A Review on Integrating Zero-Trust Security with Artificial Intelligence in Multi-Sensor Decision-Level Data Fusion for Industrial Internet of Things (IIoT)

Simran A. Sodha[1], Gunjani J. Vaghela[2]
[1]*Lecturer, Atmiya University, Rajkot, Gujarat, India*
[2]*Assistant Professor, Atmiya University, Rajkot, Gujarat, India*

***Abstract*—The Industrial Internet of Things (IIoT) is transforming industries by enabling real-time data collection, monitoring, and decision-making through interconnected sensors and devices. However, this increased connectivity also brings significant security challenges, as IIoT systems are vulnerable to cyber attacks, unauthorized access, and data breaches. Zero-Trust security, a model that assumes no entity—inside or outside the network—should be trusted by default, offers a robust framework for securing IIoT environments. At the same time, Artificial Intelligence (AI) plays a critical role in enhancing decision-making through intelligent data analysis and anomaly detection. This review explores the integration of Zero-Trust security with AI in multi-sensor decision-level data fusion for IIoT, highlighting the synergies between these two technologies to address both security and operational challenges. By combining continuous authentication and monitoring from Zero-Trust with AI-driven decision-making, IIoT systems can enhance data integrity, optimize performance, and proactively detect security threats. The paper reviews the concepts, methodologies, and applications of this integration, examining case studies from various industries and discussing potential future directions. Ultimately, the review emphasizes the promise of a secure, intelligent, and efficient IIoT ecosystem through the convergence of Zero-Trust security and AI-enhanced multi-sensor data fusion.**

***Index Terms* —Artificial Intelligence, Decision-Level Fusion, Industrial Internet of Things (IIoT), Zero-Trust Security.**

I. INTRODUCTION

The Industrial Internet of Things (IIoT) encompasses a network of connected devices, sensors, and machines that communicate and share data in real time. These devices generate a wealth of data that is critical for optimizing industrial processes, improving maintenance schedules, and enhancing productivity. However, as IIoT systems become more interconnected, they also become increasingly vulnerable to cybersecurity threats. Traditional security models, which trust devices and users inside the network, are inadequate for such dynamic and large-scale environments. This has led to the widespread adoption of the Zero-Trust security model, which operates on the principle that no device or user should be trusted by default, and continuous verification is required for every access attempt.

At the same time, Artificial Intelligence (AI)**,** including machine learning and deep learning techniques, is being used to process vast amounts of sensor data in real time. AI techniques are adept at detecting patterns, anomalies, and trends within the data, enabling smarter, more informed decision-making. In IIoT systems, AI can optimize operations, enhance predictive maintenance, and improve system performance. However, the effectiveness of AI models relies heavily on the trustworthiness of the data. Data integrity is paramount in IIoT systems, and this is where the integration of Zero-Trust security can play a key role in ensuring the security and reliability of sensor data used by AI models.

The fusion of data from multiple sensors (referred to as multi-sensor decision-level data fusion**)** is crucial for making accurate and reliable decisions in IIoT systems. Multi-sensor fusion combines data from various sources, improving the quality and reliability of the decisions made by IIoT systems. However, this fusion process also introduces vulnerabilities, as compromised sensor data could lead to faulty decision-making. The integration of Zero-Trust security with AI-powered multi-sensor data fusion ensures that data is authentic,

reliable, and secure, enhancing both system security and operational efficiency.

II. BACKGROUND

A. Zero trust security in IIoT

Zero-Trust Security is a modern cybersecurity approach that fundamentally changes the way networks and systems are protected. Instead of relying on traditional perimeter-based security, which assumes that everything inside the corporate network is trustworthy, Zero-Trust operates on the principle that no user, device, or system—whether inside or outside the network—is inherently trusted. This means that access is granted based on a strict, continuous authentication and authorization process, and all traffic, whether internal or external, is treated as potentially malicious until verified.

In the context of the Industrial Internet of Things (IIoT), Zero-Trust security is especially important because IIoT networks consist of a vast number of interconnected sensors, devices, machines, and endpoints, many of which are deployed in remote or unsecured environments. These devices are often vulnerable to cyber threats, making it critical to enforce strict security protocols to protect the data integrity, confidentiality, and operational continuity of IIoT systems.

B. Artificial Intelligence in IIoT

Artificial Intelligence (AI) is revolutionizing the way industries manage and operate their assets, processes, and systems. When combined with the Industrial Internet of Things (IIoT), AI offers unprecedented opportunities for automation, optimization, predictive maintenance, and enhanced decision-making. IIoT refers to the network of physical devices, sensors, and machines in industries that communicate and exchange data over the internet. AI, on the other hand, enables machines to learn from data, make predictions, and automate processes without explicit programming.

