WHITE PAPER

CYBERSECURITY AND DATA PRIVACY AS CORNERSTONES OF AMI 2.0

Abstract

As the utility industry transitions from first-generation advanced metering infrastructure (AMI 1.0) to next-generation AMI 2.0, the importance of robust cybersecurity and stringent data privacy cannot be overlooked. Cybersecurity and data privacy are integral to design, deployment, and operation of AMI 2.0.

As AMI 2.0 moves beyond traditional automated meter reading to serve as a cornerstone of the energy transition, it significantly expands the digital attack surface and increases the sensitivity of the data being collected. It enhances grid visibility, integration of distributed energy resources (DER), and sophisticated customer engagement.

Gartner predicts that by 2025, cyber attackers will have weaponized operational technology environments with the potential to cause physical harm and even loss of life.

This paper explains how cybersecurity and data privacy are not ancillary considerations but fundamental prerequisites for building a resilient, reliable, and trustworthy future grid. The central thesis underscores the imperative for utilities to proactively integrate and continually adapt holistic security and privacy strategies. These measures are essential to safeguard critical infrastructure, maintain customer trust, ensure regulatory compliance, and unlock the transformative potential of AMI.

Infosys®
Navigate your next

External Document © 2025 Infosys Limited

Introduction:

The energy landscape is in the midst of rapid transformation. Driven by ambitious decarbonization targets, the need for stronger grid resilience, and the evolving expectations of digitally empowered consumers, utilities are increasingly turning to next-generation technologies to build a smarter, more flexible, and sustainable energy future.

Central to this evolution is advanced metering infrastructure (AMI) 2.0, envisioned as the intelligent sensory and communication backbone of the modern grid. AMI 2.0 offers unprecedented capabilities for real-time visibility, dynamic load management, seamless integration of distributed energy resources (DERs), proactive outage response, and personalized customer experiences.

As utilities prepare for widespread AMI 2.0 deployment, the scale of opportunity is matched by the scale of responsibility. Distributed intelligence, two-way communication, granular data collection, and direct control capabilities make AMI 2.0 very powerful. These features also introduce a significantly expanded cyber-attack surface and heightened concerns over the privacy and security of sensitive consumer and operational data.

This white paper examines how utilities can adopt a strategic approach to a critical, non-negotiable aspect of this transition: the foundational role of robust cybersecurity and stringent data privacy in building and operating AMI 2.0 solutions. These are not merely compliance exercises or technical add-ons, but core pillars essential to:

- Safeguarding the reliability of critical infrastructure
- Maintaining customer trust
- Navigating an increasingly complex regulatory environment
- Unlocking the full spectrum of AMI 2.0 benefits

More specifically, we explore:

- The role of cybersecurity and data privacy as enablers, not inhibitors, of the potential of AMI 2.0
- The applications within the AMI 2.0 ecosystem that require heightened security and privacy measures
- The evolving technologies and threat vectors that demand proactive defenses
- Architectural considerations vital to security and interoperability
- Comprehensive mitigation strategies for building resilient, trustworthy infrastructure

The objective of this paper is to provide insights and a forward-looking perspective, ensuring that as we build the grid of tomorrow, security and privacy are at its core.

The Crucial Role of Cybersecurity and Data Privacy in AMI 2.0

AMI 1.0 primarily focused on automated meter reading for billing. AMI 2.0, however, transforms the meter into an intelligent edge device, deeply embedded in grid operations and customer engagement. This evolution expands the range of vulnerable areas that utilities must focus on, as listed in Table 1.

Table 1: Vulnerabilities and potential impact areas

Vulnerabilities	Potential impact areas
Expanded attack surface	Millions of smart meters, communication modules, and associated network infrastructure create countless entry points for malicious actors.
Increased systemic risk	A compromise could trigger widespread outages, grid instability, energy market manipulation, or coordinated denial-of-service attacks, threatening critical infrastructure.
Heightened data sensitivity	Granular energy consumption data can reveal lifestyle patterns, occupancy, and specific appliance usage. Protecting this data is essential to maintain customer trust and meet evolving privacy regulations.
Real-time control implications	Features like remote connect/disconnect, demand response commands, and firmware updates, if compromised, could have immediate physical consequences.

