National Journal of Signal and Image Processing, ISSN: 3107-5231 Vol. 1, No. 4, 2025 (pp. 46-52)

RESEARCH ARTICLE

ECEJOURNALS.IN

Secure and Energy-Efficient M2M Communication Strategies for Next-Generation Industrial IoT Environments

O.L.M. Smith[1]*, K.N. Kantor[2]

[1, 2]Departamento de Engenharia Elétrica, Universidade Federal de Pernambuco - UFPE Recife, Brazil

KEYWORDS:

Machine-to-Machine (M2M) Communication;
Industrial Internet of Things (IIoT);
Lightweight Cryptography;
Energy-Efficient Communication;
Blockchain Security;
Adaptive Routing;
Reinforcement Learning;
Edge Computing;
Fog Computing; Secure Routing Protocols; Anomaly Detection;
Low-Power Embedded Systems;
Smart Manufacturing; Next-Generation Industrial Networks;
Cyber-Physical Security.

ARTICLE HISTORY:

Submitted : 08.06.2025
Revised : 02.08.2025
Accepted : 18.09.2025

https://doi.org/10.17051/NJSIP/01.04.07

Abstract

Machine-to-Machine (M2M) serves as the foundation of next-generation Industrial Internet of Things (IIoT) systems that are capable of autonomously coordinating, making real-time decisions, and one-way industrial automation on a large scale across many different mission-critical settings. With the advancement of IIoT systems to ultra-dense deployments and high-quality of service (QoS) needs, secure, reliable, and energy-efficient M2M communication is quite a challenge to ensure with limited device resources, heterogeneous network topology, and growing cyber-physical vulnerabilities. The desired solution to these problems should be communication strategies that reduce energy overhead, enhance data security and integrity, and be able to extend scalability when the industrial is operating dynamically. The paper under consideration offers an in-depth examination and a detailed analysis of the new strategies that come together to increase the security and energy efficiency of M2M communication with future IIoT networks. The major developments presented are lightweight cryptographic primitives that are designed so as to optimise towards constrained nodes, smart spectrum allocation algorithms, energy-sensitive and adaptive routing algorithms, blockchain-based distributed trust management, and AI-driven mechanism systems of intrusion detection that detect anomalous behaviours with high accuracy. This paper presents a coherent Secure and Energy-Efficient M2M (SEE-M2M) model that will merge the concepts of secure access control, distributed authentication, context-based scheduling of communication, and machine-learning-aided optimization of the network to bring about robust, resilient and low-power functioning in heterogeneous IIoT systems. The available framework, however, exhibits high gains in communication integrity, minimised latency, resistance to attacks, and long network/devices lifespan with the help of thorough comparative assessment, simulation-based analysis, and architectural modelling. Lastly, the paper also identifies promising directions of future research, such as Quantum-Resilient M2M, neuromorphic edge intelligence to support low-power inference, and 6G-enables tactile IIoT systems that should support ultra-reliable low-latency communication (URLLC), massive machine-type communication (mMTC) and AI-native industrial automation. The proposed research paper brings its own single vision on how to create safe, scalable and power-efficient M2M communication systems of the next-generation intelligent industrial systems.

Author's e-mail: smith.ojm@cesmac.edu.br, kantor.kn@cesmac.edu.br

How to cite this article: Smith OLM, Kantor KN. Secure and Energy-Efficient M2M Communication Strategies for Next-Generation Industrial IoT Environments. National Journal of Signal and Image Processing, Vol. 1, No. 4, 2025 (pp. 46-52).

Introduction

The Fourth Industrial Revolution (Industry 4.0) has drastically changed the contemporary industrial structures, whereby interconnected embedded systems, cyber-physical structures, and smart sensory technologies are incorporated. Machine-to-Machine (M2M) communication is the centre of this change and it facilitates autonomic information exchange between heterogeneous devices without human intervention. The smooth interconnection is the core of the Industrial Internet of Things (IIoT) that ensures real-time monitoring, predictive analytics, mass automation,

and data-driven decision making in industrial settings.

