

RESEARCH ARTICLE

A zero-trust cybersecurity architecture for AI-enabled smart manufacturing systems

✉ Vamsi Krishna Avineni

✉ Mechanical Engineer, Diversified Services Network Inc., IL, USA

Corresponding Author: Pending confirmation, E-mail: vamsikrishnaavineni@gmail.com

ABSTRACT

The rise of artificial intelligence (AI), IIoT, cyber-physical systems, edge, and cloud computing technologies, and intelligent automation is leading to the creation of a highly connected and data-driven space for modern manufacturing. On the other hand, it broadens the attack surface and poses challenges to traditional perimeter security models based on implicit trust inside corporate networks. In this paper, we introduce Zero-Trust cybersecurity architecture for AI-powered smart manufacturing environments. The architecture incorporates five security domains: Identity and Access Security, Device and Operational Technology (OT) Protection, Network and Communication Security, Data, Application, and AI Security, as well as Continuous Monitoring Powered by AI. The integration of those domains is realized by means of the Centralized Zero-Trust Policy and Trust Engine, which enables context-aware and adaptive access control based on the user identity, device posture, resource sensitivity, operation context, and behavioral patterns. Special emphasis is made on the dual purpose of the AI technologies as both the instrument for cybersecurity and important part of the manufacturing infrastructure that needs to be protected from manipulation and malicious activity. The study considers the issues of dynamic trust assessment, least-privilege access authorization, micro-segmentation, and continuous verification as the ways of minimizing the risks of unauthorized access and lateral movement across interconnected manufacturing resources. We also discuss practical challenges related to legacy OT equipment, real-time requirements, interoperability, scalability, and manufacturing availability. The proposed architecture offers the framework for the implementation of the Zero-Trust approach in the case of cybersecurity of AI-powered manufacturing.

KEYWORDS

Zero Trust Architecture, smart manufacturing, artificial intelligence, Industrial Internet of Things, cybersecurity

ARTICLE INFORMATION

ACCEPTED: 3 September 2026

PUBLISHED: 3 October 2026

DOI: 10.32996/fcsai.2026.5.10.4

1. Introduction

With increasing digitization of the manufacturing industry, manufacturers have been able to achieve highly interconnected and intelligent manufacturing systems where there is convergence of physical and computational, communication, and decision-making technologies. Current smart manufacturing systems leverage IIoT, CPS, AI, cloud and edge computing, robotics, and data analytics to achieve real-time monitoring, predictive maintenance, automatic quality control, process optimization, and autonomous decision-making. The advent of Industry 4.0 has further helped in converging machines, sensors, production systems, enterprise software solutions, and other external services throughout the manufacturing value chain [1][2]. Even though increased interconnectedness helps in achieving higher levels of productivity and visibility in operations, it also increases the attack surface and creates new ways for cyberattacks to penetrate from IT systems into OT systems.

Cybersecurity is especially important in smart manufacturing due to the potential impact that cyber-attacks can have not just on the confidentiality but also on the integrity and availability of physical production processes. Industrial device tampering, alteration of production data, modifications in process parameters, ransomware, and attacks on control systems can cause disruption in production process, degradation in product quality, damage to the equipment, economic losses, and safety impacts. Toussaint et al. (2024) pointed out that the high level of dependency of the manufacturing process in Industry 4.0 on data-based operations increases the importance of the problem of data manipulation in cybersecurity. In the same way, research on manufacturing cybersecurity highlights that growing digitalization and automation necessitate security solutions for tackling evolving cyber threats (Alqudhaibi et al., 2026)[3][4].

Moreover, the growing use of AI makes the cybersecurity situation even more complicated. Nowadays, there are already examples of using AI models and machine learning in manufacturing for anomaly detection, predictive maintenance, visual inspections, process optimization, scheduling, and decision-making. However, AI brings new challenges in terms of cybersecurity, namely, threats associated with training data, model integrity, manipulation of AI models, malicious inputs, and access to AI resources. As a result, there is a dual role of AI in smart manufacturing cybersecurity: it can help in protecting against various cyber threats and provide an understanding of complex patterns, whereas AI technology becomes a new element of the cybersecurity infrastructure that should be protected as well (Lezzi et al., 2025). It means that the cybersecurity architecture in the future manufacturing system will have to include not only users and machines but also industrial data and AI technology.

This type of security model becomes inefficient in such environments since it assumes a clear-cut boundary of the network and relies heavily on the trust associated with the entities located within the boundary. The combination of information technology (IT) and operations technology (OT), use of cloud services, remote management, industrial Internet-of-Things (IIoT) technologies, third-party vendors, and distributed edge computing makes the traditional approach to security ineffective since it blurs the line between trusted internal systems and external untrusted networks. After breaking into a system through a trusted account or a connected device, lateral movements towards other critical resources are possible based on the implicit trust. The Zero-Trust architecture proposed for industrial environments faces similar challenges due to convergence of artificial intelligence, IIoT, distributed computing, and industrial systems [5].

