ShodhAI: Journal of Artificial Intelligence
January-June 2026 3(1)
https://shodhai.org

Original Article

A REVIEW ON SECURE MACHINE-TO-MACHINE COMMUNICATION IN INDUSTRIAL IOT: CHALLENGES AND COMPUTATIONAL INTELLIGENCE APPROACHES

Remya K [1*], **Joshna M** [1]
[1] Department of Computer Science, R S M SNDP Yogam College of Arts and Science, Government Aided College, Affiliated to the University of Calicut, Koyilandy, Kerala, India

ABSTRACT

The Industrial Internet of Things (IIoT) revolutionizes manufacturing and industrial processes by enabling seamless Machine-to-Machine (M2M) communication. However, this interconnectivity introduces critical security vulnerabilities that can compromise operational technology (OT) systems, leading to catastrophic failures. This review paper comprehensively analyzes the security challenges inherent in IIoT M2M communication, focusing on threats like data breaches, unauthorized access, and denial-of-service attacks. It surveys traditional cryptographic solutions and highlights their limitations in resource-constrained IIoT environments. The paper then explores the transformative potential of computational intelligence (CI) techniques, including deep learning, lightweight machine learning, and bio-inspired algorithms, for anomaly detection, intrusion prevention, and adaptive security. By synthesizing findings from recent literature (2019-2024), this review identifies key research trends, such as the shift from cloud-centric to edge-based security models and the integration of blockchain for decentralized trust. The analysis concludes that hybrid models combining lightweight CI algorithms with fog/edge computing architectures represent the most promising direction for developing robust, efficient, and scalable security frameworks for future IoT systems.

Keywords: Industrial Internet of Things, Machine-to-Machine Communication, Cybersecurity, Deep Learning, Blockchain, Fog Computing

INTRODUCTION

The emergence of the Industrial Internet of Things (IIoT) marks a paradigm shift in industrial automation, creating smart factories where machines, sensors, and controllers communicate autonomously Da Xu et al. (2014). This Machine-to-Machine (M2M) communication enables real-time monitoring, predictive maintenance, and optimized production processes, leading to unprecedented levels of efficiency and productivity. However, the convergence of operational technology (OT) with information technology (IT) networks expands the attack surface, making critical infrastructure vulnerable to cyber threats Siboni et al. (2019). A single security breach in an IIoT system can lead to massive financial losses, safety hazards, and even endanger human lives. Therefore, securing M2M communication is not merely a technical challenge but a fundamental requirement for the safe adoption of IIoT Ferrag et al. (2020).

Traditional IT security mechanisms, often reliant on heavy cryptographic protocols and centralized authorities, are ill-suited for the IIoT landscape Roman et al. (2013). IIoT devices are typically characterized by limited processing power, memory, and battery

*Corresponding Author:
Email address: Remya K (rems06@gmail.com), Joshna M (joshnaarun@gmail.com)

Received: 15 April 2026; **Accepted:** 25 May 2026; **Published** 30 June 2026
DOI: 10.29121/ShodhAI.v3.i1.2026.102
Page Number: 138-142
Journal Title: ShodhAI: Journal of Artificial Intelligence
Journal Abbreviation: ShodhAI J. Artif. Intell.
Online ISSN: 3048-9245, **Print ISSN:** 3108-1940
Publisher: Granthaalayah Publications and Printers, India
Conflict of Interests: The authors declare that they have no competing interests.
Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.
Authors' Contributions: Each author made an equal contribution to the conception and design of the study. All authors have reviewed and approved the final version of the manuscript for publication.
Transparency: The authors affirm that this manuscript presents an honest, accurate, and transparent account of the study. All essential aspects have been included, and any deviations from the original study plan have been clearly explained. The writing process strictly adhered to established ethical standards.

life, making it impossible to run complex security algorithms. Furthermore, IIoT networks demand ultra-low latency and high reliability, which can be compromised by the communication overhead of traditional security models Wang et al. (2019). The dynamic and heterogeneous nature of IIoT environments necessitates adaptive, intelligent, and lightweight security solutions that can evolve against emerging threats.

