INNOVATIVE WORLD
Ilmiy tadqiqotlar markazi

INNOVATSION TALABALAR AXBOROTNOMASI

htttps://innoworld.net

+998335668868

ILMIY JURNAL

INNOVATSION TALABALAR AXBOROTNOMASI

3-JILD, 3-SON
2026

Jurnal quyidagi xalqaro bazalarda indekslanadi:

Google Scholar | doi digital object identifier | ResearchGate | zenodo

ADVANCED SCIENCE INDEX | OpenAIRE | Academic Resource Index ResearchBib | DRJI Directory of Research Journals Indexing

Ilmiy jurnalning rasmiy sayti:
www.innoworld.net

O‘ZBEKISTON-2026

Security Issues on Industrial Internet of Things: Overview and Challenges

G'anijonov Mukhammadali Shavkatbek o 'g'li
Master student of Sharda University Uzbekistan

Abstract: The Industrial Internet of Things (IIoT), where numerous smart devices associated with sensors, actuators, computers, and people communicate with shared networks, has gained advantages in many fields, such as smart manufacturing, intelligent transportation, and smart grids. However, security is becoming increasingly challenging due to the vulnerability of the IIoT to various malicious attacks. In this paper, the security issues of the IIoT are reviewed from the following three aspects:

1. security threats and their attack mechanisms are presented to illustrate the vulnerability of the IIoT;
2. the intrusion detection methods are listed from the attack identification perspectives; and
3. some defense strategies are comprehensively summarized. Several concluding remarks and promising future directions are provided at the end of this paper.

Keywords: IIoT; security analysis; attacks; defense strategies; communication protocol

Introduction. Communication technology, big data, and edge computing, which are deeply in tegrated with the industrial economy, promote the booming development of the IIoT (Industrial Internet of Things). Industrial networks, especially Industrial Control Systems (ICSs) and the IIoT, are no longer isolated environments. The introduction of the communication network and advanced computing technology has brought many benefits to the IIoT, such as low costs, easy maintenance, and high efficiency. However, the spread of network security threats is also accelerating in the industrial field, which harms the operation of the IIoT. Because many new and complex attacks are being distributed in all physical and cyber spaces, the existing security mechanisms in the current IIoT are not sufficient for addressing the increasing security demands, allowing multiple security problems to emerge in various industrial application scenarios. A large amount of industrial equipment can be easily threatened or damaged by illegal intruders, which can even lead to large-scale security incidents. In 2018, the CICS-CERT conducted research and evaluation based on relevant collected data and found that a total of 432 security vulnerabilities existed in the industrial control systems, smart devices, and IoT fields. These vulnerabilities were primarily distributed in the key manufacturing, energy, water, and chemical industries. Out of these vulnerabilities, 276 were high-risk, and 151 were medium-risk, accounting for 99% of the total. Buffer overflow vulnerabilities were the most common type, accounting for as much as 20% of the total. The five most common types of vulnerabilities were authentication error vulnerabilities, permission control vulnerabilities, information disclosure vulnerabilities, and input validation vulnerabilities. According to the report by the CICS-CERT, the number of identifiable industrial control systems and smart devices on the Internet in China currently exceeds 10,000, and approximately 89% of the devices and systems are still not using effective security measures. The number of industrial control system vulnerabilities has exploded, and industrial control system attacks have exhibited an upward trend.

The basic architecture of the IIoT and the security issues. In this section, the basic architecture of the IIoT and the security issues corresponding to each structure level are discussed. As shown in Figure 1, the general architecture of the IIoT is divided into four main parts: the device layer, application layer, transport layer, and processing layer.