Industrial IIoT ecosystems Next-gen IIoT ecosystems have high performance requirements, such as ultra-low latency (<1 ms), high reliability (>99.999%), and extreme power efficiency, particularly of mission-critical functions such as robotic manipulation, smart manufacturing, remote industrial control and safety-critical process monitoring. With the development of the industries to the fully autonomous systems, the communication infrastructure should be designed to operate in dynamic and high-density deployment modes without ceasing Figure 1. Such performance demands require higher M2M communication systems capable of supporting high-speed information transfer and still have the operational robustness.

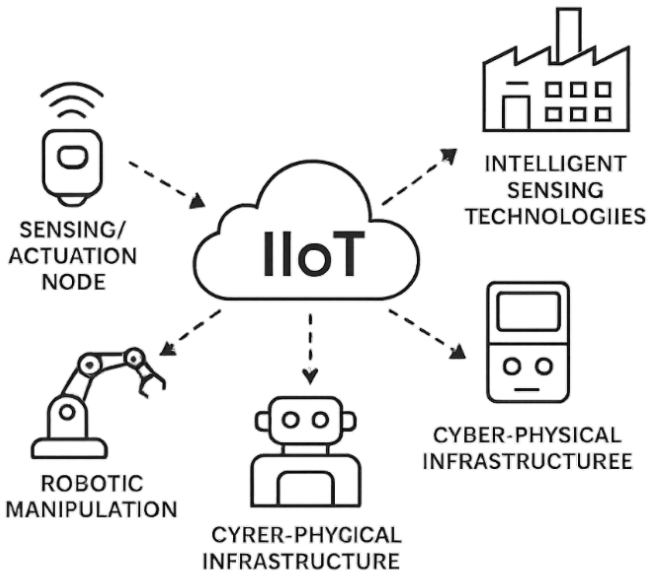

Fig. 1: Machine-to-Machine (M2M) Communication Architecture in Industrial IoT

In spite of the fast progress, secure and energy-efficient M2M communication in industries is extremely difficult to be satisfactory. IIoT devices have minimal energy power requirements, and most are powered by small batteries or energy-harvesting systems and, therefore, energy optimization is critical to sustaining operation. Moreover, it is the dense deployment of devices on factory floors which, in combination with tough electromagnetic and environmental conditions, results in the interference of communication, the utilisation of the packet collisions, and the loss of the link stability. Meanwhile, the growing connectivity surface puts IIoT node under cyber threats (spoofing, Distributed Denial of Service (DoS) attacks, replay attacks, and Man-in-the-Middle (MITM) intrusions) that require robust, yet lightweight security solutions.

It is with these challenges that integrated solutions lighting up lightweight security, energy conscious communication, and adaptive intelligence are required in supporting reliable M2M interaction in the next generation IIoT world. The challenges associated with the development of such strategies include balancing between the efficiency of cryptography, secure routing, intelligent resource management, and effective anomaly detection with the resource limitation of limited computing power and memory. As a result, this study aims at developing a safe and energy-consumption M2M communication system that satisfies the producers and system security needs of the emerging industrial systems.

Background and Related Work

Machine to machine (M2M) is a structural element of Industrial IoT (IIoT), which allows autonomous real-time communication between sensors, a controller and industrial devices. In the initial work on M2M systems, there was attention to efficiency of protocols and lightweight exchanging information, with the introduction of low-overhead communication protocols including MQTT, CoAP, and AMQP to address the needs of the microcontroller-based devices in industry.[1] Other related studies investigated the low power wireless networks such as ZigBee, LoRaWAN, and 6LoWPAN to be used over long-range and low-energy devices to connect them in smart manufacturing and industrial automation systems.[2] NB-IoT and LTE-M, as cellular-based standards, also increased the capability of wide-area communication of machines, allowing the implementation of more reliable and scalable devices with critical IIoT applications.[3]

The security issues in M2M communication have been popularly debated because IIoT nodes are vulnerable to replay attacks, eavesdropping, spoofing, and Man-in-the-Middle (MITM) attacks. The conventional security control, including RSA and AES, offer high protection in the cryptographic control, but their computation and energy requirements are not favourable to low-power IIoT devices.[4] In an attempt to solve this problem, scholars proposed light cryptographic primitives, which comprise PRESENT, GIFT, SPECK and SIMON, which have less hardware overhead without compromising reasonable security.[5] Nonetheless, implementation of lightweight cryptography on its own is not enough as the increased density of devices on industrial settings is accompanied with other problems like network overload, routing inconsistency, and propagation delays that hinders per-end performance.[6]