External Document © 2025 Infosys Limited

Failure to adequately address cybersecurity and data privacy can lead to catastrophic operational disruptions, significant financial losses, severe reputational damage, stringent regulatory penalties, and an erosion of consumer trust, thereby hindering the very progress AMI 2.0 aims to achieve.

Focus Areas Across Critical Assets and Applications Within the AMI 2.0 Ecosystem

A holistic security and privacy strategy must factor every component and application within the AMI 2.0 ecosystem. Table 2 highlights the key focus areas and associated risks across critical assets.

Table 2: Key assets and applications: Security focus areas and risks

Assets and applications	Focus	Risks
Smart meters and edge devices	Secure boot, device identity, and authentication (e.g., using public key infrastructure or PKI), tamper detection (physical and cyber), secure firmware updates, encryption of data at rest and in transit, as well as secure local data processing for edge analytics	Unauthorized access, malicious firmware injection, data manipulation, and denial of service
Communication networks (field area network - FAN, neighborhood area network - NAN, wide area network - WAN)	Strong encryption protocols (e.g., DLMS/COSEM security profiles and IEC 62351), network segmentation, intrusion detection/prevention systems (IDS/IPS) tailored to AMI traffic, secure network management, and authentication of all communicating entities	Eavesdropping, man-in-the-middle attacks, jamming, replay attacks, and unauthorized network access
Head-end system (HES)	Robust access controls (such as multi-factor authentication or MFA), secure application programming interfaces (APIs), vulnerability management, regular security audits, secure data aggregation as well as command dissemination	Unauthorized system control, data modification, and denial of service affecting large meter populations
Meter data management system (MDMS)	Secure data storage, data integrity checks, role-based access control (RBAC), comprehensive audit trails, data anonymization / pseudonymization techniques as appropriate, and secure data exchange interfaces with other utility systems like CIS, OMS, DMS, DERMS	Large-scale data breaches, billing fraud, unauthorized data alteration, and privacy violations
Customer information systems (CIS) and billing	Secure transfer of validated meter readings, financial data protection, and data accuracy for billing processes	Billing errors, financial fraud, exposure of sensitive financial details
Customer portals and mobile applications	Secure authentication, encrypted communication, protection against common web/mobile vulnerabilities, clear privacy notices, and granular consent management for data sharing	Customer account takeover, personal and consumption data exposure, as well as phishing
Grid operations and analytics platforms (OMS, DMS, DERMS)	Secure and authenticated data feeds ensuring integrity of control signals based on AMI data, secure interfaces for DER control and monitoring	Incorrect operational decisions from compromised data and DER manipulation impacting grid stability

External Document © 2025 Infosys Limited

Evolving Technological Concepts for Consideration

The threat landscape and supporting technologies are constantly evolving. AMI 2.0 strategies must take into consideration various emerging technological concepts and their associated threat vectors as outlined in Table 3.

