Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th February 2026. Vol. 5. No. 2; e-ISSN: 2808-4519

Basic Analysis of Cybersecurity in Facing Digital Threats in the Industrial Era 5.0

Mellina Izzetil M[1*], Elsa Ayu Wardani[2], Anisah Fitriah[3], A. Hamdani[4]

[1,2,3,4]*Sains dan Teknolgi Universitas Ibrahimy*
Mellinaizzetil@gmail.com[1 *], elsawardani216@gmail.com[2], fitriahanisah2005@gmail.com[3], dan.kidz88@gmail.com[4]

Abstrak

Industry 5.0 focuses on cooperation that puts people first, as well as sustainability and resilience. Advanced technologies such as artificial intelligence (AI), industrial internet of things (IIOT), and robots that work alongside humans (cobots) are integrated into this industry. Because there is a better connection between the physical world and the digital world, this increase has a greater impact on increasing the risk of digital attacks, thus threatening data, systems, and even human safety. This research aims to analyze in depth the foundations of cybersecurity in the context of industry 5.0, as well as find strategies that can adapt to the evolving digital threats. The methods used are a systematic review of reading materials and descriptive qualitative analysis of existing cybersecurity frameworks, such as NIST, ISO 27001, and IEC 62443, especially in the context of industrial technology 5.0. The results show that there needs to be a shift from protection that is only around physical boundaries to a more proactive, distributed, and risk-based security model. This model emphasizes the importance of zero trust architecture, End-to-end data protection, and AI-enhanced threat monitoring. In addition, awareness and training of the workforce has also been found to be an important part of cybersecurity.

Keywords: *Cybersecurity, Industry 5.0, Digital Threats, Industrial IoT (IIoT), Zero Trust, Cyber Resilience.*

1. Introduction

The development of digital technology in the last two decades has changed the way organizations manage businesses, provide services, and process data. The previous industrial revolution took place from the mechanistic stage (Industry 1.0), electrification (2.0), automation (3.0), to intelligent digitalization (4.0), now it is heading to a new round, namely Industry 5.0. At this stage, technology not only plays a role as an automation tool, but also as *a collaborative partner* for humans through the integration of artificial intelligence (AI), *Industrial Internet of Things* (IIoT), collaborative robots (cobots), big data, and cyber-physical *systems* (CPS). Industry 5.0 emphasizes an approach that emphasizes humans, sustainability, and resilience, so that human-machine collaboration becomes the main foundation in creating a more personalized and adaptable production and service system.

However, the increasing connection between physical devices and the digital world is drastically expanding the digital attack surface. Every sensor, cloud-edge connection, IIoT device, and integrated CPS system presents a potential entry point for attackers. The increasing reliance on digitalization also increases the risk of cybersecurity incidents that have an impact not only on data compromise, but also physical consequences that can harm humans (*human-in-the-loop*).

Modern cyber threats are growing more complex. Attacks such as ransomware, *deepfake phishing*, industrial data theft, *IoT hijacking*, and AI-based polymorphic malware are now challenges that must be anticipated. Attackers are leveraging AI to create faster, more adaptive, and harder-to-detect methods of attack. This condition shows that the traditional security paradigm that relies on *perimeter-based security* is no longer adequate to deal with threat dynamics in the Industry 5.0 era.

Indonesia as a country with internet penetration of 77% in 2023 is in a vulnerable position. The BSSN report recorded 370.02 million cyberattacks in 2022, an increase from 266 million attacks in the previous year. This increase shows that the acceleration of digitalization has not been accompanied by optimal security readiness. With increasingly massive digital integration in the public sector, manufacturing, energy, healthcare, and financial services industries, the need for a strong cybersecurity foundation is becoming even more urgent.

In this context, proactive, adaptive, and distributed security models are needed, such as Zero Trust Architecture, end-to-end data protection, IIoT security based on global standards (ISO 27001, NIST Cybersecurity Framework, IEC 62443), and continuous threat monitoring systems strengthened by AI analytics. In addition to technical aspects, improving cybersecurity literacy and training human resources are important components to build effective digital resilience.