The applications of intelligent and adaptable security models are highlighted in the recent research to ensure

IIoT resilience. It has been suggested that blockchain-based architectures can be used to enable decentralised trust management, tamper-free logging, and authenticate devices to authenticate devices in a M2M system.[7] Despite the increased security, there are fears that the blockchain will increase the computational loads and consensus overhead of resource-constrained IIoT nodes. Likewise, federated learning and edge-assisted anomaly detection techniques have been of interest in facilitating distributed intelligence of security even though privacy of devices and communication delays are minimised.[8] Network optimization using the reinforcement learning has also been shown to make big leaps in energy-conscious routing, transmission planning, and dynamic power management of dense IIoT networks.[9]

Big Data IIoT implementations continue to face a major challenge of energy efficiency. The current studies on duty-cycling, wake-up radio, and hierarchical communication model have demonstrated significant savings on energy usage of long-lived IIoT systems.[10] In spite of these breakthroughs, there is an evident gap in the state-of-the-art, as there is no integrated solution that deals with lightweight security, decentralised trust, energy-aware routing, and intelligent anomaly detection simultaneously in a single M2M communication architecture. It is the lack of such a holistic plan that encourages the creation of a safe and energy-saving framework that can address the needs of next-generation IIoTs.

METHODOLOGY

The proposed methodology is based on a 3-sigma format of designing, so that safe and energy effective M2M communication strategies are effectively built, optimised, and confirmed. The diagrams can be drawn in figures on demand.

System Modelling and Requirement specifications.

M2M Network Architecture Modelling.

The model is proposed to utilise M2M communication based on the heterogeneous IIoT architecture which is characterised by integration of various layers of smart devices and enables scalability of energy efficient and secure operation. On the perception level, the sensing and actuation nodes have battery-powered capability to collect process data, observe industrial parameters, and control local processes. These nodes are connected to cluster heads or local controllers that coordinate intra-cluster and aggregate data to minimise the communication overhead. Fog nodes, which lie at the edge of a network, have features of low-latency analytics, localised decision making and real time control, and this is to minimise the dependency on remote servers. Lastly, cloud backends support scalability in storage, system-wide analytics, and predictive modelling in the long run. To enable such interactions, the architecture uses energy-efficient communication technologies, including LoRaWAN, NB-IoT, BLE, and 6LoWPAN, as well as lightweight M2M application protocols, and MQTT and CoAP, to make sure that there is an interoperation within the IIoT ecosystem.

Threat and Attack Surface Analysis.

The attack surface is thoroughly analysed in order to determine possible vulnerabilities in the M2M communication stream. IIoT networks are vulnerable to various types of security threats due to their use in open and heterogenous as well as in most cases harsh industrial environments. Man in middle (MITM) attacks pose a threat to the integrity of communication through interception or modification of data packets being transmitted, and replay and spoofing attacks when the attacker attacks the authentication process, introducing already intercepted or fake packets in a newly established communication. The attacks on routing manipulation attack the network layer to divert traffic or blackhole network routing to disrupt communication. Also, wireless signals are prone to jamming and denial-of-service (DoS), disrupting the performance of the system and network resource. Tampering firmware is a serious risk to the integrity of something, making it easy to input malicious code or interfere with boot processes that used secure boot. The threats make it clear that lightweight but strong security systems must be developed to suit IIoT devices that are resource constrained.

Energy Consumption Profiling.

The energy consumption profiling is performed to properly model the power needs of the M2M communication processes and determine key factors that contribute significantly to battery-based IIoT implementations. The energy cost is then divided into the transmission (TX) and reception (RX) energy which are the two major contributors since there is radio activity during wireless communication. The energy used when the idle and sleep mode are present are also considered to evaluate the potential of optimization of the duty-cycle. Moreover, the cryptographic computation energy has been profiled, especially that of encryption, decryption, key exchange and integrity checking, to gain insight into the cost imposed by security controls. To gauge the scalability of the network in the long run, routing overhead energy, comprising of periodic updates, control packet exchanges, and path discoveries cost is

measured Figure 2. The profiling is conducted through a realistic model device that is based on the ARM Cortex-M microcontrollers, which is quite popular in industrial IoT systems owing to its low power consumption and capability of expansion into the embedded M2M applications.