Zero Trust Architecture (ZTA) offers an alternative security model by replacing location-based trust in cybersecurity with resource-based access control, which is constantly validated. As stated in NIST Special Publication 800-207, Zero Trust is an environment that does not inherently trust any single individual, group, process, service, system, or asset based on location or ownership [6]. Authentication and authorization procedures are carried out prior to access to any resources being granted; in doing so, security measures take into account both the subject requesting the access and the device itself (Mushtaq et al., 2025). This is extremely important for smart manufacturing as operators, engineering stations, industrial controllers, robots, IIoT devices, edge computing nodes, cloud services, and AI applications need access to various resources, which cannot necessarily be trusted just because they are inside the factory network.

Nevertheless, the application of traditional Zero Trust principles in manufacturing faces difficulties due to the presence of certain features inherent to industrial infrastructure which significantly distinguish it from the traditional corporate IT infrastructure. The manufacturing systems typically comprise legacy infrastructure components, a heterogeneous collection of industrial communication protocols, limited IIoT devices, high demands on the availability, real-time control systems, and equipment with a long life cycle. The implementation of the Zero-Trust in industrial environments therefore requires the provision of continuous and adaptive security without causing any unacceptable delays or disturbing the safe operation of the critical production process (Ananthakrishnan, 2026a)[7].

With this backdrop, this paper discusses an architectural approach that takes the form of Zero-Trust cybersecurity framework for AI-powered smart manufacturing systems. The framework discussed in this paper includes aspects related to identity and access security, device and OT security, network micro-segmentation, data and application security, AI/ML security, and intelligent monitoring as part of a single Zero-Trust decision plane. Instead of placing an onus on authentication once only and then offering perpetual trust thereafter, this approach focuses on verification and context-based access in human-human, human-machine, machine-machine, and human-AI and machine-AI interaction scenarios. The intent of this architecture is to create a security architecture for manufacturing applications that not only provides the ability to restrict any kind of unauthorized access and lateral movements but also ensure the security of the AI-enabled manufacturing process.

2. Cybersecurity Challenges in AI-Enabled Smart Manufacturing

The manufacturing environments empowered with artificial intelligence are typified by intense interactivity of physical machinery, industrial control systems, digital technologies, and intelligent decision-making systems. From the operational standpoint, IIoT sensors, PLCs, CNC machines, robots, actuators, SCADA systems are constantly producing and exchanging data regarding production processes. Increasingly, these systems are becoming interconnected via edge computing platforms, MES, ERP systems, digital twins, and cloud computing infrastructures. Although such integration provides opportunities for real-time visibility and data-based decision making, it results in the interdependence of the environments of OT and IT technologies, which were once separated from each other. According to NIST, increasing connectivity, wireless networks, sensors, and the prevalence of IT in manufacturing are critical sources of potential cybersecurity threats [8][9].

The intersection of IT and OT cybersecurity is especially crucial, as any breach from the company's network could lead to spreading out to production-related networks. Availability, reliability, deterministic nature, and safety are the primary concerns of manufacturing control environments; while protection of information and access are more important when speaking about cybersecurity in IT. In addition, industrial systems often contain legacy devices and communication protocols that have not been created to work in conditions of constant connectivity and in line with modern cybersecurity standards. Thus, security solutions like software updates, extensive encryption, or typical endpoint security controls cannot be implemented without regard for

performance impact on production (Crowther, 2024). The National Institute of Standards and Technology (NIST) industrial cybersecurity recommendations specifically mention the need to ensure cybersecurity while meeting production needs [10].

Due to the interconnectedness of smart manufacturing, there are many possible ways to launch an attack. Hacked user accounts, vulnerabilities in IIoT, malware, unauthorized remote access, insider threats, as well as manipulation of industrial data, can be used to gain access to production networks. After gaining initial access, poor network segmentation, as well as high levels of permissions within the production network, will enable an adversary to conduct lateral movement and access critical manufacturing assets. Specifically, it is important that the integrity of industrial information and control commands be maintained, as unprivileged changes in the software code, firmware, process parameters, or information from sensors can result in changes in behavior of the manufacturing process itself (Zarreh et al., 2019).