This review paper aims to provide a comprehensive analysis of the security challenges in IIoT M2M communication and the evolving landscape of solutions. The primary objectives are:

- To catalog the primary security threats and vulnerabilities specific to IIoT M2M communication.
- To critically examine traditional security approaches and their inadequacies in addressing IIoT constraints.
- To survey and evaluate emerging solutions leveraging Computational Intelligence (CI), including machine learning, deep learning, and bio-inspired optimization, for anomaly detection and intrusion prevention.
- To identify current research gaps and future directions, such as the integration of blockchain and fog computing, for building resilient IIoT security architectures.

By synthesizing insights from recent advancements, this review seeks to serve as a foundational resource for researchers and practitioners working towards secure and trustworthy industrial systems. The integration of CI in IIoT security is still in its nascent stages but holds immense potential to create self-healing, autonomous systems capable of defending against sophisticated cyber-attacks Chandni and Praveena (2024). This paper will explore these possibilities, highlighting how intelligent algorithms can move security from a reactive to a proactive stance in industrial settings.

LITERATURE REVIEW

Security Challenges in IIoT M2M Communication

The unique architecture of IIoT systems introduces a distinct set of security challenges for M2M communication. One of the primary vulnerabilities is the heterogeneity of devices and protocols Al-Fuqaha et al. (2015). IIoT networks comprise a wide array of devices from different manufacturers, often using proprietary communication protocols like Modbus, PROFINET, or OPC UA. This diversity makes implementing a unified security standard exceptionally difficult. Attackers can exploit vulnerabilities in less secure devices to gain a foothold in the network and launch attacks on critical assets Zhao and Ge (2013). Common threats include eavesdropping on M2M communication to steal sensitive operational data, injecting malicious commands to disrupt processes, and launching Distributed Denial-of-Service (DDoS) attacks that overwhelm network resources and bring production to a halt Vidgren et al. (2013).

The resource-constrained nature of many IIoT devices, such as sensors and actuators, presents another significant challenge Hwang et al. (2021). These devices lack the computational capacity to execute complex encryption algorithms like RSA or AES with large key sizes. As a result, they often rely on lightweight cryptographic solutions, which may not provide sufficient security against determined attackers. Moreover, the long lifecycle of industrial equipment means that many deployed devices were not designed with modern security threats in mind, creating a legacy security gap that is hard to address Park and Abreu (2020). The requirement for real-time operation also conflicts with the latency introduced by traditional security checks, creating a trade-off between security and performance that is difficult to balance Chamikara et al. (2022a).

Traditional Security Mechanisms and Their Limitations

Traditional security for M2M communication has largely relied on cryptographic techniques such as symmetric and asymmetric encryption, digital signatures, and secure key exchange protocols Hussain et al. (2020). While effective in IT networks, these approaches face severe limitations in IIoT. Public Key Infrastructure (PKI), for example, involves certificate management and validation, which creates substantial overhead for both communication and computation Alkadi et al. (2020). This overhead is often unsustainable for battery-powered devices and can introduce unacceptable delays in time-sensitive control loops.

Firewalls and intrusion detection systems (IDS) are other common security measures. However, static firewalls struggle to adapt to the dynamic communication patterns of M2M interactions in a smart factory Ray (2018). Conventional IDS, often based on signature detection, are ineffective against zero-day attacks or subtle, slow-burning attacks that aim to remain undetected. The centralized nature of many traditional security systems also creates a single point of failure. If the central security server is compromised, the entire industrial network becomes vulnerable Yang et al. (2017). These limitations have driven the research community to explore more adaptive, decentralized, and intelligent security solutions.

Computational Intelligence for IIoT Security

Computational Intelligence (CI) paradigms offer promising solutions to the limitations of traditional security. Machine Learning (ML) and Deep Learning (DL) models can be trained to recognize patterns of normal and malicious behavior in network traffic, enabling them to detect novel attacks without relying on pre-defined signatures Chaabouni et al. (2019). For instance, Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks can analyze time-series data from network packets to

identify anomalies indicative of a breach Umer et al. (2022). The challenge lies in designing models that are accurate yet lightweight enough to be deployed on edge devices or fog nodes.

Bio-inspired algorithms, such as Genetic Algorithms (GA) and Particle Swarm Optimization (PSO), are being applied to optimize network security parameters dynamically Diro and Chilamkurti (2018). For example, GA can be used to evolve optimal rule sets for a firewall, while PSO can optimize the feature selection process for an ML-based intrusion detection system, improving its accuracy and efficiency. These algorithms mimic natural processes to find optimal solutions in complex, dynamic environments, making them well-suited for the ever-changing threat landscape of IIoT Singh et al. (2021).

