy distribution, monitor consumption patterns and improve operational efficiency, while reducing losses and improving grid stability.

4G connectivity was selected for the DCU-to-HES link because it offers high-speed, low-latency transmission; wide coverage, including remote areas without fixed infrastructure; reliable connectivity that minimizes data loss; and cost-effectiveness relative to laying fibre or other physical links. Within the wider metering ecosystem, this 4G-enabled link automates data collection in place of manual meter reading, improves billing accuracy through precise real-time consumption data, supports demand forecasting and grid-management decisions, and enables remote monitoring and fault detection without on-site visits.

The objectives of the system are to (i) enable seamless, real-time communication between smart meters, DCUs and the HES while minimizing data loss and transmission errors over 4G; (ii) give utilities instant, on-demand access to consumption data, including rapid detection of anomalies such as energy theft or tampering; and (iii) do so securely, with authentication, encryption and access-control mechanisms appropriate to critical utility infrastructure.

II. BACKGROUND: SMART ENERGY METERS

A smart meter is an advanced electronic device that records electricity consumption with high accuracy and, unlike a simple energy meter, supports two-way communication with the utility. Metering has evolved over more than 140 years, from electrolytic and electromechanical (induction) meters, through static/digital meters, to today's smart meters, which report usage at least daily — often hourly or more frequently — and enable advanced metering infrastructure (AMI) rather than one-way automatic meter reading (AMR). Communication from the meter to the network may be wired, over power-line carrier (PLC), or wireless — cellular, Wi-Fi, wireless mesh, LoRa or Zigbee among the common options — with cellular chosen here for its wide-area reach and independence from dedicated physical infrastructure.

III. SYSTEM ARCHITECTURE

The system architecture has five layers: smart meters, which measure consumption in real time and communicate over RF, PLC or direct cellular; the DCU, which collects data from multiple meters in a designated area and acts as an aggregator; a 4G cellular module, which provides wireless communication between the DCU and the HES with secure, reliable, real-time transmission; the HES, which receives, processes and stores the data before forwarding it to utility backend systems; and the utility backend itself — a Meter Data Management System (MDMS) for storage and analysis, a billing system for invoicing, and grid-management/analytics tools for demand forecasting, outage detection and load balancing.

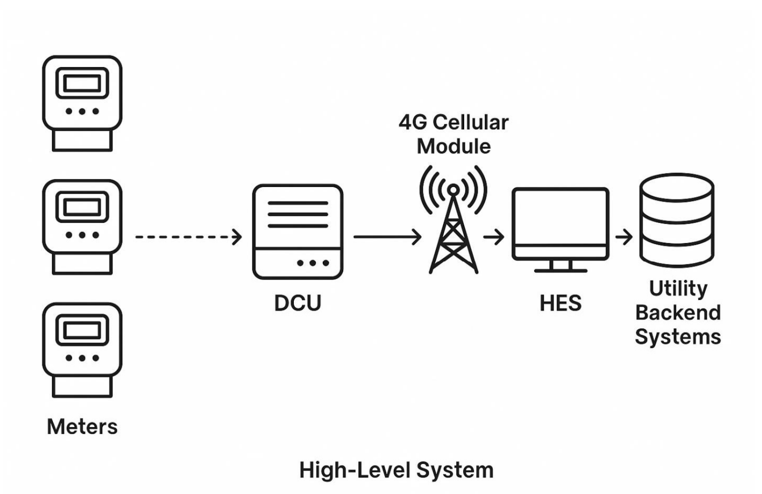

Fig. 1. High-level system view: meters, DCU, 4G cellular module, HES and utility backend.

In the implemented prototype, each meter connects over UART to its own Network Interface Card (NIC), and the NIC array feeds a single NIC/DCU pair over UART; the DCU, in turn, communicates over the cellular link to an MQTT broker, which a Windows-hosted Gurux tool and a Gurux-to-MQTT converter script use to bridge the metering protocol into standard MQTT/UDP messaging for the HES side of the system, as shown below.

