International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 14, Issue 8, August 2025)

A Review on Cognitive Machine Learning for Cybersecurity Systems in Operational Technology Networks

Mustafa Emre Cansev[1], Hüseyin Canbolat[2]

[1]*Ankara Yildirim Beyazit University & Ankara Yıldırım Beyazıt Üniversitesi Esenboğa Külliyesi Esenboğa/ANKARA*
[2]*Ankara Yildirim Beyazit University & Ankara Yıldırım Beyazıt Üniversitesi Esenboğa Külliyesi Esenboğa/ANKARA*

[1]memrecansev@gmail.com
[2]huseyin.canbolat@aybu.edu.tr

***Abstract*— In Manufacturing Technologies (OT), with the advent of Industry 4.0, Human-Machine Interaction (HMI) has evolved into Machine-Machine Interaction (MMI). This development has made the digitalization of manufacturing processes critical. The combined use and digitalization of machine, HMI, and MMI systems has also raised significant cybersecurity challenges.**

Because manufacturing technology networks lack a standardized structure, traditional security mechanisms are often inadequate to address the heterogeneity and time-sensitive nature of these environments. Therefore, systematic, adaptive, and learning-based solutions are required to provide resilient protection mechanisms in OT networks. In this context, unlike traditional approaches, cognitive machine learning offers systems that can dynamically adapt learning processes by understanding environmental data. Combining adaptive reasoning and contextual awareness, cognitive learning enables OT networks to identify new attack patterns and respond in real time, increasing their resilience and providing more effective security solutions.

This article systematically reviews scientific publications on the use of cognitive machine learning in manufacturing technology networks. Focusing on recent contributions (2016–2025), the review highlights both the novelty and practical importance of applying cognitive machine learning to OT security challenges. The reviewed literature highlights that the use of cognitive machine learning for security purposes in OT networks has so far been largely limited to subsystem-level applications (e.g., PLCs, SCADA nodes, and IoT-enabled manufacturing devices). Furthermore, an end-to-end solution architecture has been lacking. This finding reveals a clear research gap and highlights the potential of cognitive machine learning methods as a promising and relevant topic for future academic and industrial research.

***Keywords*—Cognitive Machine Learning, Operational Technology Networks, Industrial Control Systems, Industrial Cyber Security, ioT.**

I. INTRODUCTION

During the Second Industrial Revolution, which began in 1870, computer systems were not yet used in production. However, with the Third Industrial Revolution, computer technologies rapidly entered the market and began to be integrated into industrial systems. The Fourth Industrial Revolution marked a new phase in which production tools and computer controls became inseparable, merging the cyber and physical domains. This integration played a significant role in the simultaneous growth of both production capacity and capital systems.

As production technologies advanced, the reliance on electronic and digital systems increased, enabling faster and more efficient production processes. However, this rapid digitalization also introduced significant security vulnerabilities. The interconnection of production systems via networks expanded the potential attack surface, creating new avenues for cybercriminals. Modern attackers often use ransomware or denial-of-service (DoS) techniques to disable systems and demand payment in exchange for the restoration of normal operations. As a result, a production system exposed to cyberattacks faces not only serious financial losses but also repetitional and operational damage, highlighting the critical importance of cybersecurity in Operational Technology (OT) networks. Availability, integrity, and confidentiality are three key priorities in production management systems [1]. However, with the rise of cyberattacks targeting Industrial Internet of Things (IIoT) and Industry 4.0 systems, confidentiality

and security have become even more crucial in OT environments compared to traditional Information Technology (IT) systems. At the same time, uninterrupted operational availability remains a crucial requirement.

Therefore, cybersecurity measures must be implemented to provide robust protection without compromising the continuity and efficiency of production systems.

Industrial controller suppliers have developed proprietary protocols specifically designed for production environments. These protocols typically prioritize efficiency through raw data communication, but such design choices also introduce vulnerabilities related to data security and transmission integrity. Efforts to address these issues include developing secure communication channels between devices and within device architectures. However, traditional protocols alone are not sufficient to mitigate increasingly complex cyber threats.

In contrast, machine learning (ML) techniques have emerged as a way to strengthen cybersecurity in OT systems. Among these, cognitive machine learning has emerged as a particularly promising approach because it provides advanced analysis capabilities, supports adaptive decision-making, and improves anomaly detection in complex industrial environments.

This study focuses on scientific research examining the applications of cognitive machine learning in OT networks.

The structure of this article is as follows:

- Section 2 outlines the research methodology and literature selection criteria.