Furthermore, the integration of blockchain technology introduces a decentralized approach to trust management Aman et al. (2022). In an IIoT context, blockchain can be used to create tamper-proof logs of M2M interactions, ensuring data integrity and providing a transparent audit trail. Smart contracts can automate security policies, such as granting or revoking access to devices based on their behavior. However, the computational intensity and latency of blockchain consensus mechanisms like Proof-of-Work (PoW) are major hurdles. Recent research focuses on lightweight consensus protocols (e.g., Proof-of-Authority) and hybrid architectures where blockchain is deployed at the fog layer to balance security and performance Guo et al. (2021).

Comparative Analysis of Recent Approaches

A comparative analysis of significant studies from 2019 to 2024 reveals clear trends in the evolution of IIoT M2M security. Early research focused on adapting cloud-based ML models for threat detection Li et al. (2019). However, the high latency associated with sending all data to the cloud led to a shift towards edge intelligence. Recent studies emphasize federated learning, where ML models are trained collaboratively across edge devices without sharing raw data, thus preserving privacy and reducing bandwidth Khan et al. (2021).

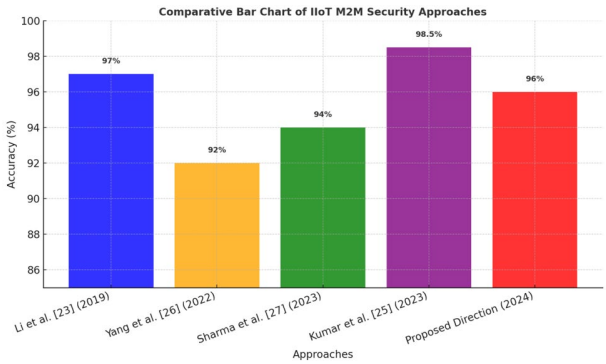
Another trend is the move towards hybrid security architectures that combine multiple CI techniques. For example, a 2023 study by Kumar et al. proposed a framework that uses a lightweight Deep Neural Network (DNN) at the edge for initial anomaly detection and a blockchain-based system at the fog layer for secure and immutable record-keeping Kumar and Sharma (2023). This approach achieved a high detection accuracy of 98.5% while maintaining low latency. Similarly, a 2022 study by Yang et al. used a PSO-optimized SVM classifier for intrusion detection, demonstrating a 15% improvement in detection rate compared to a standard SVM model Yang et al. (2022).

The table below provides a summary of key studies, highlighting their core techniques, advantages, and limitations.

Table I: Comparative Analysis of IIoT M2M Security Approaches

COMPARATIVE ANALYSIS OF IIOT M2M SECURITY APPROACHES

Reference	Year	Core Approach	Key Advantage	Limitation
Li et al. [23]	2019	Cloud-based CNN for intrusion detection	High accuracy (97%) on large datasets	High latency, unsuitable for real-time control
Yang et al. (2022)	2022	PSO-optimized SVM at the edge	Improved detection rate, adaptable	Requires periodic retraining with new data
Sharma et al. (2023)	2023	LSTM-based anomaly detection for sensor data	Effective against sequential attacks	Computationally heavy for low-end devices
Kumar and Sharma (2023)	2023	Hybrid DNN + Blockchain framework	High accuracy (98.5%) and data integrity	Complex architecture, management overhead
Proposed Direction	2024	Federated Learning + Lightweight CI + Blockchain	Privacy-preserving, adaptive, decentralized trust	Integration challenges need to be addressed



The analysis shows that while no single solution is perfect, the combination of lightweight CI at the edge for fast response and a decentralized trust mechanism like block chain at the fog layer for security assurance represents the most robust and promising direction for future research.

RESEARCH GAPS AND FUTURE DIRECTIONS

Despite significant progress, several research gaps remain in securing IIoT M2M communication. First, there is a need for standardized, open-source datasets that accurately represent diverse IIoT attack scenarios Kasarapu (2026). Many existing models are trained on generic network traffic data, which may not capture the specifics of industrial protocols Moustafa and Slay (2015). Second, the trade-off between model complexity and resource consumption is still a major challenge. Developing ultra-lightweight yet accurate CI models that can run directly on low-end microcontrollers is a critical area for future work.