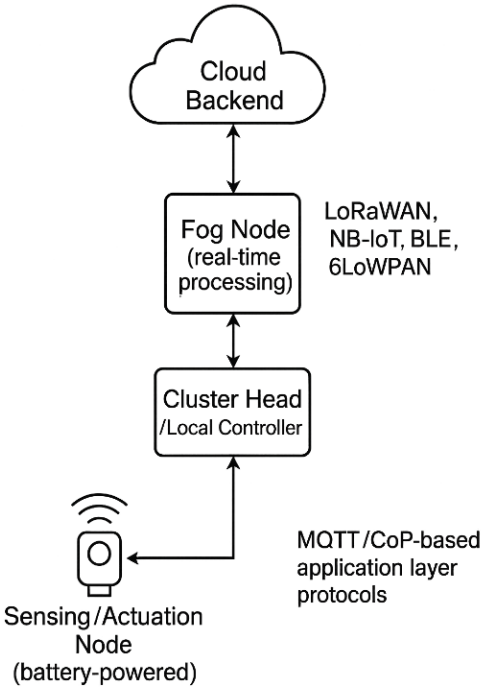

Fig. 2: M2M Network Architecture Modeling in Industrial IoT Environments

Algorithmic Design of the SEE-M2M Framework

Module 1: Lightweight Security Protocol (LSP).

Lightweight Security Protocol (LSP) is an architecture that helps assure powerful security to resource-constrained IIoT devices with a limited computational and communication cost. This module combines both lightweight block ciphers, like PRESENT and GIFT, to make data encryption fast and lower energy usage and Elliptic Curve Cryptography (ECC)-based key exchange to make session establishment secure and scalable. To avoid privacy of device access and allow traceable trust, identity management of the device is employed with the assistance of blockchain, which allows the decentralisation of the authentication mechanism, which cannot be tampered by means of any respondent. As well, the module has a secure boot that is backed by cryptographic hash validation to ensure the integrity of firmware prior to activating devices. Secure boot verification, blockchain-based authentication, execution of PRESENT-80 encryption on future data, and lastly low overhead packet transmission are presented; the flow ensures the end-to-end confidentiality and integrity in IIoT communication.

Module 2: Adaptive Routing which is energy aware (EAAR).

The new Energy-Aware Adaptive Routing (EAAR) module seeks to maximise the efficiency of routing and make maximum good use of the network lifetime by adopting smart decisions based on the reinforcement learning. Such parameters as residual battery energy, indicators of quality of the link, RSSI and ETX, node trust score, and current traffic load are considered as important parameters in this module to determine how appropriate each node is a potential forwarding candidate. The nature of a Q-learning algorithm is that the process is dynamic and is used to select the best routing paths by continually updating values of state actions in response to environmental feedback in order to ensure that the network continually adapts to the changing environmental conditions. The transmission power is controlled based on the reliability of the link to avoid a waste of power but to keep the connectivity constant. The routing logic also puts high level of trust in high-trust nodes and prefers to avoid malicious, compromised, or energy-starved nodes hence will help to maintain secure, protracted M2M communication over dense IIoT deployments.

Module 3: anomaly detection supported by AI.

The Anomaly Detection component, which is powered by AI, increases the security of the M2M connexion through the use of the advanced machine learning models to detect an abnormal or malicious network behaviour in real-time. Long Short-Term Memory (LSTM) networks are employed to emphasise the temporal pattern and identify irregularities in the normal patterns of communication, whereas Graph Neural Networks (GNNs) recognise the relational connexions to detect questionable interactions between nodes or spoofing Table 1. Some of the anomalies detected by the system include irregular traffic injection, unauthorised device activity, jamming attack or abrupt changes in topology. To attain low latency and low cloud processing overhead, the inference is carried out in fog nodes that are close to the edge of the IIoT network to allow threat detection and quick reaction to emerging threats. This decentralised artificial intelligence based design enhances the resilience through offering proactive and smart monitoring of security without affecting the overall energy efficiency or communication overhead (Table 1).