The integration of AI adds yet another layer to the existing threat environment. AI and machine learning solutions have become a common tool used to process large amounts of industrial data to help with predictive maintenance, process monitoring, quality inspection, optimization, and cybersecurity tasks. AI-based cybersecurity tools could enhance the detection of complex and hidden attack patterns and unusual activity that might not be identified using traditional security rules (Lezzi et al., 2025). On the other hand, increased reliance on AI technologies results in new assets and attack vectors. Training data manipulation, adversarial inputs, tampering of the model itself, and corruption of data pipelines could impact the outcome produced by intelligent manufacturing solutions. This is especially important as AI-generated data might affect the decision making related to equipment status, processes, quality, and maintenance. Therefore, the reliability of the intelligent manufacturing system depends on network security and data/intelligent component integrity as well [11].

It is evident from the above cybersecurity threats that smart manufacturing should not be based solely on the binary view of trusted internal network versus untrusted external parties. The users, devices, applications, artificial intelligence services, and manufacturing applications can change their security stance during their usage. Moreover, even when the user credentials and devices are compromised, they can pose serious security threats. Thus, the security framework needs to assess the security stance on a finer grain and limit the interaction of the compromised party with other manufacturing assets. It forms the rationale behind implementing Zero-Trust in the realm of smart manufacturing, where identity, state of the device, requested resources, context, and behavior can all together make continuous security decisions.

3. Zero-Trust Principles and Requirements for Smart Manufacturing

The cybersecurity issues presented above highlight the need for moving from a perimeter-based approach to securing AI-assisted manufacturing facilities towards a more dynamic resource-focused approach. One of the approaches that meets this need is the ZTA, which removes implicit trust associated with network location, device possession, or any other previously established form of authentication. As per NIST SP 800-207, the Zero Trust approach concentrates its security efforts on users, assets, and resources rather than network perimeters (Mushtaq et al., 2025). This means that a user, engineering workstation, industrial machine, application, or AI-based service should not be trusted to have access to production resources solely on account of being connected to the internal plant network.

Explicit verification of all access requests is a key necessity of ZTA. The authentication process must take into account both the identity of the user and the security status of the corresponding device prior to accessing the resource (Mushtaq et al., 2025). This necessity is especially true for production facilities where there exist many IIoT devices, industrial gateways, engineering workstations, and remote users. As a result, continuous authentication techniques have been researched for the purpose of making sure that an authenticated device is still trustworthy during its whole session [12].

The second prerequisite is that of granting access based on the principle of least privilege, whereby users, devices, applications, and services are given only those rights which are sufficient to carry out the tasks they are meant to do. Accordingly, access must be granted session-wise and resource-wise instead of giving full access to large chunks of the industrial network (Mushtaq et al., 2025). For instance, a workstation authorized to change parameters for a particular production unit does not need access to other PLCs, robots, database, or AI systems as well.

The assumption of breach also takes into account the fact that authentic entities cannot be always considered trustworthy. Manufacturing plants should be engineered in such a way that the possibility to move laterally is limited and interactions within connected assets are constantly assessed. Micro-segmentation can help achieve this by splitting inter-connected environments into smaller security segments with access policies defined between them. According to recent studies dedicated to ZTA in industrial settings, continuous authentication, dynamic authorization, micro-segmentation, and real-time risk assessment are important mechanisms to use ZTA in IIoT [13].

Lastly, Zero Trust calls for continuous monitoring and policy enforcement. According to NIST, a policy engine can be defined as the logical element that evaluates access decisions to a particular resource, which are carried out by the policy administrator and policy enforcement point, respectively (Mushtaq et al., 2025). While decisions are usually made based on access policies alone, they can also involve identity, condition of the device, sensitivity of the resource, behavior information, and environment context.

Such an approach is especially relevant in AI-assisted manufacturing, as the security context can rapidly change as different users, machines, edge devices, applications, and AI models exchange data. The security requirements for manufacturing-oriented Zero-Trust architecture are outlined in the next section.

4. Proposed Zero-Trust Cybersecurity Architecture for AI-Enabled Smart Manufacturing

Based on the security needs that were identified in previous sections, in this research work, we propose the Zero-Trust cyber security architecture to secure heterogeneous resources and flows of information in AI-assisted smart manufacturing systems. As discussed above, in order to expand the Zero-Trust security paradigm to manufacturing systems, all resources – human users, industrial devices, applications, data, and AI models should be considered as secured separately. According to NIST, the policy engine (PE), policy administrator (PA) and policy enforcement point (PEP) are the key elements of the logic of access decision making in Zero-Trust security model (Mushtaq et al., 2025). The proposed Zero-Trust architecture adopts the same decision-making logic but applies security layers specific to manufacturing for identity, OT assets, industrial communications, data, applications, and AI-assisted services.