- Section 3 provides a comprehensive literature review on the use of cognitive machine learning in OT networks.

-Section 4 discusses the findings and their implications.

- Section 5 concludes with key insights and highlights potential directions for future research.

II. Methodology

This study uses a systematic literature review approach to identify and analyze research on the use of cognitive machine learning in Operational Technology (OT) networks. The methodology includes keyword selection, database querying, and application of defined inclusion and exclusion criteria.

A. *Keyword Selection*

Keywords were derived from the core concepts of the study, with an emphasis on cognitive machine learning, cybersecurity, and operational technology (OT) systems. The following keyword combinations were used during the search process:

"Cognitive machine learning" AND "operational technology", "Cognitive computing" AND "OT networks""Machine learning" AND "industrial control systems" AND "cognitive", "Cybersecurity" AND "OT" AND "cognitive machine learning", "Intelligent machine learning" AND "IIoT", "Cognitive algorithms" AND "optimization" AND "operational technology", "Smart manufacturing" AND "cognitive machine learning".

B. Data Sources

The literature review was conducted using reputable and peer-reviewed scientific databases, namely IEEE Xplore, Web of Science, and ScienceDirect. These platforms were selected because they provide comprehensive coverage of publications in engineering, industrial systems, and cybersecurity.

C. *Inclusion and Exclusion Criteria*

To ensure the relevance and quality of the selected studies, the following criteria were applied:

Inclusion Criteria:

- Direct relevance to OT networks
- Use of cognitive or advanced machine learning techniques
- Relevance to cybersecurity, network architecture, or production devices

Exclusion Criteria:

- Studies focusing exclusively on traditional IT systems
- Research limited to conventional machine learning without cognitive aspects
- Publications lacking practical application (purely theoretical work without implementation).

D. Selection Process

An initial pool of 143 publications was identified. After screening based on titles and abstracts, 48 articles were selected for full-text review. Among these, studies that emphasized end-to-end OT networks and real-

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 14, Issue 8, August 2025)

world industrial applications were prioritized in the content analysis stage.

E. Research Objective

The main objective of this methodology is to present the current state of cognitive machine learning applications in OT environments, highlight emerging research directions, and identify gaps in the literature that can guide future investigations.

III. Literature Review

Operational Technologies (OT) is a rapidly developing field in recent years. While hardware manufacturers aim to be among the leading competitors in the market in this field, standards have also begun to be created through universities. However, since the field is very wide and there are few systems that have proven themselves in terms of hardware, this slows down the process. Some institutions design their systems as IT systems, while others try to standardize their business plans as much as possible.

The integration of Cognitive Machine Learning (CML) into Operational Technology (OT) networks has become a critical research area due to the increasing complexity and importance of OT systems in modern industries. This section presents a comprehensive review of the relevant scientific publications from the 1980s to the present. The goal is to examine how CML has developed and been applied in OT networks, the challenges encountered, as well as identify research gaps and future directions. The number of publications by year is given in Figure 1.

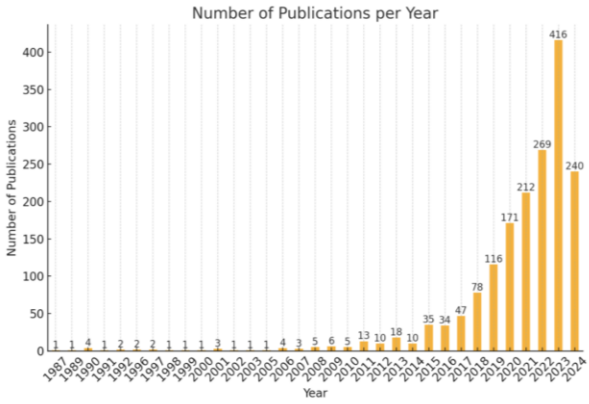

Figure 1: Number of Publication by year.