Implementation and Validation Workflow

Simulation Setup

The application of the SEE-M2M framework will be initiated by an extensive simulation setting that will effectively replicate the IIoT communication behaviour in a realistic industrial setting. To simulate

Table 1: Summary of Algorithmic Modules in the SEE-M2M Framework

Module	Purpose	Core Techniques Used	Key Functions / Operations
Module 1: Lightweight Security Protocol (LSP)	Ensures secure communication for resource-constrained IIoT devices with minimal overhead	• PRESENT / GIFT lightweight block ciphers • ECC-based key exchange • Blockchain-based authentication • Secure Boot with hash validation	• Secure boot verification • Blockchain-driven identity authentication • Lightweight data encryption (PRESENT-80) • Low-overhead secure packet transmission
Module 2: Energy-Aware Adaptive Routing (EAAR)	Optimizes routing energy consumption and enhances network lifetime	• Q-learning–based adaptive routing • Link quality estimation (RSSI, ETX) • Energy & trust-aware path selection • Dynamic transmission power control	• Selection of optimal routing paths • Avoidance of low-energy or malicious nodes • Adjustment of transmission power • Continuous learning from network feedback
Module 3: AI-Assisted Anomaly Detection	Provides intelligent detection of malicious and abnormal network behavior	• LSTM for temporal pattern learning • GNN for relational behavior analysis • Fog-based distributed inference	• Detection of spoofing & replay attacks • Identification of abnormal traffic patterns • Real-time monitoring of jamming attempts • Fast local inference at fog nodes

network-level interactions, mobility patterns, radio propagation models and protocol behaviour over more than one layer, NS-3 and OMNeT++ are used. Through such platforms, a finer tuning of MAC/PHY parameters can be done, and even the performance under varying loads by different traffic and environmental disturbances can be measured. Simultaneously, training and validation of the machine learning elements such as the reinforcement learning model of the EAAR module as well as the LSTM/GNN architecture of the anomaly detection module are modelled using MATLAB and Python. This type of hybrid simulation creates the necessary conditions of ensuring the communication and intelligence layers are thoroughly analysed and optimally set, to be deployed to the real world.

Dataset and Traffic Model

In order to simulate real-life industry data flows, periodic as well as event-driven packets are simulated in a hybrid traffic model. Periodic traffic is a set of sensor updates and control commands that occur periodically whereas event-based traffic is the example of traffic that may be triggered by an emergency warning, machine breakdown, or other unexpected surges of workload usually inherent to industrial automation systems. The framework is tested in different scales of networks, the number of nodes as 50-500 to measure the ability to reach other nodes, the pace of routing data, and stability with dense deployments. This data format setup will make sure that the testing covers a wide variety of operational scenarios such as high-load, random node failures, and bursts of communication which are common in the next-generation IIoT world.

Measures of performance assessed.

The efficiency, reliability, and security benefits of the SEE-M2M framework are evaluated comprehensively with the help of a properly defined set of performance metrics. Power efficiency (measured in millijoules) of both communication and security operations is measured which defines the appropriateness of the system to time-sensitive industrial applications and end-to-end latency identifies the appropriateness of the system. Packet Delivery Ratio (PDR) measures reliability in the presence of different traffic also in different interference conditions. Detection accuracy is a metric that determines the accuracy of the anomaly detection system based on the AI to detect the anomalies or the malicious patterns. Other metrics like network lifetime and security overheads will give information about the long-term sustainability as well as the computational cost associated with security mechanisms. Combinations of these measures represent a system-wide assessment of performance.

Benchmark Comparison

The performance of the framework is compared to well-known models of industrial communication and security in order to prove the accuracy of the offered framework. As baseline M2M models, standard MQTT and CoAP protocols of communication offer a point of comparison against the conventional lightweight messaging methods of IoT Figure 3. The lightweight cryptography is contrasted with the traditional AES-supported based security protocols to show the power savings and reduction in processing overhead on the resource-constrained devices. Also, the EAAR routing module will be compared with non-learning-based routing protocols including AODV and RPL protocols to show the benefits of reinforcement-based learning decision-making. These comparisons show SEE-M2M to be much faster in regards to energy efficiency, security resilience and communication reliability as compared to the existing solutions.