4.1 Identity and Access Security

In the first level, secure identity management is provided for both human and non-human parties. In manufacturing, there are operators, engineers, administrators, vendors, distant technicians, industrial components, applications, and machine-to-machine services. Access control is thus performed based on the identity and not trust in the requests as they come from the factory environment. Multi-factor authentication, access control based on roles and attributes, privileged access management, and machine identities can all be used to implement a least privilege access policy. The above identity-focused approach fits well into the zero-trust architecture where authentication and authorization policies are applied regardless of the network boundaries and to users, applications, and service identities [14]. For instance, an authorized technician could get access to one industrial machine temporarily without having unrestricted access to other production machines.

4.2 Device and OT Asset Security

The second level provides protection to the physical and cyber-physical resources used during manufacturing operations, which may include such components as PLCs, CNC machines, robots, sensors, actuators, industrial gateways, engineering workstations, and edge devices. Devices are expected to have a validated identity and maintain an appropriate security posture before initiating any communication with protected resources. Such factors as device inventory, firmware integrity, configuration state, behavior, and communication patterns can be taken into consideration when making this evaluation. This approach becomes especially critical given the fact that industrial networks are heterogeneous and comprise of devices with different computational and operational properties. Zero Trust in IIoT research points out that industrial network architectures need to be heterogeneous, real-time, reliable and decentralized [15].

4.3 Network and Communication Security

Thirdly, there is the layer that is responsible for communication among manufacturing resources. Unlike the architecture that sees the entire network in the factory as a secure domain, the architecture presented here sees critical assets grouped into small zones and manages communication among these zones through policy enforcement points. This micro-segmentation ensures that unnecessary communication among manufacturing cells, IIoT devices, edge computing platforms, enterprise apps, and cloud platforms is limited. As such, compromise of a single sensor, workstation, or gateway cannot be enough to open a communication channel towards PLCs, MES platforms, engineering data bases, and other critical resources. Micro-segmentation has been identified as one of the ways to implement Zero Trust for heterogeneous IIoT architectures, especially when flexible policy enforcement is used (Wan et al., 2025).

4.4 Data, Application, and AI Security

The fourth layer ensures that digital assets required for intelligent manufacturing are secured. The digital assets are such as process parameters, production history, quality information, product designs, MES and ERP data, digital twin data, cloud applications, datasets used to train AI models, and machine learning models. The access to such digital assets should be controlled based on their identity, intended use, sensitiveness, and operating environment. Application identities play a critical role in intelligent manufacturing involving different environments (Ananthakrishnan et al., 2024).

AI models need to be protected due to the reason that attacks on them can affect automated decisions made without damaging the production network itself. It has been shown by the research in adversarial machine learning that AI systems can also be targets of attacks [16]. Hence, the suggested architecture provides for provenance of data set, version control of model, checking the integrity of the model, authenticated model deployment, validating the input and observing the output of the model. The recommendation or control input made by an AI system cannot be trusted unconditionally just because the model is authorized.

4.5 Continuous Monitoring and AI-Assisted Threat Detection

The fifth layer constantly gathers security information from the four layers above. Identity events, access requests, network communications, device conditions, application logs, AI model activities, and production anomalies contribute to the context used

in decision-making related to security. The anomaly detection based on artificial intelligence could be considered a supplement to rule-based systems and could identify abnormal behavior which would signal an issue with account, machine communication, tampering with industrial data or abnormal interaction of cyber-physical resources. Modern industrial cybersecurity designs also utilize Zero-Trust architecture and artificial intelligence in anomaly detection and context-based risk assessment [17].

The core of all these layers is the Zero-Trust Policy and Trust Engine, which controls the decisions regarding access. Based on the logical structure set forth in NIST SP 800-207, the policy engine makes a decision about granting, denying, or revoking resource access based on the security data available, whereas the policy administration and enforcement elements enable or disable the respective communication channel (Mushtaq et al., 2025). In the suggested manufacturing system architecture, information on authentication of identities, device health, network behavior, sensitive resources, operational context, and anomalies detected by AI is used as input to this decision-making procedure.

Conceptualized, the interaction takes place following the order Access Request → Identity and Device Verification → Context and Risk Assessment → Policy Decisions → Access Control → Ongoing Monitoring. Any alteration to the status of the device, user actions, network interactions, or model interactions thus constitutes a basis for re-evaluation even after the initial access has been allowed. The framework, thus established, combines traditional Zero-Trust decision-making with particular considerations for AI-based manufacturing processes, creating a basis for the adaptive access control described in the next chapter.