The concept of machine learning (ML) was first introduced by Arthur Samuel in 1959, but the first significant applications of cognitive learning and ML methods in cybersecurity emerged in 1987 [2]. These early studies laid the foundation for the integration of machine learning techniques into more complex systems, including OT networks. Although machine learning began with theoretical models, by the late 1980s and early 1990s, more practical cybersecurity applications began to develop, paving the way for the inclusion of cognitive capabilities in these systems. OT networks started to gain significant attention with the rise of Industry 4.0 in the 2010s. As hardware and software in manufacturing systems became more interconnected, the need for secure and efficient methods to manage these systems increased. The first significant wave of cognitive learning and machine learning applications in OT systems emerged around 2016, when academics and industry experts began advocating for the integration of cognitive networks into OT environments [3]. This was in response to the growing issue of cybersecurity threats and vulnerabilities in OT systems. In 2021, attention was given to IoT network architecture for AI-based security applications [4]. Published studies highlighted the potential of machine learning for securing, monitoring, and managing OT systems. Developing cognitive algorithms capable of learning from real-time data and dynamically adapting to network conditions became an important focal point. In the 2020s, techniques such as

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 14, Issue 8, August 2025)

deep learning, federated learning, and transfer learning began to emerge as promising methods for cybersecurity in OT networks [5, 6].

Recent developments in the use of cognitive machine learning (CML) in OT networks have been observed in 2023-2024, with a significant increase in the number of related publications. During this period, studies have focused on how machine learning and cognitive systems can be used alongside existing cybersecurity measures to prevent advanced threats such as DDoS attacks. Researchers have begun proposing hybrid models that integrate machine learning with traditional security mechanisms [6]. In 2024, the focus shifted to protocol-based examinations used in IIoT systems, with an emphasis on the importance of strong security measures to protect data transmission between devices. Many publications have pointed out the security vulnerabilities arising from the lack of standards in OT systems [7, 8].

These vulnerabilities have emerged as significant challenges that hinder the implementation of effective cybersecurity measures in OT networks. Due to the increase in Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, research has been conducted on the need to analyze the entire system and take preventive measures accordingly [9].

Additionally, the IEC 62443 standard, which provides a critical framework for OT network security, has been discussed in studies examining the systems required to ensure secure transitions between IT and OT systems [9, 10]. The need for physical and systematic segmentation as part of cybersecurity measures has also been emphasized [11].

Recent literature has extensively explored the use of advanced computing systems, such as Fog Computing, Edge Computing, and Blockchain—to enhance OT network security [12]. It has been suggested that traditional security systems have low success rates, and the use of deep neural networks (DNNs) is proposed [13]. The use of Cognitive Controller models to better manage Enterprise Wireless Local Area Networks (WLANs) in OT networks has been discussed [14].

Digital twin technology has also started to be used recently to close security gaps. This technology helps to predict potential security risks by modeling and simulating OT networks before they occur in the real world [15]. Blockchain technology has been investigated due to its potential to provide decentralized, immutable event logs to prevent IDS and DDoS attacks [16].

A recurring theme in the literature is the use of anomaly detection techniques to identify abnormal behaviors in OT systems. Traditional methods have been insufficient, leading to a shift towards more advanced machine learning models. Research has examined how models such as Poisson Unauthorized Entry Models (PIM), Bayesian Inference Models, and Markov Game Models can be effectively used for anomaly detection [17]. These models are seen as highly effective for detecting cybersecurity breaches in OT networks. Additionally, many studies have suggested that OT systems have a high number of security vulnerabilities, which could lead to a high diversity of attacks [18]. This points to a potential risk of significant damage to infrastructures due to the lack of a holistic approach, as most current research focuses on detecting issues in subsystems [19]. Due to the size and diversity of OT network architectures, the use of a central structure is also deemed important [20].

These challenges indicate that more collaboration is needed between academia, industry, and regulatory bodies to create effective, scalable security solutions for OT networks.

A. Challenges and Future Directions

Despite the progress achieved, several challenges remain in this field. The absence of standardized structures in OT networks, combined with their growing complexity, makes it difficult to implement consistent and effective security measures. For the effective integration of Cognitive Machine Learning (CML) into OT networks, researchers emphasize the need for advancements in the following areas:

- Development of standardized protocols to ensure secure communication in OT environments.
- Integration of cognitive systems with existing IT security infrastructures to provide holistic protection.
- Real-time analysis and adaptive response mechanisms capable of detecting and mitigating threats dynamically.
- Lightweight and advanced machine learning models that can function effectively on resource-constrained OT devices.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 14, Issue 8, August 2025)

The identified challenges and proposed solution approaches discussed in the reviewed studies are systematically summarized in Table 1.

IV. Results and Discussion

The reviewed publications can be categorized into two primary groups based on their focus: general solution methods and local solution methods. Among the reviewed studies, eight publications focused on general solutions [3,6,7,8,10,15,20,22], while fourteen publications examined local solutions, as summarized in Table 1 [4,5,9,11,12,13,16,17,18,19,21,23,24]. Based on the focus of these studies, the following observations were made:

Networking: 1 study addressed networking aspects.