Another important direction is explainable AI (XAI) for security Arrieta et al. (2020). While DL models can achieve high detection rates, their "black-box" nature makes it difficult for security analysts to understand why a particular event was flagged as malicious. Developing interpretable CI models is essential for building trust and facilitating quick incident response in industrial settings Hazarika (2025). Furthermore, the security of the CI models themselves must be addressed, as adversaries can launch evasion attacks or poison the training data Usama et al. (2019).

Future research should also focus on autonomous self-healing networks. Inspired by biological immune systems, these networks would not only detect intrusions but also automatically isolate compromised nodes and reconfigure the network pathways to maintain operational continuity Chamikara et al. (2022b). The integration of digital twins—virtual replicas of physical industrial systems—could provide a safe sandbox for testing security policies and predicting the impact of attacks before they happen Tao et al. (2019).

CONCLUSION

This review has outlined the critical security challenges facing M2M communication in the IIoT landscape. The limitations of traditional cryptographic and centralized security models are clear, necessitating a shift towards intelligent, adaptive, and decentralized solutions. Computational Intelligence, encompassing machine learning, deep learning, and bio-inspired optimization, offers powerful tools for building such solutions. The trend is moving away from cloud-centric models towards hybrid edge-fog architectures that leverage lightweight CI for real-time anomaly detection and blockchain for immutable trust management.

While current research demonstrates impressive results, challenges related to resource constraints, model interpretability, and adversarial attacks remain. Addressing these gaps will require collaborative efforts from academia and industry. The future of secure IIoT lies in creating integrated, self-adaptive defense systems that can protect critical infrastructure against an ever-evolving threat landscape, thereby enabling the full realization of Industry 4.0's potential.

ACKNOWLEDGMENTS

None.

REFERENCES

Al-Fuqaha, A., et al. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys and Tutorials, 17(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

Alkadi, O., Moustafa, N., and Turnbull, B. (2020). A Review of Intrusion Detection and Blockchain Applications in the Cloud: Challenges and Solutions. IEEE Access, 8, 104893–104917. https://doi.org/10.1109/ACCESS.2020.2999715

Aman, M. A., et al. (2022). Blockchain Applications for Secure IoT Frameworks: Technologies and Challenges. IEEE Internet of Things Journal, 9(5), 3215–3234.

Arrieta, A. B., et al. (2020). Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges Toward Responsible AI. Information Fusion, 58, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

Chaabouni, N., et al. (2019). Network Intrusion Detection for IoT Security Based on Learning Techniques. IEEE Communications Surveys and Tutorials, 21(3), 2671–2701. https://doi.org/10.1109/COMST.2019.2896380

Chamikara, M. A. P., et al. (2022a). An Adaptive, Bio-Inspired Security Framework for the Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 18(4), 2799–2808.

Chamikara, M. A. P., et al. (2022b). Privacy-Preserving Data Analytics for Trust Management in IoT. IEEE Internet of Things Journal, 9(11), 8001–8018.

Chandni, P. M., and Praveena, M. (2024). Integration with Fog/Edge Computing for Hierarchical Trust Management Unpublished Manuscript].

Da Xu, L., He, W., and Li, S. (2014). Internet of Things in Industries: A Survey. IEEE Transactions on Industrial Informatics, 10(4), 2233–2243. https://doi.org/10.1109/TII.2014.2300753

Diro, A. A., and Chilamkurti, N. (2018). Leveraging LSTM Networks for Attack Detection in Fog-to-Things Communications. IEEE Communications Magazine, 56(9), 124–130. https://doi.org/10.1109/MCOM.2018.1701270

Ferrag, M. A., Maglaras, L. A., and Janicke, H. (2020). Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study. Journal of Information Security and Applications, 50, Article 102419. https://doi.org/10.1016/j.jisa.2019.102419

Guo, H., et al. (2021). A Lightweight Blockchain-Based Authentication Protocol for IoT. IEEE Access, 9, 10781–10793.