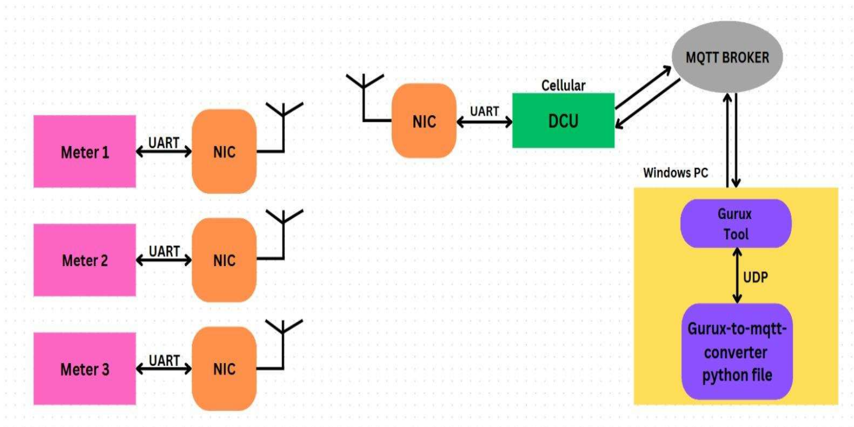

Fig. 2. Detailed data path from meters through NIC/DCU to the MQTT broker and host-side Gurux tooling.

IV. HARDWARE COMPONENTS

A. Rugged Board (i.MX6UL) as the DCU

The DCU is built around the NXP i.MX6UL processor (ARM Cortex-A7, 686 MHz) on a phyCORE-i.MX6UL System-on-Module, with 512 MB RAM and 512 MB NAND flash, running Yocto embedded Linux (kernel 4.9) over an industrial temperature range of -40°C to +85°C. It exposes 1× CAN, 1× RS-485, 1× RS-232, 8× digital I/O, 10/100 Ethernet, 2× USB, a microbus socket, mini-PCIe, a SIM/SD card slot and I2C/SPI/UART/PWM expansion, which lets it interface with meters and other field devices while remaining suitable for outdoor/industrial deployment.

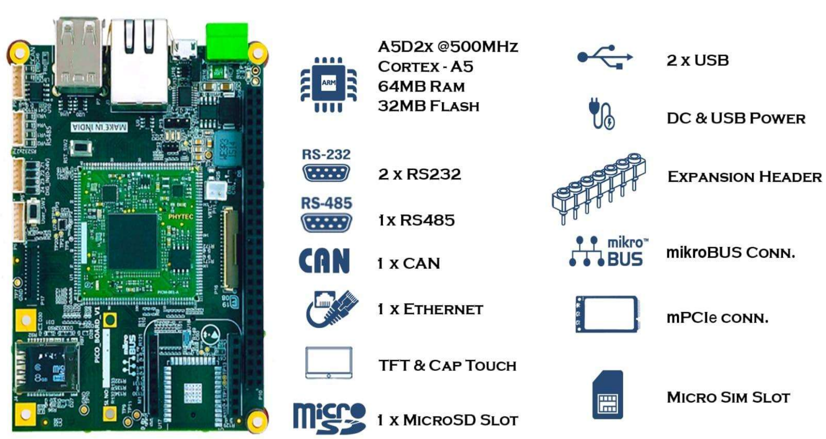

Fig. 3. Rugged Board (i.MX6UL) used as the Data Concentrator Unit, with key interfaces.

ISSN 2277-2685
IJESR/April-June. 2025/ Vol-15/Issue-2/848-854
K Satish *et. al.,* / International Journal of Engineering & Science Research

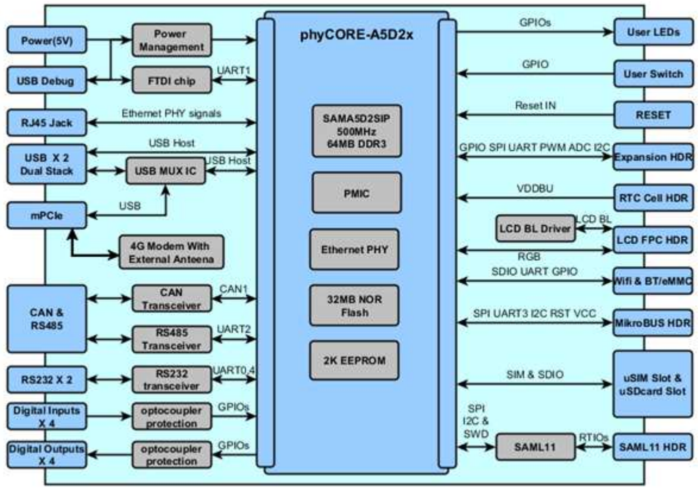

Fig. 4. Internal block diagram of the Rugged Board (phyCORE-A5D2x).

B. 4G Cellular Module and Head-End System Platform

The 4G module uses LTE Cat 1, Cat M1 or NB-IoT modems (bands B1/B3/B5/B8/B20/B28/B40) depending on speed and bandwidth needs, reaching roughly 10 Mbps downlink / 5 Mbps uplink on Cat 1, with an external SMA antenna. It connects to the network through a dedicated Access Point Name (APN), supports VPN/encryption for data security, and can fail over to 3G or a backup network if the 4G signal weakens. On the HES side, the platform performs data acquisition and storage, real-time monitoring and diagnostics, remote configuration and OTA firmware updates, alarm/event management, and integration with billing and SCADA systems, typically via REST, SOAP or OPC-UA APIs and either cloud or on-premise deployment.