Protocols: 2 studies focused on communication protocols, including OPC and MQTT.

Local security measures: 8 studies emphasized localized cybersecurity applications.

General cybersecurity approaches: 3 studies addressed general security strategies.

Architecture and new techniques: 2 studies explored architectural design and the implementation of advanced techniques.

Machine learning applications: 4 studies highlighted the use of machine learning, with 3 focusing on local solutions and 1 on general solutions.

Key findings from the literature analysis include: No end-to-end study covering the entire OT network was found.

Among 124 publications related to OT networks, no test studies were found in the defense industry or involving critical data.

Architectural designs for end-to-end OT network security systems are lacking; only three publications discussed designs for end devices.

Limited attention has been given to segmented network structures, with only one publication addressing this topic.

While some studies explored cognitive WLAN systems and future technologies such as quantum computing, there is no comprehensive study examining the full scope of OT operations for a secure network.

Overall, the literature demonstrates growing interest in the application of cognitive machine learning and other advanced methods for cybersecurity in OT networks. However, the current research primarily addresses subsystems rather than comprehensive network-level solutions.

V. Conclusion

This paper presents a systematic literature review on the application of cognitive machine learning (CML) in Operational Technology (OT) networks. Although no comprehensive study currently exists, partial studies have examined specific aspects such as protocol security, architectural design for end devices, and localized machine learning applications.

The review highlights the following:

Technical information on systems and protocols used in IoT and OT networks is essential for implementing CML effectively.

Current research primarily addresses subsystems, while end-to-end network security remains largely unexplored.

The field is in its early stages, with commercial considerations possibly limiting publicly available research.

As commercial and technological advancements continue, it is expected that the number of studies on CML applications in OT networks will increase.

This study underscores the urgent need for holistic approaches that integrate cognitive machine learning into the full OT infrastructure, providing adaptive, real-time, and robust cybersecurity solutions.

References

[1] D. G. O'Brien and W. A. Yasnoff, "Privacy, confidentiality, and security in information systems of state health agencies," Am. J. Prev. Med., vol. 16, no. 4, pp. 351–358, May 1999.

[2] A. Samuel, "Some Studies in Machine Learning Using the Game of Checkers," IBM J. Res. Dev., vol. 3, no. 3, pp. 210–229, 1959.

[3] L. Xu et al., "CogNet: A network management architecture featuring cognitive capabilities," in 2016 European Conference on Networks and Communications (EuCNC), 2016.

[4] S. Dunlap et al., "Using timing-based side channels for anomaly detection in industrial control systems," Int. J. Crit. Infrastruct. Protect., vol. 15, pp. 12–26, 2016.

[5] S. Chaudhary and P. K. Mishra, "DDoS attacks in Industrial IoT: A survey," Comput. Netw., vol. 236, p. 110015, 2023.

[6] C. Avci, B. Tekinerdogan, and C. Catal, "Reference architecture design for machine learning supported cybersecurity systems," in Management and Engineering of Critical Infrastructures, B. Tekinerdogan et al., Eds., Academic Press, 2024, pp. 193–221.

[7] B. Babayigit and M. Abubaker, "Industrial Internet of Things: A Review of Improvements Over Traditional SCADA Systems for Industrial Automation," IEEE Syst. J., vol. 18, no. 1, pp. 120–133, 2024.

[8] I. Behnke and H. Austad, "Real-Time Performance of Industrial IoT Communication Technologies: A Review," IEEE Internet Things J., vol. 11, no. 5, pp. 7399–7410, 2024.

[9] M. R. Kadri et al., "Survey and classification of DoS and DDoS attack detection and validation approaches for IoT environments," Internet Things, vol. 25, p. 101021, 2024.

[10] T. Kampa, C. K. Müller, and D. Großmann, "Interlocking IT/OT security for edge cloud-enabled manufacturing," Ad Hoc Netw., vol. 154, p. 103384, 2024.

[11] E. D. Knapp, "Implementing Security and Access Controls," in Industrial Network Security (Third Edition), Syngress, 2024, pp. 331–381.

[12] M. Kokila and S. Reddy K, "Authentication, access control and scalability models in Internet of Things Security–A review," Cyber Security Appl., vol. 3, p. 100057, 2024.

[13] Y. Lu et al., "Intrusion detection for Industrial Internet of Things based on deep learning," Neurocomputing, vol. 564, p. 126886, 2024.