In the context of IIoT, AI enhances the capabilities of connected devices by providing intelligent solutions that can analyse vast amounts of data in real-time, improving the efficiency, safety, and reliability of industrial operations.

C. Multi-Sensor Decision-Level Data Fusion

Multi-Sensor Decision-Level Data Fusion (DLD) refers to the process of integrating data from multiple sensors or sources at the decision-making stage to produce a more accurate, reliable, and informed output. It is a critical approach in applications where data from various sensors, operating in diverse conditions, is required to work together to make decisions or predictions. Instead of merely merging raw sensor data, decision-level fusion combines the decisions made by each sensor (or sensor system) to improve overall performance, often in real-time.

Multi-sensor decision-level fusion is especially useful in environments where sensor data can vary due to noise, different sensor types, or environmental strengths of each sensor's decision to generate a unified, robust, and more reliable decision.

III. LITERATURE REVIEW

As the traditional paradigm of the engineering, manufacturing, and architectural sectors shifts to the digital platform, data from many sources becomes available for the extraction and collection of pertinent data. [1]. The main characteristic of DLDF that sets it apart from other data fusion techniques is that it generates intermediate information or results from the extracted dataset, cross-verifying the quality and relevance of the data acquired. Once the information generated is confirmed, the final decision is made using the information that is revealed as the process's output. [2]. Additionally, the usefulness of deep learning in improving security is examined in light of the security element of IoT infrastructure. Peer authentication solutions are insufficient to address the heightened security requirements of complex networks with the advent of Industry 4.0, often known as the fourth industrial revolution. When taking into account intricate networks with thousands of devices, deep reinforcement learning offers an ambient solution to effectively identify the device.[3]. Attacks from insiders or intruders are always a danger in every network. The well-thought-out zero-trust security architecture prevents attacks by requiring devices to verify themselves each time they connect to the network, rather than merely trusting them based on their location. Smart sensors are used by IIoT devices to

retrieve and aggregate data from various sources. The IIoT networks greatly benefit from multi-sensor data fusion since it makes wise decisions easier. [4]. The IIoT, where information is generated from multiple sources of data extracted from various devices involved in the network, is the result of digitization, also known as the industrial fourth revolution. In order to balance real-world situations with the networked space, IIoT infrastructure aims to create a system where coordination and association between the devices in the network are enabled. For a given situation or state, data fusion conducts a collective analysis of the various data from various sources. The more raw data that is tracked and observed, the more accurate and logical conclusions the system can draw. [5]. Due to the involvement of a vast number of distinct devices, data fusion has been widely experienced in IoT frameworks. IIoT infrastructure is made up of a vast number of devices that are connected to one another in order to communicate over the Internet. Smart sensors on each device are able to detect and gather the necessary data for pertinent information. These days, digital and intelligent educational systems have replaced the traditional educational system.[6]. Sensor involvement has increased as a result of the transition from traditional paradigms to digital platforms, necessitating interactive algorithms that enable the effective retrieval and fusion of datasets. According to Kong et al.[7]. The process of configuring a robust system to approximate the Q-values obtained through distance learning or deep-quality learning network-driven e-learning is described. El Faouzi and Klein propose an enhanced Q-learning algorithm based on approximate state matching in an agricultural plant protection setting to determine the best course of action for the Unmanned Aerial Vehicle (UAV) in agricultural plant protection. [8]. The current state of zero-trust security-based prevention and security measures is reviewed, along with their applications and related difficulties. Wang et al. propose an ensemble learning-based analysis and anomaly prediction method using log processing.[9]. To examine the uses and applications of deep learning in anomaly detection, a review is carried out. The survey separates deep learning into 11 fine-grained categories and 3 high-level categories. AlDahoul et al. conceptualize a model for anomaly detection that combines a binary normal/attach classifier with a multi-attacks classifier.[10]. The problems with data fusion are discussed, as is the strategy for filling the technique's gap. According to the study, the data fusion technique's use of ensemble learning performs exceptionally well in addressing the issues raised by peer approaches. How data from the Internet of Things and information systems can be combined to create data-driven AEC is described in digitally driven architecture, engineering, and construction (AEC), and Huangtal proposes a two-level conceptual framework that connects BIM and IoT. [11]. Two main topics are reviewed: the architecture and methodology, and the security and privacy offered by deep learning in the Internet of Things. He et al. review the foundational implementation, architecture, and applications of zero-trust security. [12].