V. DATA FLOW AND COMMUNICATION OVER 4G

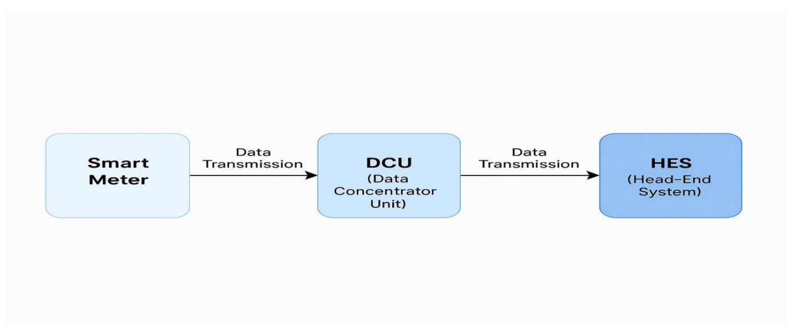

Fig. 5. End-to-end data flow: smart meter to DCU to Head-End System.

At the meter, the system continuously captures energy consumption (kWh, kVARh), power-quality parameters (voltage, current, frequency, power factor), time-stamped load profiles, event logs (outages, tamper alerts, overvoltage) and billing-relevant data such as time-of-use tariffs. The DCU then preprocesses this stream — filtering out redundant or corrupted packets, compressing and aggregating multiple meter readings, flagging anomalies such as theft or tampering, and time-stamping records against a real-time clock — before forwarding it to the HES over 4G LTE, Ethernet or Wi-Fi.

Three transmission modes are supported: periodic transmission at fixed intervals (e.g., every 15 minutes, hourly or daily) for routine billing and monitoring; on-demand transmission, where the HES requests specific data for manual verification or remote diagnostics; and event-driven transmission, where the DCU pushes data immediately on a critical event such as an outage, tampering attempt or voltage fluctuation. Depending on latency, bandwidth and security requirements, the link uses MQTT (a lightweight publish/subscribe protocol well suited to constrained, high-latency 4G links), HTTPS for RESTful API integration, CoAP for very low-power constrained devices, or FTP/SFTP for scheduled bulk transfers, all typically running over TCP/IP with TLS/SSL for confidentiality.

On arrival, the HES ingests the data (via MQTT, HTTPS or CoAP, in JSON/XML/CSV or DLMS/COSEM framing), decodes it, synchronizes timestamps, and authenticates the originating DCU before validation: checking format, verifying checksums, discarding duplicates and flagging anomalies such as sudden consumption spikes. Validated data is written to both a short-term store for live dashboards and a long-term archive for billing and trend analysis, in a SQL/NoSQL or cloud database with redundancy and scheduled backups, and is then used for tariff/billing calculation, demand forecasting, power-quality monitoring and tamper/fraud detection.

VI. AUTHENTICATION, AUTHORIZATION AND DATA SECURITY

Because metering data is sensitive and the link traverses a public cellular network, the DCU, 4G module and HES authenticate one another before exchanging data. Device authentication relies on the 4G module's IMEI, SIM-based authentication against a private APN, and mutual TLS (mTLS) certificate exchange between DCU and HES; network-level authentication uses EAP within the LTE network and an IPsec VPN tunnel between DCU and HES; and server-side authentication uses OAuth 2.0/API keys for third-party access and X.509 certificates for mutual authentication. Once authenticated, role-based access control (admin, operator, auditor), access-control lists, and time- or location-based restrictions determine what a device or user may do.

Data is encrypted both at rest and in transit: AES-256 protects stored meter readings, configuration and logs (with keys held in a Hardware Security Module and rotated regularly), while TLS 1.2/1.3, IPsec and MQTT-over-TLS protect data in transit between meter, DCU and HES; end-to-end encryption keeps intermediate hops — including the DCU itself — from reading commands sent from the HES to a meter, using RSA-2048 for particularly sensitive commands. At the network layer, firewalls (including next-generation, deep-packet-inspection firewalls) filter traffic, IPsec/OpenVPN tunnels and a private APN isolate metering traffic from the public internet, and IDS/IPS deployed at the DCU, HES and cloud tiers monitor for anomalous access attempts.