[14] S. M. Nadaf et al., "Cognitive Controller Framework for Seamless Orchestration and Management in Enterprise Wireless Networks," in 16th Int. Conf. on COMmunication Systems-NETworkS (COMSNETS), 2024.

[15] M. Qian et al., "Secured digital-twin data service for the Internet of smart things," in Smart Spaces, Z. Lyu, Ed., Academic Press, 2024, pp. 71–102.

[16] K. Shalabi, Q. A. Al-Haija, and M. Al-Fayoumi, "A Blockchain-based Intrusion Detection/Prevention Systems in IoT Network: A Systematic Review," Procedia Comput. Sci., vol. 236, pp. 410–419, 2024.

[17] X. Tu et al., "Architecture for data-centric and semantic-enhanced industrial metaverse: Bridging physical factories and virtual landscape," J. Manuf. Syst., vol. 74, pp. 965–979, 2024.

[18] S. Umbrello, "Quantum Technologies in Industry 4.0: Navigating the Ethical Frontier with Value-Sensitive Design," Procedia Comput. Sci., vol. 232, pp. 1654–1662, 2024.

[19] P. Yao et al., "Statistical knowledge and game-theoretic integrated model for cross-layer impact assessment in industrial cyber-physical systems," Adv. Eng. Inform., vol. 59, p. 102338, 2024.

[20] C. Zanasi, S. Russo, and M. Colajanni, "Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures," Ad Hoc Netw., vol. 156, p. 103414, 2024.

[21] A. Schlemitz and V. Mezhuyev, "Approaches for data collection and process standardization in smart manufacturing: Systematic literature review," J. Ind. Inf. Integr., vol. 38, p. 100578, 2024.

[22] S. Shiu, C. Dalton, and B. Balacheff, "Security for digital manufacturing," in Digital Manufacturing, C. D. Patel and C.-H. Chen, Eds., Elsevier, 2024, pp. 409–442.

[23] C. Smiliotopoulos, G. Kambourakis, and C. Kolias, "Detecting lateral movement: A systematic survey," Heliyon, vol. 10, no. 4, p. e26317, 2024.

[24] M. Snehi, A. Bhandari, and J. Verma, "Foggier skies, clearer clouds: A real-time IoT-DDoS attack mitigation framework in fog-assisted software-defined cyber-physical systems," Comput. Secur., vol. 139, p. 103702, 2024.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 14, Issue 8, August 2025

TABLE I
LITERATURE REVIEW LIST

Num.	Year	Problem	Solution Method	Category	Area	Ref. Num
1	2016	The network's variety and scale	Establishing cognitive networks and applying machine learning is necessary.	General	Network	3
2	2021	IoT Network Cyber Risks	Artificial intelligence	Local	Protocol	4
3	2023	DDos attacks	Machine learning, deep learning, federated learning and transfer learning methods	Local	Cyber Security	5
4	2023	Architectural structure and cyber attacks	Machine learning methods	General	Cyber Security	6
5	2024	The use of various protocols	General review	General	Protocol	7
6	2024	Lack of standard	General review	General	Protocol	8
7	2024	Attack type analysis	General review	Local	Cyber Security	9
8	2024	IT/OT Security	IEC 62443 standard	General	Architectural and Protocol	10
9	2024	IT/OT Segmentation	Physical and systemic Segmentation	Local	Architectural	11
10	2024	Security	Machine learning, fog computing, edge computing and blockchain	Local	Cyber Security	12
11	2024	The Inadequacy of Traditional Defense Systems	Using a Deep Neural Network	Local	Cyber Security	13
12	2024	The Difficulty of Network Management-WLAN	Cognitive Controller Model	Local	Network	14
13	2024	Systemic Explanations	Digital Twin	General	Cyber Security	15
14	2024	Protocol Review	OPC UA	Local	Protocol	21
15	2024	IDS and DDoS attacks	Blockchain	Local	Cyber Security	16
16	2024	IT/OT	General review	General	Cyber Security	22
17	2024	Industry 4.0	Quantum Technology	Local	New Technic	23
18	2024	Industry 5.0-Metaverse	Definition of Lateral Movement and Use of Machine Learning	Local	Cyber Security	24

19	2024	Anomaly Detection	Poisson intrusion model (PIM), Bayesian inference model and Markov game model	Local	Cyber Security	17
20	2024	Industry 4.0	General review	Local	New Technic	18
21	2024	The inclusion of subsystems of the studies	General review	Local	Cyber Security	19
22	2024	Architectural Structure	Central Administration	General	Architectural	20