Table 3: Evolving technological concepts relevant to AMI 2.0

Evolving technology concepts	Considerations
Zero trust architecture (ZTA)	AMI 2.0 requires a shift from perimeter-based defenses to a model where no user or device is inherently trusted. Every access request must be verified, regardless of whether it originates from inside or outside the network. This is crucial for complex and distributed AMI networks.
Artificial intelligence (AI) and machine learning (ML) in security and operations	AI/ML can be leveraged for advanced threat detection (e.g., anomaly detection in network traffic or consumption patterns) and predictive maintenance. Conversely, attackers may also use AI to develop more sophisticated attacks.
IoT proliferation and edge computing security	AMI 2.0 introduces more IoT devices and pushes intelligence to the edge, which requires securing resource-constrained devices and managing their lifecycle.
Quantum computing threats to cryptography	Quantum computing has the potential to break current cryptographic standards. Utilities should monitor developments in quantum-resistant cryptography (QRC) for long-term data protection.
Supply chain security (C-SCRM)	The hardware and software supply chain can introduce vulnerabilities at any point, making it necessary to conduct rigorous vendor assessments, secure component sourcing, and verify firmware as well as software integrity. The National Institute of Standards and Technology (NIST) CyberSecurity Framework (CSF) 2.0 now explicitly includes a "Govern" function (GV.SC) that focuses on CSF's cybersecurity supply chain risk management (C-SCRM) program.
Cloud and hybrid deployments	As AMI systems leverage cloud services for scalability and analytics, understanding and managing shared responsibility models for security, robust data residency, and access controls are critical.
Evolving regulatory landscape	Utilities must comply with NERC CIP standards (which increasingly impact AMI systems with control capabilities like mass remote disconnect), state-level data privacy laws (e.g., California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA) like legislations), and relevant federal guidance.

External Document © 2025 Infosys Limited

Interoperability and Security – Standard Architectural Considerations

A secure and interoperable AMI 2.0 ecosystem should be built with the standard architectural considerations listed in Table 4.

Table 4: AMI standard architectural considerations

Standard architectural considerations	Description
Secure by design and by default	Security and privacy considerations must be integrated from the initial design phase rather than added later, and default configurations must be secure.
Defense-in-depth (Layered security)	Multiple layers of security controls (e.g., physical, network, application, data) must be implemented so that if one layer is breached, others continue to protect critical assets.
Standards-based approach	Adherence to industry standards is crucial for both security and interoperability. Key standards include: ➤ **NIST CSF 2.0** for managing cybersecurity risk ➤ **IEC 62351 series** for power system information exchange ➤ American National Standard: Protocol Specification for Interfacing to Data Communication Networks **ANSI C12.22/IEEE 1703** for meter data transport over networks ➤ **Device Language Message Specification (DLMS) and Companion Specification for Energy Metering (COSEM) (IEC 62056)** for smart meter data exchange and security ➤ **IEEE 2030.5 (SEP 2.0)** for smart energy profile application protocol, facilitating DER integration ➤ **Common Information Model (CIM - IEC 61970/61968)** for interoperability between utility IT systems ➤ **Open Field Message Bus (OpenFMB)** for interoperability at the grid edge
Public key infrastructure	PKI must be used to provide strong device identity, authentication, secure key exchange, and data integrity across the AMI ecosystem.
Network segmentation	Critical AMI network segments must be isolated from corporate networks and from each other to limit the blast radius of a potential breach.
Robust data governance framework	Policies for data classification, ownership, access, retention, and secure disposal must be clearly defined, and privacy-enhancing technologies (PETs) such as data minimization, anonymization, and pseudonymization must be applied where feasible.
Secure APIs	Secure, authenticated, and authorized application programming interfaces (APIs) are essential as AMI data is shared with third-party applications (with customer consent) or integrated with other utility systems.
Scalability and resilience	The architecture must be able to securely scale to millions of devices and remain resilient to failures and attacks, ensuring high availability of critical functions.

External Document © 2025 Infosys Limited

Cybersecurity and Data Privacy – Comprehensive Mitigation Strategies

A multi-faceted approach covering technology, process and people is necessary to factor comprehensive mitigation strategies for cybersecurity and data privacy with respect to AMI 2.0 exploration. The various approaches and their details have been presented in Table 5.