The device layer consists of many devices distributed in the IIoT infrastructure field. Because the devices connected to the IIoT are relatively fragile and vulnerable to network attacks, managing the security of the IIoT is extremely difficult. The baseband chip is one of the most critical components in the wireless communication module, which incurs a high cost. In addition, the industry is relatively concentrated, and the materials are usually provided by foreign manufacturers. Driven by their own interests, some overseas manufacturers often arrange "connected households". Once exposed, these manufacturers hide, steal, or destroy important data under the pretext of product defects. With the popularization and application of smart factories, many previously relatively closed devices or systems have been connected to networks, which exposes the distribution and use of industrial equipment to the network. Devices produced solely to complete operations are very fragile. While production is becoming more efficient, these devices may also be manipulated by illegal molecules, which poses a great threat to the security of the devices or systems in the industrial network. Supervisory Control and Data Acquisition (SCADA) networks provide interconnection for field devices on the factory floor. These field devices, such as sensors and actuators, are monitored and controlled via a SCADA network by a PC or programmable logic controller (PLC). SCADA networks are IT systems designed to oversee technical or production processes. The specific functions of a production process monitoring system include collecting current data from measuring elements, visualizing the data, controlling the production process, alerting to errors or deviations, and archiving data using a comprehensive database. SCADA systems play an excellent role in PLCs and other equipment that directly affects the production process. However, multiple access points are available in the SCADA network, and attackers can enter any machine in the IIoT through these access points. Additionally, SCADA networks use commercial off-the-shelf (COTS) hardware and software for equipment development. The use of COTS equipment has resulted in many SCADA development protocols needing to run over traditional Ethernet and TCP/IP. These protocols are usually serial line-based protocols that are placed in TCP packets through standard process encapsulation, and these protocols usually provide additional application layer interfaces. When incorporated with an enterprise network, production information can be easily collected for higher-level management. However, these services also make devices on the SCADA network vulnerable to application layer and TCP/IP-based attacks.

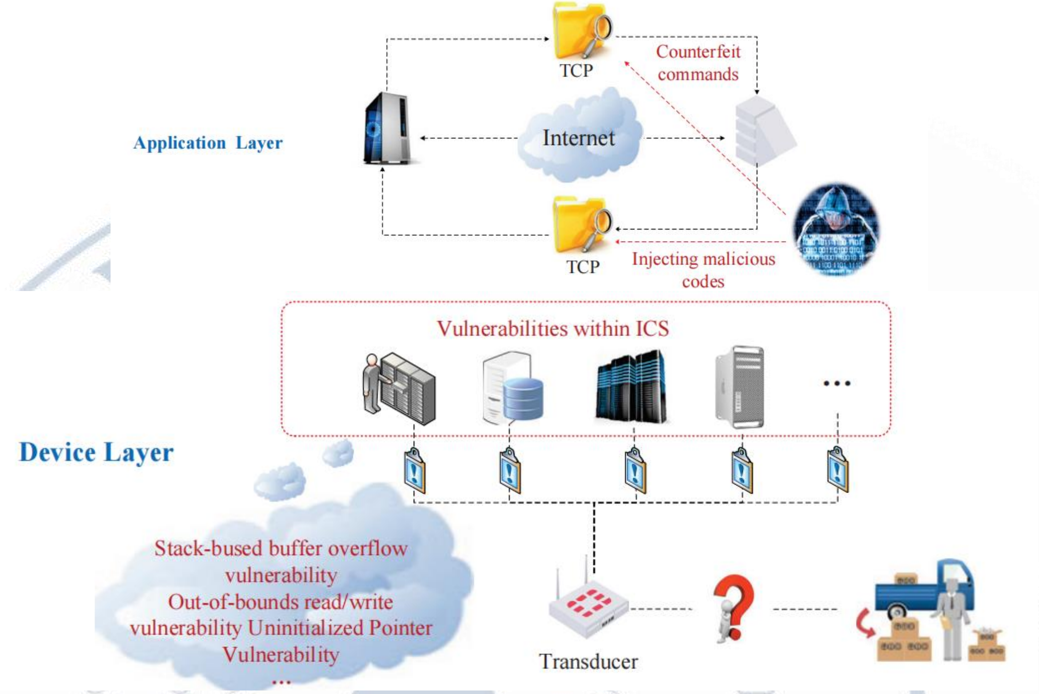
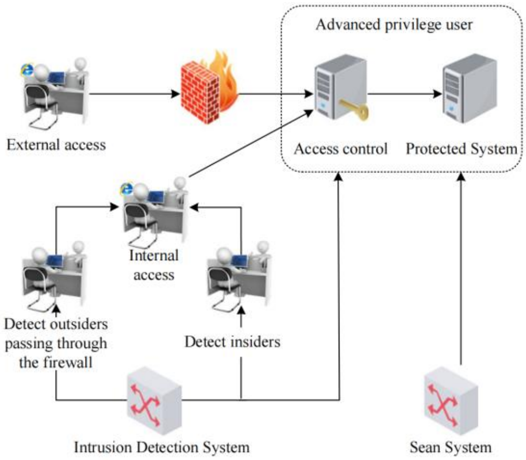