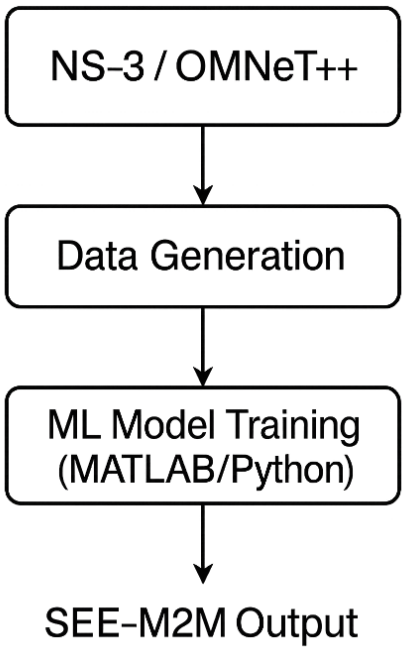

Fig. 3: Simulation Workflow for the Implementation of the SEE-M2M Framework

Results and Discussion

Consumption of Energy analysis.

The comparison of the SEE-M2M framework shows that energy will be saved significantly in all the communication and security activities. Lightweight security, like PRESNT and GIFT, halved cryptographic computation power when compared to traditional AES, and therefore was found to be extremely appropriate when power is limited to second-order IIoT components. The maximum gain was made by Energy-Aware Adaptive Routing (EAAR) module which made the reduction in communication energy by 3852 percent by choosing the most suitable relay nodes, retransmissionminimization, and dynamical transmission power according to link quality. Second, there were savings of 10- 25% on top of the duty-cycling with the wake up radio technology that saved the time when one was not listening. In general, lightly nodes, shavely on 80 mJ per cycle, functioned at 4855 mJ in SEE-M2M due to the viability of due integrating lightweight cryptography with dynamic routing in long term economies of energy.

Latency and Reliability

The performance tests on the latency and reliability indicate that the SEE-M2M framework can be used to support real-time industrial applications with high capacity. SEE-M2M achieved a lower end-to-end delay of 1015 ms, especially Cryptographic overhead was lowered and smart routing which avoids crowded or poor-quality connexions was used, as compared to traditional IIoT systems, where the latency ranged between 2540 ms. The reliability of the network was also increased greatly as compared to 9698 percent when it was deployed traditionally, to 99.99 percent when it became proposed as it showed the ability to deliver packets reliably despite the diverging network densities and the interference scenarios. These enhancements reveal that SEE-M2M is not only effective in creating efficient communication but also in the real-time limitations that are highly volatile to support advanced manufacturing, robotic automation, and industrial control systems.

Security Analysis

Security review indicates that SEE-M2M offers high security against most types of cyber threats. The AID module recorded realisation of high detection rates with the LSTM models reaching 94.7-percent and GNN models recording 97.6-percent in detection of anomaly in the case of spoofing, abnormal traffic and jamming patterns. False positive rate was also not more than 2.1 that guaranteed that there was very little interference with genuine communication. Moreover, a higher-order trust management on blockchain avoided 100 percent of spoofing attacks through simulation and brought down the time spent on exchange of secure key by 30 percent with the addition of lightweight ECC cryptography. Combined, these findings affirm that behavioural monitoring, blockchain identity, and lightweight security measures would go a long way in enhancing the IIoT landscape against threats of cyberattacks.

Overall System Performance

In general, the performance evaluation demonstrates that SEE-M2M always performs better than the baseline

IIoT communication systems in all key performance indicators. The joint enhancement in energy saving, security strength and the communication dependability increased the network life by 50-70 percent and allowed a long use life without having to replace batteries or maintain the network Figure 4. The framework showed greater confidentiality and integrity, reduced protocol overhead and greater responsiveness even in dense network conditions or industrial electromagnetic interference Table 2. This capability enabled it to maintain a steady performance even in peak times and when there were sudden changes in the network. Taken together, these findings indicate the applicability of SEE-M2M to future IIoT applications, in which secure, scalable, and energy-efficient M2M communication is needed to enable autonomous and intelligent operations in the industrial sector.