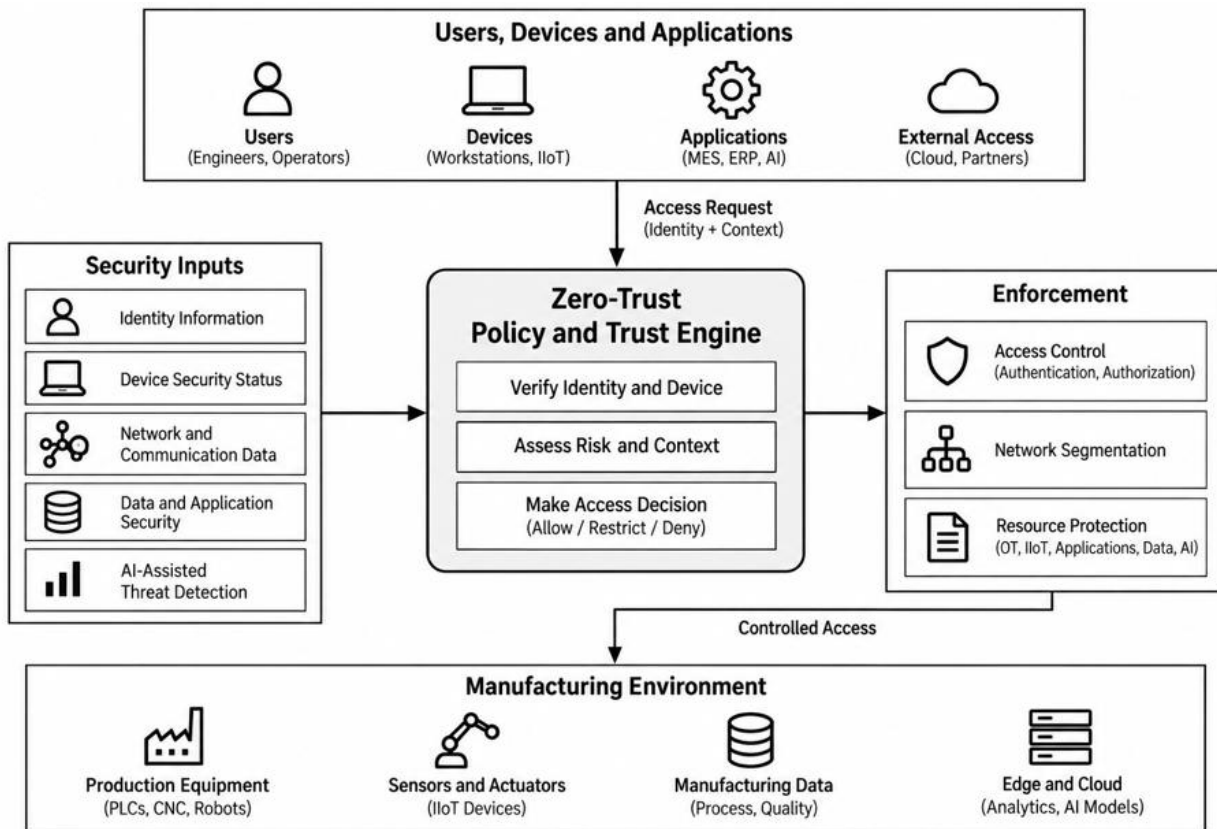


Fig 1. proposed Zero-Trust architecture

The Zero-Trust framework highlights how there is a continuous verification and control process on access to the smart manufacturing environment powered by AI and not an implicit trust-based process. Access requests from different types of users, devices, applications, or third-party service providers are analyzed by the central Zero-Trust Policy and Trust Engine with security inputs that include identity, device security status, networking and communication information, application security information, and threat detection using AI. It checks the identities and devices making access requests, analyzes the risk and context and decides whether to allow, restrict or deny the access request. This process is done using access control, network segmentation, and resource protection and after the process, access is allowed to the manufacturing resources like PLCs, CNC machines, robots, IIoT sensors, manufacturing data, edge computing infrastructure, and AI models.

5. Dynamic Trust Assessment and AI-Assisted Access Control

The efficiency of the proposed Zero-Trust approach will be determined by the ability of this framework to constantly check whether the user, the device, the application, and the service need access to manufacturing resources. The traditional approach to authentication allows establishing the identity of a user at the very beginning of the session; nevertheless, the successful

authentication does not always mean that the entity will continue being trustworthy while interacting with the system. In the case of inter-connected manufacturing systems, the state of engineering workstations, IIoT devices, industrial gateways, applications, and remote services could change while operating; hence, Zero Trust needs to make access decisions based on the current security state (Mushtaq et al., 2025).

Dynamic trust assessment helps in facilitating such continuous decision-making process. Rather than providing permanent trust/un-trust status, the security status of an entity can be assessed based on the information gathered from various sources. This information can include the factors related to the assurance of the identity, device status, authentication history, communication pattern, requested resources, past security incidents, and current threats. Zero-Trust model for risk-based studies has proved the significance of considering the current as well as historical information in order to determine trust, where the suspicious behavior can impact future access decisions rather than considering the entity fully trustworthy after having normal behavior [18]. The context-aware models for IIoT environment also consider that the authorization should be flexible according to the changing conditions of user/device/network [19].