Based on this background, this study aims to recognize and analyze the basics of cybersecurity that need to be strengthened in dealing with digital threats in the Industry 5.0 era. Specifically, this study attempts to answer the following questions:

1. What are the development and characteristics of cyber threats in the Industry 5.0 era?
2. What are the basic principles of cybersecurity that are relevant and should be applied in the modern industrial environment?
3. How is Indonesia's readiness to build cybersecurity resilience to face challenges in the Industry 5.0 era?

Thus, this research is expected to provide a comprehensive understanding and strategic recommendations to support the development of a safe, resilient, and sustainable industrial ecosystem in the Industrial 5.0 era.

2. Literature Review

2.1. The concept of Industry 5.0 and the differences from industry 4.0

Industry 4.0 is a period of digitalization and automation through the application of technologies such as the Internet of Things (IoT), cloud computing, big data, and cyber-physical systems (CPS). The goal is to make the production process more efficient and automated with the help of intelligent machines. However, now Industry 5.0 has emerged, which actually not only focuses on efficiency, but also puts people first in the midst of an industrial ecosystem.

Menurut Breque et al. (2021), Industri 5.0 berlandaskan tiga pilar utama:
1. Human-Centric, which is the design of a production system that ensures that humans remain in control and work side by side with technology.
2. Sustainable, which is the use of technology to support energy efficiency, waste reduction, and environmentally friendly processes.
3. Resilient, which is the ability of the system to survive and recover from disruptions, including cyber disruptions.

Unlike Industry 4.0 which focuses on automation, Industry 5.0 emphasizes collaboration between humans and collaborative robots (*cobots*), deeper integration of CPS, and the use of generative AI, IIoT, and big data as support for adaptive and intelligent production processes. Key technologies supporting Industry 5.0 include:
1. Artificial Intelligence dan Machine Learning, untuk pengambilan keputusan otomatis dan prediktif.
2. Industrial Internet of Things (IIoT), yang menyediakan konektivitas antarmesin dan sensor.
3. Cyber-Physical System (CPS), sebagai integrasi dunia fisik dan digital.
4. Blockchain, untuk menjamin transparansi, integritas, dan akuntabilitas data

With these characteristics, Industry 5.0 is not only efficient but also has a social and ecological impact

2.2. Digital Threat Landscape in Industry 5.0 Key Threats Include:

The increasing use of IIoT devices, CPS systems, and AI has made cyber threats in industrial environments even more complex. According to researchers such as Mahendra (2023), cyber threats in the Industrial 5.0 era are no longer simple, but multidimensional because attacks can directly affect physical processes, industrial infrastructure, and even human safety.

Some of the main threats to Industry 5.0 are as follows:

a. Supply chain attack
   Attackers exploit vulnerabilities in software, firmware updates, or third-party components to gain access to industrial systems. The SolarWinds attack (2020) is a relevant global example.
b. IIoT and CPS vulnerabilities
   IIoT devices often have computational limitations, lack security update mechanisms, and use default protocols that are easy to exploit. This makes it one of the attackers' favorite entry points.
c. Threats to AI/ML (AI-based attacks)
   AI models can be attacked through:
   1. Data poisoning, inserting malicious data to affect the model's output.
   2. Inversion attack model, to extract sensitive training data.
   3. Adversarial examples, manipulate inputs so that the AI model makes the wrong decision.
d. Ransomware and industrial malware
   Ransomware attacks can stop factory operations, lock down SCADA systems, or damage production machine configurations. This type of attack has increased sharply in the manufacturing industry since 2021.

Thus, the digital threat landscape in Industry 5.0 is not only about data theft, but also the potential for physical interference that can hamper industrial operations and threaten human safety.

2.3. Cybersecurity Framework for Industry (Comparative Study)

Evaluate the application of standard frameworks such as IEC 62443 (which is specifically used for the IACS industry), NIST cybersecurity framework, and ISO/IEC 27001 (information security management systems/ISMS) in the context of industry 5.0 needs.

3. Metodologi Penelitian

This study uses a descriptive qualitative approach with a systematic literature study (SLS) method.

Here are the steps taken:

1. Data Source Collection: Collect journals, industry reports, and security standards from 2018–2025 with the keywords "Cybersecurity", "Industry 5.0", "Zero Trust", and "IIoT Security".
2. Content Analysis: Examine various frameworks and case studies of cybersecurity applications in intelligent industries.
3. Data Synthesis: Integrating findings from various sources to construct a cybersecurity model that is relevant to the Industry 5.0 era.