Application Layer
TCP
Counterfeit commands
Internet
TCP
Injecting malicious codes
Vulnerabilities within ICS
...
Device Layer
Stack-bused buffer overflow vulnerability
Out-of-bounds read/write vulnerability Uninitialized Pointer Vulnerability
...
Transducer

Figure 1. IIoT architecture.

The application layer mainly uses transport layer protocols (such as the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)) to support the transfer and exchange of data between host-to-host, client–server, or peer-to-peer models. Because the TCP/IP used by the IIoT is open and transparent, the IIoT is vulnerable to intrusion attacks by third parties. Network attack measures are gradually maturing, which greatly increases the probability of network security problems.

The Solutions to Security Protection of IIoT. Intrusion Detection technology monitors and detects internal and external network attacks and internal error operations in real time through intrusion detection systems (IDSs). The IDS is generally deployed in the local computer or the key node of the computer network. It collects, detects, and analyzes the activity status of users, systems, networks, etc., without affecting normal operations. Its detection objects and scope of operation are shown in Figure 2.



Conclusions. The security issues of the IIoT have been reviewed in this paper. Thus far, the security issues on the IIoT have been characterized by a wide range of applications under complex interactions among physical space, cyberspace, and various threats resources. Threats, detections, and defenses have been analyzed in detail, and security issues have been generally classified into the following categories based on the basic architecture of the IIoT:

• Threats to the IIoT. The equipment in the IIoT connected by the device layer is vulnerable to external attacks. Device exposure also greatly threatens the IIoT and industrial control system security.

• Attack detections. Due to the open communication protocol in the application layer, the IIoT is vulnerable to third-party intrusion attacks. The transmission layer and the processing layer are also very vulnerable to attackers during data transmission, with these attacks resulting in the leakage of a large amount of private and confidential information and irreversibly damaging the IIoT.

• Defenses against attacks. Many secure strategies have been developed to handle various malicious attacks from different perspectives. However, the deep integration of cyberspace and physical plants causes such defense or protection methods to only partially protect the IIoT.

References

1. Alenazi, M.J.; AlSowaygh, N.A.; Humayed, A.A.; Alablani, I.A. Cyber resilience in industrial networks: A state of the art, challenges, and future directions. J. King Saud Univ. Comput. Inf. Sci. 2023, 35, 101781.

2. Zhang, N.; Liu, L.; Tian, Z.; Wu, Y. Progress and trend of industrial Internet security. J. Guangzhou Univ. (Nat. Sci. Ed.) 2019, 18, 68–76.

3. Alrawi, O.; Lever, C.; Antonakakis, M.; Monrose, F. SoK: Security Evaluation of Home-Based IoT Deployments. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; pp. 1362–1380.

4. Yan, H.; Li, D. Industrial Internet Security Risk Analysis and Countermeasure Research. Cyberspace Secur. 2020, 11, 81–87.

5. Guo, X.; Liu, J.; Yu, Z.; Zhang, H.; Di, X. Prospect of Industrial Information Security Situation in 2019. China Inf. Secur. 2019, 6, 51–52.