In the suggested architecture, such an assessment will be done via the Zero-Trust Policy and the Trust Engine presented in Section 4. For instance, one can consider the case of an industrial gateway that has passed the authentication stage and regularly communicates with certain production devices. In regular operation mode, the gateway is allowed to communicate with the specified set of resources in accordance with its permissions. If something unusual happens, and, for example, the gateway starts communicating with unauthorized PLC or has a degraded security status, the policy engine is able to reevaluate this connection. In accordance with the level of risk, the connection can remain the same, be limited only to certain resources, require additional validation, or be completely blocked.

In the case of human users and applications, the same concept may be applied. While an engineer might typically have access to design data or equipment assigned for manufacturing purposes, an unusual request to change settings on several controllers, access resources beyond the engineer's responsibilities, or use a strange piece of equipment will prompt further authentication. The nature of resources in question must also be taken into account. Accessing information that is not critical to production does not mean that the same degree of verification is necessary as in cases involving modification of PLC settings, programming robots, changing settings on the digital twin, or deploying new AI algorithms.

Monitoring using AI is useful in this aspect by analyzing the vast amount of telemetry that is collected in smart manufacturing systems. Network traffic, authentication events, device communications, activities within applications, system logs, and activities could be used as a way of detecting any anomalies or suspicious activities. With AI-supported cybersecurity practices, the complex pattern or anomaly detection could be done with ease unlike signature-based methods (Lezzi et al., 2025). In AI-enabled factories, AI can help detect any abnormal communications between devices, user actions, data transfers, or interaction between the cyber and physical entities.

Nevertheless, it is important to note that the security decisions made by AI should not be considered automatically reliable. AI models may generate false alarms, find themselves in unfamiliar operational conditions, or even be hacked intentionally. Therefore, the suggested architecture considers the information about anomalies produced by AI as one part of the overall security context, and not as the only reason to give or deny access. Important operations concerning assets which are critical for the safety or production processes might also need some pre-established policies, stricter authentication, or even human approval.

As a result, dynamic trust evaluation and AI-based monitoring become a continuous feedback loop in the suggested architectural framework. Information related to security collected at identity, device, network, application, data, and AI levels becomes continuously provided to the policy decision engine. Any behavioral changes or changes in security posture, therefore, lead to appropriate adjustments of access rights. The use of contextual assessment, least privilege authorization, continuous monitoring, and AI-based anomaly detection makes it possible to achieve adaptive security and maintain operational requirements of AI-powered smart manufacturing. It is important, however, to take into account several issues related to implementation that need to be addressed and are described in the next section.

6. Implementation Challenges, Benefits, and Future Directions

The discussed architecture promises numerous advantages for AI-powered intelligent manufacturing; however, its deployment calls for an in-depth evaluation of the peculiarities of operation of industrial facilities. First, unlike typical corporate networks, manufacturing systems commonly use not only new IIoT and AI technologies but also older devices that utilize PLCs, SCADA systems, proprietary protocols, and equipment designed to have a very long operational life. Such assets were often created before continuous authentication and advanced cryptography became necessary. Thus, the deployment of Zero Trust may require some intermediary solutions, such as gateways or proxies, to enforce security policies without modifying the old equipment directly. Recent research names brownfield legacy integration as one of the unsolved problems for deployment of Zero Trust in the era of Industry 5.0 and IIoT (Powell et al., 2022). The same problem is mentioned in the NIST report on integration of legacy industrial assets with digital infrastructures [20].

A second issue related to this is the trade-off between verification and manufacturing in real-time. The Zero Trust model involves constant assessment of identity and access management and this could mean increased communication and computing load. This might be an acceptable overhead in enterprise settings but it would be more noticeable in industrial manufacturing processes. It is essential then that the process of authentication, policy assessment, and monitoring is done without increasing unacceptable latency or interfering with the deterministic manufacturing processes. Some recent reviews indicate that latency, resource constraints, policy complexity and scalability should be considered while implementing Zero Trust into heterogeneous IoT and industrial systems [21]. One way of dealing with this might be using edge devices to process security information locally without having to move each decision to cloud computing.

However, these difficulties do not undermine the capacity of such architecture to mitigate the impacts of a successful intrusion. With explicit verification and least privilege authentication being applied, there will not be any unnecessary accesses to the production environment, while micro-segmentation will prevent the lateral spread when a user/device is compromised. Monitoring constantly will make it easier to observe interactions between IT, OT, IIoT and AI systems to detect malicious behavior earlier. At the same time, securing the AI models themselves and their related data within the same security architecture will take Zero Trust beyond traditional network security [22].