Because smart-meter data can reveal household activity patterns, the system also incorporates privacy-by-design measures aligned with regulations such as GDPR, the CCPA and India's DPDP Act, and with security-management standards such as ISO/IEC 27001: data minimization and purpose limitation, explicit user consent and transparency, anonymization/pseudonymization for analytics, encrypted storage with role-based access, and defined data-retention and breach-notification procedures, together with a periodic Privacy Impact Assessment (PIA) covering data inventory, risk assessment, mitigation and policy review.

VII. TESTING AND VALIDATION

The system was validated through four stages. Unit testing checked each component in isolation: DCU data collection and buffering during network outages; 4G-module network registration, signal stability, APN authentication and TLS/IPsec behaviour; and HES API responsiveness, data processing and storage. Integration testing then validated the links between components — meter data reaching the HES over 4G without packet loss, correct failover on signal drop, TLS-encrypted MQTT/HTTP transmission, and rejection of connection attempts from unauthorized DCUs. System testing exercised the whole pipeline under realistic load (for example, simulating on the order of 100,000 meters reporting simultaneously), alongside security testing (firewall, RBAC, IDS/IPS, simulated MITM/DDoS attempts) and failover/recovery testing after simulated network loss. Finally, user-acceptance testing had utility operators, field engineers and IT staff verify billing-system integration, the consumer portal/mobile app, and remote meter connect/disconnect commands against real operational scenarios, before a deployment checklist (tests passed, vulnerabilities remediated, UAT feedback incorporated, backup/rollback plan ready, phased rollout defined) was signed off.

VIII. DEPLOYMENT AND OPERATIONAL MONITORING

Deployment begins with a site survey covering 4G coverage, power availability, physical security and maintenance access, followed by physical installation of the DCU (pole-, wall- or enclosure-mounted, in a weatherproof housing outdoors), wiring to meters over RS-485/Modbus/PLC or RF/Zigbee/Wi-Fi, and power-up with LED verification. The 4G module is then commissioned: inserting an IoT SIM and configuring its APN, positioning the antenna and checking signal strength, registering on the carrier network with TLS/VPN/IP-whitelisting security applied, and test-transmitting data to confirm there is no latency or packet loss. System configuration registers the DCU in the HES, applies the latest firmware, validates the full meter-to-DCU-to-4G-to-HES data path, and applies encryption/authentication/firewall settings; post-installation checks confirm network stability, data accuracy, remote-command capability and power-backup behaviour, with serial numbers, GPS coordinates, signal logs and security configuration all documented.

Once live, the system is monitored against key metrics: signal quality (RSRP/RSRQ/SINR), data throughput, latency and packet loss, error/retransmission rates, device uptime, and storage/database health, using network-monitoring tools, bandwidth analysers, ping tests, uptime monitors and SQL/log analysers. Threshold-based alerts (e.g., RSRP below about -100 dBm, or packet loss above roughly 5%) and periodic reports support continuous improvement, and a documented troubleshooting procedure covers the common failure modes — no data from the DCU, weak or absent 4G signal, high latency/packet loss, data not updating at the HES, and authentication failures — together with a scheduled OTA firmware/software update process for the DCU, 4G module and HES.

IX. CONCLUSION

Routing smart-meter data through a Rugged Board DCU and a 4G cellular link to the Head-End System gives utilities a wide-area, real-time metering communication path that does not depend on fixed physical infrastructure. Lightweight protocols such as MQTT, layered with device/network/server authentication, TLS/IPsec encryption and a private APN, keep the link both bandwidth-efficient and secure, while a structured testing regime and deployment plan, backed by continuous performance monitoring and a defined update process, support reliable long-term operation. Together, these elements enable more accurate billing, faster fault detection and better-informed grid management than legacy, manually read metering infrastructure.

References

[1] IEC 62056 (DLMS/COSEM), "Electricity metering data exchange — The DLMS/COSEM suite," International Electrotechnical Commission.

[2] OASIS, "MQTT Version 5.0 / 3.1.1 Specification," OASIS Standard.

[3] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); LTE physical layer," 3GPP Technical Specifications (36-series).

[4] IETF RFC 7252, "The Constrained Application Protocol (CoAP)."

[5] IETF RFC 4301 / RFC 8446, "Security Architecture for the Internet Protocol (IPsec)" and "The Transport Layer Security (TLS) Protocol Version 1.3."

[6] ISO/IEC 27001, "Information security, cybersecurity and privacy protection — Information security management systems — Requirements."

[7] Regulation (EU) 2016/679, "General Data Protection Regulation (GDPR)."

[8] California Civil Code §1798.100 et seq., "California Consumer Privacy Act (CCPA)."

[9] Digital Personal Data Protection Act, 2023, Government of India.

[10] NXP Semiconductors, "i.MX 6UltraLite Applications Processor Reference Manual."