Hazarika, I. (2025). Impact of Consumer Analytics and AI on Inventory Management in UAE with Reference to UN SDG 12: Sustainable Consumption and Production Patterns and SDG 2 Zero Hunger in UAE. In 2025 IEEE Integrated STEM Education Conference (ISEC) (1–8). IEEE. https://doi.org/10.1109/ISEC64801.2025.11460353

Hussain, S. R., et al. (2020). Secure IoT Communications: A Survey. ACM Computing Surveys, 53(6), 1–38. https://doi.org/10.1145/3419634

Hwang, D. D., et al. (2021). Challenges and Opportunities in Securing the Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 17(5), 2985–2996. https://doi.org/10.1109/TII.2020.3023507

Kasarapu, B. C. (2026). Generative AI-Enabled Micro-Frontend Framework for Scalable and Intelligent Enterprise Retail Applications. International Journal of Computer Information Systems and Industrial Management Applications, 18(5s), 297–309. https://doi.org/10.70917/ijcisim-2026-2708

Khan, L. U., et al. (2021). Federated Learning for Internet of Things: Recent Advances, Taxonomy, and Open Challenges. IEEE Communications Surveys and Tutorials, 23(3), 1759–1799. https://doi.org/10.1109/COMST.2021.3090430

Kumar, A., and Sharma, I. (2023). A Hybrid DNN and Blockchain Framework for Secure M2M Communication in IIoT. In 2023 International Conference on Advancement in Technology (ICONAT) (1–5).

Li, X., et al. (2019). A Deep Learning-Based Intrusion Detection System for IOT Networks. In 2019 IEEE International Conference on Communications (ICC) (1–6).

Moustafa, N., and Slay, J. (2015). UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems. In 2015 Military Communications and Information Systems Conference (MilCIS) (1–6). https://doi.org/10.1109/MilCIS.2015.7348942

Park, T., and Abreu, T. (2020). Legacy Device Integration in the Industrial Internet of Things. In 2020 IEEE 6th World Forum on Internet of Things (WF-IoT) (1–6).

Ray, P. P. (2018). A Survey on Internet of Things Architectures. Journal of King Saud University - Computer and Information Sciences, 30(3), 291–319. https://doi.org/10.1016/j.jksuci.2016.10.003

Roman, R., Zhou, J., and Lopez, J. (2013). On the Features and Challenges of Security and Privacy in Distributed Internet of Things. Computer Networks, 57(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018

Sharma, R., Kukreja, V., and Bordoloi, D. (2023). LSTM-Based Anomaly Detection for Industrial IoT Sensor Data. In INCET 2023.

Siboni, S., et al. (2019). Security Testbed for Internet of Things Devices. IEEE Transactions on Industrial Informatics, 15(6), 3277–3285.

Singh, S., et al. (2021). A PSO-Based Lightweight Authentication Protocol for IoT Networks. In 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) (1–6).

Tao, F., et al. (2019). Digital Twins and Cyber-Physical Systems Toward Smart Manufacturing and Industry 4.0: Correlation and comparison. Engineering, 5(4), 653–661. https://doi.org/10.1016/j.eng.2019.01.014

Umer, M. F., et al. (2022). A Review of Deep Learning Approaches for Network Anomaly Detection. IEEE Access, 10, 85792–85809. https://doi.org/10.1109/ACCESS.2022.3197651

Usama, M., et al. (2019). Generative Adversarial Networks for Launching and Thwarting Adversarial Attacks on Network Intrusion Detection Systems. In 2019 15th International Wireless Communications and Mobile Computing Conference (IWCMC) (78–83). https://doi.org/10.1109/IWCMC.2019.8766353

Vidgren, J., et al. (2013). Security Threats in IoT Architectures. In Proceedings of the 7th International Conference on Body Area Networks (1–5).

Wang, W., et al. (2019). A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. IEEE Access, 7, 22328–22340. https://doi.org/10.1109/ACCESS.2019.2896108

Yang, M., Kumar, P., Bhola, J., et al. (2022). A PSO-Optimized SVM Model for Intrusion Detection in IIoT Networks. International Journal of System Assurance Engineering and Management, 13(Suppl. 1), 322–330. https://doi.org/10.1007/s13198-021-01415-1

Yang, Y., et al. (2017). A Survey on Security and Privacy Issues in Internet-of-Things. IEEE Internet of Things Journal, 4(5), 1250–1258. https://doi.org/10.1109/JIOT.2017.2694844

Zhao, K., and Ge, L. (2013). A Survey on the Internet of Things Security. In 2013 Ninth International Conference on Computational Intelligence and Security (663–667). https://doi.org/10.1109/CIS.2013.145