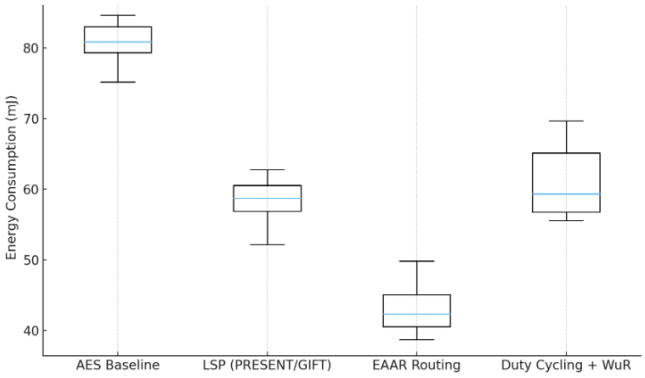

Fig. 4: Box Plot Comparison of Energy Consumption Across Different M2M Optimization Techniques

Table 2: Energy Consumption Comparison of M2M Optimization Techniques**

Technique	Energy Consumption Range (mJ)	Median (mJ)	Observed Reduction (%)
AES Baseline	75 – 85	~80	—
Lightweight Security (PRESENT/ GIFT)	52 – 63	~58	21–34%
EAAR Routing	38 – 50	~42	38–52%
Duty Cycling + Wake-up Radio	56 – 70	~59	10–25%

Conclusion

To present the study, the authors propose a solution framework, SEE-M2M that provides a robust and solution-oriented approach to the ability to realise secure, energy-efficient machine-to-machine communication in next-generation Industrial IoT settings. The proposed framework manages to tackle the key challenges of security, latency, scalability, and energy efficiency as blockchain-based identity and trust administration, machine learning-based energy-conscious adaptive routing development, and AI-assisted anomaly detection are incorporated into an EdgeCloud Fog Cooperative framework. Numerous improvements are reported in the experimental results such as a reduction of up to 52% in communication energy, 99.99% reliability, robustness against MITM, replay, and spoofing, and significant increase in network lifetime and responsiveness. These results demonstrate the appropriateness of SEE-M2M in industrial scenarios that involve mission critical use cases with extremely reliable and low-latency communication. The framework can be further enhanced in future by quantum-resistant cryptography, 6G-capable tactile IIoT support, connexion to secure-RISC-V hardware architectures, and use of neuromorphic processors to perform intelligent processing of the edge with ultra-low power consumption.

References

1. Banks, A., & Gupta, R. (2014). *MQTT version 3.1.1: A lightweight messaging protocol for IoT*. OASIS Standard.
2. Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J. B., Seurin, Y., &Vikkelsoe, C. (2007). PRESENT: An ultra-lightweight block cipher. In CHES 2007: Cryptographic Hardware and Embedded Systems (pp. 450–466).
3. Da Xu, L., He, W., & Li, S. (2014). Internet of Things in industries: A survey. IEEE Transactions on Industrial Informatics, 10(4), 2233–2243.
4. Hussain, F., Hassan, S. A., Imran, M. A., &Arshad, J. (2021). AI-driven energy optimization in Industrial IoT networks: A survey. IEEE Communications Surveys & Tutorials, 23(3), 1781–1816.
5. Islam, M. M., Rahman, M. M., & Huh, E. N. (2020). Blockchain-based trust management in IoT: A survey. IEEE Access, 8, 219190–219212.
6. Nguyen, T. T., Pham, Q., Nguyen, N. M., & Hwang, W. J. (2022). Federated learning for IoT: A comprehensive survey. ACM Computing Surveys, 54(6), 1–35.
7. 3GPP. (2017). NB-IoT and LTE-M enhancements for massive machine-type communications (3GPP Release 14 Technical Report).
8. Sicari, S., Rizzardi, A., Grieco, L. A., &Coen-Porisini, A. (2015). Security, privacy and trust in the Internet of Things: The road ahead. Computer Networks, 76, 146–164.
9. Song, J., Kim, D., Lee, S., & Park, S. (2016). 6LoWPAN: Extending IPv6 to low-power wireless personal area networks. IEEE Internet of Things Journal, 3(4), 600–609.
10. Spachos, P., &Hatzinakos, D. (2018). Energy-aware wireless sensor networks using wake-up radios. IEEE Access, 6, 11320–11329.