Table 5: Comprehensive mitigation strategies - technology, process and people

Mitigation strategy	Approach	Details
Technology-based mitigation	Strong authentication and authorization	All human access to critical systems must use MFA, while all devices must use PKI, and granular role-based access controls (RBAC).
	End-to-end Encryption	Data must be encrypted at rest (on meters, in databases) and in transit (across all network segments) using robust, up-to-date algorithms.
	Intrusion detection / prevention systems (IDS/IPS)	IDS and IPS solutions must be tailored for OT/AMI protocols and traffic patterns.
	Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR)	SIEM and SOAR must be used for centralized logging, correlation of security events, and automated response capabilities.
	Vulnerability management	Regular scanning, assessment, and prioritized remediation of vulnerabilities must be conducted in all AMI components.
	Secure device lifecycle management	Devices must be securely provisioned, configured, patched with over-the-air (OTA) updates verified by strong integrity checks, and decommissioned.
	Data Loss Prevention (DLP)	DLP tools and processes must be implemented to prevent sensitive data from leaving secure system boundaries.
Process-based mitigation	Comprehensive risk management	Cybersecurity risk assessments and privacy impact assessments (PIAs) must be conducted regularly, specific to the AMI 2.0 deployment.
	Incident Response Plan (IRP)	An IRP tailored to AMI-specific scenarios (e.g., mass meter compromise and data breach) must be developed, maintained, and regularly tested.
	Security awareness and training	Continuous training programs must be conducted for all personnel involved in AMI operations, IT, operational technology (OT), customer service, and even third-party contractors.
	Secure software development lifecycle (SSDLC)	All custom applications and integrations for the AMI system must be developed under a secure software lifecycle process.
	Third-party risk management (TPRM)	Rigorous security and privacy assessments must be performed for all vendors and service providers in the AMI ecosystem.
	Change management	Secure processes must be established to manage changes to AMI systems and configurations.
People-based Mitigation	Dedicated cybersecurity and privacy expertise	Organizations must invest in or contract with skilled professionals with expertise in OT, industrial control systems (ICS) cybersecurity, and data privacy.
	Clear roles and responsibilities	Security and privacy responsibilities must be clearly defined and communicated across the organization.
	Cross-departmental collaboration	Strong collaboration must be fostered between IT, OT, cybersecurity, legal, and customer service teams.

External Document © 2025 Infosys Limited

Conclusion

AMI 2.0 marks a pivotal step in modernizing the energy grid. Its success hinges on collective ability to build an infrastructure that is not only intelligent and efficient but also demonstrably secure and respectful of customer privacy. By embedding cybersecurity and data privacy principles into the very foundation of AMI 2.0 architecture, strategy, and operations, utilities can unlock its full potential. Doing so will help them in fostering customer trust, ensuring regulatory compliance, and strengthening energy resilience. A proactive, risk-informed, and continuously adaptive approach is not just recommended but essential.

About the Authors

Pradyumna Kishore Das
Utility Consulting | AMI and MDM | CIS and Billing | Energy Transition
Domain Consulting Group at Infosys

Pradyumna is a seasoned AMI techno-functional leader with over 20 years of experience supporting Fortune 500 utility companies. He specializes in driving business transformation across AMI and customer service domains, and serves as a trusted advisor on initiatives spanning AMI, CIS, billing, and customer experience. His expertise bridges functional, technical, and operational dimensions to deliver impactful utility solutions.

Saibal Kumar Kundu
Utility Consulting | AMI and MDM | T&D | Energy Transition
Domain Consulting Group at Infosys

Saibal is a versatile IT professional with more than 30 years of experience, bringing vision and leadership insights to strategically plan, direct and execute complex initiatives. For over 23 years, he has worked with leading global energy and utilities clients specializing in industry solutions, go-to-market development, pre-sales, large deal solutioning, architecture, and technology consulting.

References

1. Gartner | Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans
2. NIST | Cybersecurity Framework
3. Federal Energy Regulatory Commission| Electric
4. ISA Global Security Alliance | ISA/IEC 62443
5. International Electrotechnical Commission | Cyber security: understanding IEC 62351
6. NEMA | American National Standard for Electricity Meters for the Measurement of DC Energy
7. US Department of Energy | DOE Distributed Energy Resource Interconnection Roadmap

For more information, contact askus@infosys.com

Infosys®
Navigate your next

© 2025 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.