Interoperability and scalability still constitute significant obstacles to implementation. There could be thousands of different devices with varying operating systems, protocols, computation capacities, and security features in a major manufacturing plant. The management of the identities, policies, certificates, telemetry, and access permissions among this disparate range of devices could become quite complicated. In addition, the lack of standardized methods to communicate contextual security information in heterogeneous environments can make policy enforcement difficult (Ma & Chiu, 2025). Consequently, the process of implementation needs to be gradual starting from the determination of important assets and communications, and then implementing identity management, asset segmentation, policy enforcement, and expanding continuous monitoring and access control.

Future work should be devoted to the enhancement of the flexibility and industriality of Zero-Trust architectures. The first one is the creation of lightweight and backward-compatibly secure mechanisms that allow for the inclusion of constrained industrial devices in Zero-Trust frameworks without a need for equipment replacement. Another one is the distributed or edge enforcement of policies which would allow for the provision of manufacturing needs in real-time and minimize dependency on centralized security frameworks (Powell et al., 2022). Research on the topic of explainable AI for the purpose of security monitoring is necessary in the case where anomaly information generated by AI influences access to critical safety or production resources.

Some other potential applications can include federated learning in order to implement threat detection privately among multiple production facilities, digital twin technology in order to test cyber attacks virtually prior to implementing security policies to actual machinery, lifecycle management of AI models with regard to security, and post-quantum protection of industrial infrastructure assets. According to current research, federated learning, post-quantum security, adaptive trust compatible with legacy systems, as well as integrated Zero-Trust technologies within the industrial environment appear to be underdeveloped fields of study (Powell et al., 2022). Experimentation will need to go beyond purely cybersecurity-based metrics and assess joint effects of Zero Trust on detection capabilities, access control efficacy, latency, scalability, availability of production, and overall resiliency under industrial conditions.

7. Conclusion

In addition to the increased use of AI, Industrial IoT, cyber-physical systems, edge, and cloud computing, intelligent automation is bringing about significant changes in traditional manufacturing setups through the emergence of smarter manufacturing systems. Despite all that, increased vulnerabilities arise from increased dependencies between IT/OT, industrial devices, applications, data, and AI models and the increased attack surface created by these technologies. It is impossible for perimeter-based security to work in this case since location and previous authentication are not a clear indicator of continued trust. Zero Trust Security offers a solution through resource-centric security that includes authentication, authorization, least-privilege access, and security posture assessment (Mushtaq et al., 2025).

This paper suggested Zero-Trust architecture for smart manufacturing systems enabled by AI that combines aspects of identity and access security, security of devices and operational technology, security of networks and communications, security of data, applications and AI as well as constant AI-based monitoring. The aforementioned aspects are combined through the use of Zero-Trust Policy and Trust Engine which evaluates context-dependent information related to security and makes it possible to make adaptive access decisions. In contrast to the traditional approach of providing perpetual trust to users who passed authentication process, the proposed one takes into account changes in device postures, access behavior, network behavior, sensitive resources and security threats constantly.

One of the significant features of the suggested framework is the consideration of AI as a tool for increasing cybersecurity capabilities, as well as a manufacturing asset that needs to be protected. AI-driven monitoring will be helpful for anomaly and

threat detection; meanwhile, AI models, datasets, and output results should be protected from being accessed or manipulated. The combination of these two needs in a unified Zero-Trust framework will be beneficial for cybersecurity in modern intelligent manufacturing systems. Nevertheless, when implementing such an architecture in practice, it will be necessary to take into account the legacy OT infrastructure, real-time communication, interoperability, computational load, scalability, and manufacturing operations' continuity. Thus, future research should experimentally evaluate the proposed framework in realistic industrial settings and analyze the cybersecurity efficiency, latency, scalability, and effect on manufacturing process of this framework. Zero Trust, in turn, should be considered as an adaptive security strategy rather than as a separate technology.

Funding: Funding information was not supplied in the manuscript.