This approach allows for a thorough understanding of the cybersecurity foundations required in the context of rapid and dynamic technological change.

3.1. Data Collection

Search various literature such as, scientific journals, conference proceedings, industry reports, and official reports using keywords: cybersecurity, industry 5.0, digital threats, IoT security, and human-centered security.

3.2. Content Analysis

Pay attention to threats, vulnerabilities, and mitigation strategies suggested from relevant literature regarding the integration of key technologies in Industry 5.0 such as, (AI, IoT, Cobot).

3.3. Sintesis

Develop findings to bring together a flexible and comprehensive cybersecurity framework for industry 5.0.

4. Results and Discussion

4.1. Basic Pillars of Industrial Cybersecurity 5.0

Hasil analisis menunjukkan bahwa fondasi keamanan siber di era Industri 5.0 bertumpu pada tiga pilar utama, yaitu teknologi canggih, proses adaptif, dan manusia sebagai pertahanan utama. Ketiga pilar ini saling melengkapi dalam menciptakan sistem keamanan yang proaktif, resilien, dan berkelanjutan.

1. Advanced Technology and Security Architecture:
   a. Implement a Zero Trust (ZTA) architecture: every user, device, and application, both internal and external, must be verified before being granted access.
   b. End-to-End data security: uses quantum-resistant and blockchain cryptography (for supply chain integration) to protect sensitive data as it is transmitted and stored across the network.
2. Adaptive and standardization process:
   a. Continuous risk management: adopt the IACS (IEC62443) standard with a focus on dynamic, rather than periodic risk assessment.
   b. Cyber resilience: focuses not only on prevention but also on the ability to recover quickly from an attack, with a proven business continuity plan (BCP) and disaster recovery plan (DRP).
3. Human-Centric and Training:
   a. Improving cybersecurity: given the human-centered role, comprehensive and ongoing cybersecurity training is the first line of defense against social engineering attacks and operational errors.
   b. Designing human-centric security: ensuring that security policies and technologies do not hinder collaboration between humans and machines, but rather support safe and efficient operations.

4.2. Industry 5.0 Special Implementation Challenges

While there are various cybersecurity principles available, the application of those principles in the industry still faces some specific problems. These problems include:

1. IT–OT (Operational Technology) system integration:
   Many OT systems still use legacy *systems* and are not compatible with modern security protocols. The integration between flexible IT and rigid OT is one of the most significant challenges.
2. Lack of experts Experts in the field of Industrial Security:
   The industry needs professionals who understand IT security, OT security, and AI governance at the same time. The availability of such experts is still limited, especially in Indonesia.
3. Low local regulations and standards:
   There are no specific national regulations regarding the safety of IIoT, CPS, or cobots, so the industry has to refer to international standards (NIST, IEC 62443, ISO 27001) which sometimes require high adaptation.
4. High Implementation Costs:
   The implementation of advanced security systems such as ZTA, AI-based SIEM, or quantum cryptography requires large investments that are difficult for Small and Medium Industries (SMEs) to reach.

These challenges demonstrate the need for a more integrated national strategy to strengthen the industrial security ecosystem

4.3. Adaptive Cybersecurity Strategy

Based on the results of the literature synthesis, some of the relevant adaptive strategies to be applied in the Industry 5.0 era are as follows:

1. Penerapan Multi-Layered Defense:
   Includes multi-layered protection from endpoints, networks, applications, production systems, to CPS, with integration of incident detection and response systems.
2. Cross-Industry and Government Collaboration:
   Cooperation is needed in the form of *threat intelligence sharing*, a national early warning system, and an industrial sector security forum.
3. Utilization of AI in Predictive Security:
   The use of AI to recognize attack patterns, predict anomalies, and automate responses before attacks has a far-reaching impact.
4. Periodic Security Audits and Assessments:
   Regular audits are required to measure gaps against international standards such as ISO/IEC 27001, NIST CSF, and IEC 62443.

Because of this, this challenge shows the need for a more comprehensive mass strategy to strengthen security systems in the industry.