IV. INTEGRATION OF ZERO-TRUST SECURITY WITH AI

In the era of Industrial Internet of Things (IIoT), where billions of connected devices generate vast amounts of sensitive data, ensuring robust cybersecurity is paramount. Traditional security approaches fail to address the dynamic and sophisticated threat landscape of modern systems. Zero-Trust Security (ZTS), with its 'never trust, always verify' principle, offers a promising solution. However, the complexity of decision-making in ZTS frameworks necessitates the integration of Artificial Intelligence (AI). AI enhances ZTS by enabling adaptive, automated, and context-aware security measures, ensuring continuous protection in real-time. The benefits are multifaceted, addressing critical vulnerabilities while enhancing operational efficiency and resilience. Below are the key advantages:

A. Enhanced Threat Detection and Response

AI enables real-time anomaly detection by analyzing vast datasets generated by connected devices. By continuously learning from user behavior and device interactions, AI can detect even subtle changes that could indicate a breach or unauthorized access.

B. Adaptive Security Controls

Zero-Trust's core principle of continuous verification is bolstered by AI, which provides context-aware decision-making. AI models assess dynamic conditions such as user location, behavior, and device health to adjust access permissions in real-time, ensuring that

only authorized entities are granted access to critical resources.

C. Automation of Security Processes

The integration of AI helps automate complex security tasks, such as policy enforcement, threat analysis, and incident response. This reduces the manual overhead involved in monitoring and securing systems, particularly in large-scale IoT environments.

V. CHALLENGES IN MULTI-SENSOR DECISION-LEVEL FUSION FOR IIOT.

Risk/Challenge	Description	Impact	Relevant Studies
Sensor Failure	Failures in one or more sensors, either due to hardware issues, environmental factors, or aging.	Leads to incomplete or erroneous data, affecting decision accuracy.	Yao et al. (2020)[13]
Adversarial Attacks	Intentional manipulation of sensor data by malicious actors, often in the form of false data injection.	Can manipulate decisions, leading to system failures or security breaches.	Dai et al. (2021)[14]
Data Overload	Large volumes of sensor data that overwhelm fusion algorithms and computational resources.	Results in delayed decision-making and potential system lag.	Zhang et al. (2021)[15]
Synchronization Issues	Data from sensors not properly synchronized, leading to mismatches in timing or order.	Inaccurate decision-making due to outdated or delayed data.	Zhu et al. (2020)[16]

VI. IMPORTANCE OF SECURE DATA FUSION IN IIOT

In IIoT systems, secure data fusion is crucial for ensuring that the decision-making processes are not only accurate but also trustworthy. Given the high stakes involved—whether in manufacturing, energy management, or autonomous vehicles—ensuring that data from multiple sensors is fused securely without interference from malicious actors or faulty sensors is vital.[17].

VII. MITIGATING THREATS IN MULTI-SENSOR DECISION-LEVEL FUSION WITH ZERO-TRUST AND AI

A. Sensor Failure

Zero-Trust: Verifies and continuously monitors sensor data to detect and prevent faulty data from entering the fusion process.[18].

AI: Predictive maintenance and fault detection algorithms identify potential sensor failures before they impact the system.

B. Data Inconsistency

Zero-Trust: Ensures continuous data validation, preventing inconsistent or erroneous data from being trusted.
AI: Anomaly detection models reconcile and correct data inconsistencies in real-time.

C. Adversarial Attacks

Zero-Trust: Uses strong authentication and encryption to prevent data tampering and false data injection.
AI: Detects adversarial manipulations by identifying anomalies in sensor data patterns.

VIII. CONCLUSION AND FUTURE TRENDS

Edge AI and Federated Learning: Edge AI enables local data processing in IIoT systems, improving real-time decision-making and reducing latency. Federated Learning allows AI models to be trained across distributed devices, reducing the need for centralized data storage.

AI-Powered Predictive Maintenance**:** AI is advancing predictive maintenance techniques by analyzing sensor data to forecast equipment failures before they occur, enhancing operational efficiency.

Zero-Trust Security in Edge and Cloud Integration**:** As IIoT systems span both edge devices and cloud networks, Zero-Trust security ensures continuous authentication and validation across decentralized environments.The integration of Zero-Trust Security (ZTS) and Artificial Intelligence (AI) in Industrial Internet of Things (IIoT) systems presents a robust solution to address challenges such as sensor failures, data inconsistency, and security risks. Zero-Trust ensures continuous verification of devices and data integrity, reducing unauthorized access and potential attacks, while AI enhances data processing, predictive maintenance, and anomaly detection, thus improving operational efficiency. The combination of these technologies creates more secure, reliable, and autonomous systems in industrial settings. However, to fully leverage their potential, an interdisciplinary approach is necessary, combining expertise from cybersecurity, machine learning, sensor technologies, and industrial automation, enabling the development of scalable and resilient IIoT solutions. This collaborative approach is essential for overcoming current limitations and addressing the evolving demands of future industrial ecosystems.