Conflicts of Interest: A conflict-of-interest declaration was not supplied in the manuscript.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

- Alqudhaibi, A., et al. (2026). Proactive cybersecurity in Industry 4.0: A survey of cybersecurity threat prediction approaches in manufacturing systems. *International Journal of Information Security*, 25(1). <https://doi.org/10.1007/s10207-025-01188-9>
- Ananthkrishnan, V. (2026a). Enterprise data migration strategies for high-assurance information systems. *Frontiers in Computer Science and Artificial Intelligence*, 5(5), 10–16. <https://doi.org/10.32996/jcsts.2026.5.5.2>
- Ananthkrishnan, V. (2026b). Governance frameworks for large-scale ETL ecosystems in complex data environments. *Journal of Computer Science and Technology Studies*, 8(5), 82–87. <https://doi.org/10.32996/jcsts.2026.8.5.5>
- Ananthkrishnan, V., Kunju, S. S., & Pachyappan, R. (2024). Autonomous GenAI agents for legacy-to-cloud ETL modernization. *Journal of Artificial Intelligence General Science*, 1(1), 274–290. <https://ideas.repec.org/a/das/njaigs/v1y2024i1p274-290id377.html>
- Bădoi, C. I., Çetin, B. K., & Çetin, K. (2026). Information integration for Industry 5.0: A review of IIoT–edge–cloud architectures with 6G/ISAC capabilities. *Journal of Industrial Information Integration*, 52. <https://doi.org/10.1016/j.jii.2026.101117>
- Barbosa, G. N. N., Andreoni, M., Nguyen, T. M. T., & Mattos, D. M. F. (2026). Zero trust architecture for internet of things devices and next-generation networks: Tools, trends, and challenges. *Annales des Télécommunications/Annals of Telecommunications*. <https://doi.org/10.1007/s12243-026-01197-2>
- Crowther, K. G. (2024). Blending shared responsibility and zero trust to secure the industrial internet of things. *IEEE Security & Privacy*, 22(5). <https://doi.org/10.1109/MSEC.2024.3432208>
- Gambo, M. L., & Almulhem, A. (2026). Zero trust architecture: A systematic literature review. *Journal of Network and Systems Management*, 34(1). <https://doi.org/10.1007/s10922-025-09998-x>
- Huma, Z. E., Jan, S. U., Ahmad, J., Buchanan, W., & Pitropakis, N. (2026). Adversarial machine learning in IoT security: A comprehensive survey. *ACM Computing Surveys*, 58(8). <https://doi.org/10.1145/3785665>
- Julio, Y. R., et al. (2026). OT cybersecurity: From perimeter security to zero trust: An AI-governed OT cybersecurity architecture for industrial systems. In *International Conference on Electrical, Computer, and Energy Technologies (ICECET 2026)*. <https://doi.org/10.1109/ICECET65726.2026.11633158>
- Lezzi, M., Montefusco, P., Lazoi, M., & Corallo, A. (2025). AI-based cybersecurity for a sustainable digital industry: Systematic literature review and future research directions. <https://doi.org/10.1016/j.jii.2025.100980>
- Ma, Y. W., & Chiu, P. H. (2025). A novel risk-based access control engine in zero trust architecture for IoT network. *International Journal of Information Security*, 24(3). <https://doi.org/10.1007/s10207-025-01030-2>
- Mallidi, R. K., Sharma, M., & Singh, J. (2021). Legacy digital transformation: TCO and ROI analysis. <https://doi.org/10.32985/IJECES.12.3.5>
- Mao, Y., Fu, W., Zhao, Y., Yuan, Z., Sun, Z., & Zhao, Y. (2025). A zero-trust access control model based on attribute and dynamic trust evaluation for cloud environments. *Symmetry*, 17(12). <https://doi.org/10.3390/sym17122059>
- Mushtaq, S., Mohsin, M., & Mushtaq, M. M. (2025). A systematic literature review on the implementation and challenges of zero trust architecture across domains. <https://doi.org/10.3390/s25196118>
- Powell, M., et al. (2022). Protecting information and system integrity in industrial control system environments. *NIST Special Publication 1900-10*.
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-207>

- Stodt, F., Reich, C., & Theoleyre, F. (2025). Beyond static security: A context-aware and real-time dynamic zero trust architecture for IIoT access control. *IEEE Internet of Things Journal*, 12(17). <https://doi.org/10.1109/JIOT.2025.3579028>
- Toussaint, M., Krifa, S., & Panetto, H. (2024). Industry 4.0 data security: A cybersecurity frameworks review. *Journal of Industrial Information Integration*, 39, Article 100604. <https://doi.org/10.1016/j.jii.2024.100604>
- Wan, T., Shi, B., & Wang, H. (2025). A continuous authentication scheme for zero-trust architecture in industrial internet of things. *Alexandria Engineering Journal*, 122. <https://doi.org/10.1016/j.aej.2025.03.012>
- Zanasi, C., Russo, S., & Colajanni, M. (2024). Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. *Ad Hoc Networks*, 156. <https://doi.org/10.1016/j.adhoc.2024.103414>
- Zarreh, A., Wan, H. D., Lee, Y., Saygin, C., & Al Janahi, R. (2019). Cybersecurity concerns for total productive maintenance in smart manufacturing systems. In *Procedia Manufacturing*. <https://doi.org/10.1016/j.promfg.2020.01.067>