5. Conclusion

The Industrial Era 5.0 offers great opportunities in increased efficiency, personalization, and innovation, but it also presents increasingly complex and exponential cybersecurity risks. The results of the analysis in this study show that the successful implementation of cybersecurity in Industry 5.0 must be built on three main pillars, namely advanced technology, adaptive processes, and humans as key elements of defense.

The implementation of Zero Trust architecture, end-to-end data security strengthening, and the use of AI for anomaly detection and incident response are critical components in dealing with modern digital threats. In addition, dynamic risk management processes, the implementation of industrial security standards (IEC 62443, NIST CSF, ISO 27001), as well as cyber resilience that includes recovery and business continuity, are increasingly important in a real-time connected industrial ecosystem.

Human factors remain central to the Industry 5.0 security ecosystem. Training, security awareness, and a strong cyber hygiene culture are the first line of defense against social engineering, operational errors, and internal threats.

Without comprehensive readiness to strengthen these pillars, the transformation towards Industry 5.0 can be hampered and pose significant risks to data, systems, industrial processes, and even human safety.

5.1. Advice and Advanced Research

Further research is recommended to conduct an empirical study on the application of Zero Trust architecture and AI-based anomaly detection in IIoT and CPS environments in Indonesia, so that its effectiveness can be evaluated directly. In addition, it is necessary to develop a cybersecurity governance framework specifically designed for Industry 5.0, including ethical and sustainability aspects in the use of AI. Improving the competence of cybersecurity human resources and studying national regulations related to digital industry security is also important to support the implementation of a safe and resilient Industry 5.0.

References

[1] Aintzane Mosteiro-Sanchez, Marc Barcelo, Jasone Astorga, & Aitor Urbieta. (2022). *Securing IIoT using Defence-in-Depth: Towards an End-to-End Secure Industry 4.0.* arXiv.
[2] Bruno Santos, Rogério L. C. Costa, & Leonel Santos. (2024). *Cybersecurity in Industry 5.0: Open Challenges and Future Directions.* arXiv.
[3] Amit Lokare, Shripad Bankar, & Padmajeet Mhaske. (2025). *Integrating Cybersecurity Frameworks into IT Security: A Comprehensive Analysis of Threat Mitigation Strategies and Adaptive Technologies.* arXiv.
[4] Ade Irawan, Wildan H. N. Fadholi, Zahwa Erikamaretha, & Fried Sinlae. (2024). *Tantangan dan Strategi Manajemen Keamanan Siber di Indonesia berbasis IoT.* JOURNAL ZETROEM, 6(1), 114–119.
[5] Ratih Windari & Sriyanto. (2024). *Tinjauan Implementasi NIST Cybersecurity Framework (CSF) di SMKN4 Bandar Lampung.* Journal Ilmu Komputer, Sistem Informasi, Teknik Informatika, 3(1).
[6] Hafizh Ghozie Afiansyah & Nur Annisa Kadarwati Febriyani. (n.d.). *Penyusunan Kebijakan Pengamanan dan Pengelolaan Infrastruktur Operasi Keamanan Siber Menggunakan NIST CSF 2.0 dan ISO/IEC 27001:2022.* Info Kripto.
[7] Nurbojatmiko, N., Karimiyah, M. S. K., Asnadi, N. M., & Anisyah, R. (2025). *ISO 27001 As Information Security Solution In Society 5.0 Era: Systematic Literature Review.* Sinkron: Jurnal dan Penelitian Teknik Informatika, 9(1), 484–492.
[8] Muhammad Noor Hasan Siregar & Mardiah. (2025). *Analisis Keamanan Data pada Sistem Informasi Menggunakan Metode ISO/IEC 27001.* Jurnal Ilmu Komputer dan Teknik Informatika, 1(2), 58–64.
[9] Mohammad Afdhal Jauhari, Bheta A. Wardijono, & Ega Hegarini. (2024). *Pengukuran Kematangan Keamanan Siber pada Perusahaan TI dengan Framework CIS Controls.* Jurnal Saintekom, 14(1).
[10] Irawan, Hafizhan. (2024). *Evaluasi dan Audit Tata Kelola Keamanan Siber menggunakan NIST CSF, ISO/IEC 27002 dan CIS Controls v8.* (Tesis, Universitas AMIKOM Yogyakarta).