REFERENCES

[1]. Tang, Y., Zhou, Y., Ren, X., Sun, Y., Huang, Y., & Zhou, D. (2023). A new basic probability assignment generation and combination method for conflict data fusion in the evidence theory. Scientific Reports (2023), pp 18, may-2023.

[2]. Chatzichristos, C., van Eyndhoven, S., Kofidis, E., & van Huf fel, S. (2022). Coupled tensor decompositions for data fusion. In Y. Liu (Ed.), Tensors for data processing. Sciencedirect (2022), pp 341–370, jan-2022.

[3]. Chen, G., Liu, Z., Yu, G., & Liang, J. (2021). A new view of multisensor data fusion: Research on generalized fusion. Mathematical Problems in Engineering (2021), vol 2021, pp 5471242, oct-2021.

[4]. Gagolewski, M.. Data fusion: Theory, methods, and applications, arXiv Preprint:2208.01644 (2022), vol 7, pp 1-89, aug-2022.

[5]. Tevera-Ruiz, A., Garcia-Rodriguez, R., Parra-Vega, V., & Ramos-Velasco, L. E.. Q-learning with the variable box method: A case study to land a solid rocket. Machines (2023), vol 11, pp 14, feb-2023.

[6]. Baratloo, A., Hosseini, M., Negida, A., & El Ashal, G. (2015). Part 1: Simple definition and calculation of accuracy, sensitiv ity and specificity. Archives of Academic Emergency Medicine (2015), pp 4, feb-2015.

[7]. Kong, L., Peng, X., Chen, Y., Wang, P., & Xu, M. (2020). Multi-sensor measurement and data fusion technology for manufacturing process monitoring: Aliterature review. International Journal of Extreme Manufacturing (2020), vol 2, pp 022001, jun-2020

[8]. El Faouzi, N. E., & Klein, L. A. Data fusion for ITS: Techniques and research needs. Transportation Research Procedia (2016), vol 15, pp 495–512, jun-2016.

[9]. Wang, B., Hua, Q., Zhang, H., Tan, X., Nan, Y., Chen, R., & Shu, X.. Research on anomaly detection and real-time reliability evaluation with the log of cloud platform. Alexan dria Engineering Journal (2022), vol 61 pp 7183–7193, jan-2022.

[10]. AlDahoul, N., Abdul Karim, H., & Ba Wazir, A. S. . Model fusion of deep neural networks for anomaly detection. Journal of Big Data (2021), vol 8, pp 106, Aug-2021.

[11]. Huang, X., Liu, Y., Huang, L., Onstein, E., & Merschbrock, C. BIM and IoT data fusion: The data process model per spective. Automation in Construction (2023), vol 149, pp 104792, feb-2023.

[12]. He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A survey onzerotrustarchitecture: Challengesandfuturetrends.Wireless Communications and Mobile Computing, (2022), vol 2022, pp 6476274, jun-2022.

[13]. Yao, H., Gao, P., Zhang, P., Wang, J., Jiang, C., & Lu, L. (2019). "Hybrid Intrusion Detection System for Edge-based IIoT Relying on Machine-learning-aided Detection." IEEE Networks,(2019), vol 33, pp 75-81, oct-2019.

[14]. Dai, W., et al. "Artificial Intelligence in Industrial Internet of Things: A Review." Journal of Industrial Information Integration (2023), pp 8-22, feb-2023.

[15]. Zhang, X., et al. "Artificial Intelligence for Industrial Internet of Things: Applications, Challenges, and Future Directions." *IEEE Transactions on Industrial Informatics* (2021), vol 9, pp 12861-12885, Aug-2022.

[16]. Zhu, X., et al. "AI-Based Data Analytics for IoT: Recent Developments, Applications, and Future Directions." *Sensors* (2020), vol 20, pp 4609, Aug-2020.

[17]. da Silva, A., & Marques Cardoso, A. J. Designing the future of coopetition: An IIoT approach for empowering SME networks. The International Journal of Advanced Manufacturing Technology (2024), pp 1-16, oct-2024.

[18]. Hakimi, O., Liu, H., Abudayyeh, O., Houshyar, A., Almatared, M., & Alhawiti, . Data fusion for smart civil infrastructure management: A conceptual digital twin framework. Buildings (2023), vol 13, pp 2725, oct-2023.