

Cybersecurity Integration in Enterprise Architecture for IoT Infrastructure in Steel Manufacturing

Djarot Hindarto^{1)*}

^{1)*}Informatika, Fakultas Teknologi Komunikasi dan Informatika, Universitas Nasional, Jakarta

^{1)*}djarot.hindarto@civitas.unas.ac.id

ABSTRACT

As a result of the widespread adoption of Internet of Things technology in the steel manufacturing industry, there is an urgent requirement for the implementation of robust cybersecurity measures. The proliferation of IoT devices has caused a data explosion, which in turn has increased the risk of cyberattacks. The purpose of this research is to develop an enterprise architecture model that is capable of effectively managing cybersecurity risks on Internet of Things infrastructure in the steel manufacturing industry. This is a response to the urgent challenge that has been presented. The methodology utilized in this study is a rigorous qualitative approach, which involves the collection and analysis of data through interviews and literature reviews related to the topic. Following an in-depth analysis of the findings of the research, several important goals have been established. These goals include the identification of potential dangers, the reduction of potential risks, and the effective implementation of security controls. Within the context of the steel manufacturing industry, this research makes a significant contribution to the improvement of cybersecurity in Internet of Things infrastructure. In addition to identifying potential dangers and mitigating risks, the architecture model that has been proposed is about more than that. It offers a comprehensive and well-coordinated safety strategy, which guarantees a strong defense against cyber threats.

Keywords: Cybersecurity; Internet of Things; Mitigation Risk; Steel Manufacture; Threats

1. INTRODUCTION

The steel manufacturing industry has undergone a significant transformation with the implementation of Internet of Things (IoT) technology, which enables real-time monitoring and control of production processes. With IoT, various devices and machines in steel mills can connect and communicate with each other, enabling faster data analysis and more informed decision-making (Abawajy et al., 2021), (Sze et al., 2022). Using sensors and smart devices can help find problems before they get too bad, which cuts down on downtime and boosts productivity. IIoT also makes it easier for different parts of the production process to work together better, from processing raw materials to making the finished product. This makes the whole process more efficient and well-coordinated.

However, the adoption of IoT in the steel manufacturing industry also presents new challenges related to cybersecurity. Threats like malware, ransomware, and Distributed Denial of Service (DDoS) (Karthick et al., 2022), (Hindarto & Djajadi, 2023), (Saxena et al., 2023) attacks are becoming more likely to target IoT infrastructure that is connected to manufacturing systems. A literature review shows that these attacks can result in significant operational disruptions, hinder production processes, and cause substantial financial losses. In addition, cyberattacks can compromise sensitive data and damage a company's reputation in the eyes of customers and business partners.

In this situation, the steel manufacturing industry (Hindarto et al., 2021) needs to come up with and use a complete cybersecurity plan to keep IoT infrastructure safe from new threats. This research aims to analyze and evaluate the effectiveness of various existing security approaches and identify gaps between current security measures and ideal security needs. The problem formulation in this study is how to effectively integrate cybersecurity in enterprise architecture to protect IoT infrastructure (Amalia & Hindarto, 2024) in the steel manufacturing industry. The increasing frequency and sophistication of cyberattacks emphasizes the urgency of this problem.

The purpose of this research is to develop a comprehensive enterprise architecture model that includes cybersecurity measures to protect IoT infrastructure in the steel manufacturing industry. We will identify critical risks and weaknesses, develop effective risk reduction strategies, and implement comprehensive and immediate security

* Corresponding author



This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0).

measures. The results of this research are expected to provide practical guidance for steel manufacturing companies in implementing proactive and sustainable cybersecurity measures. These measures are not just theoretical concepts but strategies that can be used to make IoT infrastructure safer in the steel manufacturing sector.

2. LITERATURE REVIEW

According to wide-ranging literature reviews, enterprise architecture is the framework used to align business strategy with IT infrastructure. Many companies now prioritize cybersecurity to protect their assets from cyberattacks. Advanced security strategies can protect data integrity, confidentiality, and availability. As more devices transmit sensitive data over the Internet of Things (IoT), this protection is crucial.

Several viewpoints regarding Cybersecurity, Enterprise Architecture, and the Internet of Things:

The IoT ecosystem encompasses the architecture and business model of essential IoT services. This service is for innovation in hotel rooms, demonstrating the practical application and benefits of IoT technology in improving the user experience (Lee, 2021).

A framework that uses IoT, BIM, and blockchain to improve offsite manufacturing supply chain transparency and efficiency. This research shows how interconnecting Hyperledger Fabric-based decentralized systems can improve security, reliability, and quality control, as well as enable real-time supply chain optimization (Brandín & Abrishami, 2024).

Users lose control over data once they send it to the cloud, leaving it vulnerable to corrupt providers and complicating forensic investigations. The Secure Cloud Storage System (SCSS) is a fast identity-based cryptography (IBC) architecture that supports distributed key management with multiple public key generators (PKGs). It makes forensic investigations more secure and scalable while also being faster than other encryption and decryption methods (Unal et al., 2025).

Industry 5.0 employs a hierarchical fog computing architecture for critical energy systems, enhancing efficiency and security via attribute-based encoding (Rani & Srivastava, 2024). The article discusses IoT's potential in manufacturing innovation and uses LPDR algorithm to design products based on consumer needs and business growth (Babu et al., 2022).

Research shows innovations in IoT, enterprise architecture, and cybersecurity, but gaps remain: Cybersecurity has not been discussed in relation to IoT in hospitality. Supply chain IoT, BIM, and blockchain integration require enterprise architecture interoperability knowledge. The lack of study on SCSS effects on complex enterprise architecture underscores the need for your contribution to this area. Fog computing architecture for critical energy systems in Industry 5.0 needs more research on industrial sector integration. The integration of LPDR algorithm manufacturing innovation with enterprise architecture and cybersecurity is a crucial area that requires the attention and expertise of our audience. Research has the power to address these issues and significantly enhance the fields of IoT, enterprise architecture, and cybersecurity, offering a promising future.

3. METHOD

We developed and evaluated a cybersecurity-integrated enterprise architecture model for IoT infrastructure in the steel manufacturing sector using a qualitative research methodology. This research uses a qualitative approach with a focus on the integration of cybersecurity into enterprise architecture in the steel manufacturing sector. The scope of the study includes identifying basic ideas, recent developments, and best practices in enterprise architecture and cybersecurity. Research data was collected through a comprehensive literature review to identify basic ideas, recent developments, and best practices in enterprise architecture and cybersecurity. In addition, in-depth interviews and group discussions were conducted with key stakeholders, including IT teams, cybersecurity specialists, and operational managers. These data collection techniques were designed to gain a deep understanding of the business procedures and security issues encountered. Data analysis was conducted using thematic analysis methods to understand the business procedures and security issues encountered deeply. The results of this analysis were used to develop an enterprise architecture model consisting of three main elements: business, technology, and application architecture. In addition, risk analysis was used to assess the effectiveness of the model in addressing cybersecurity risks and improving operational efficiency. The steel manufacturing company used the evaluation findings to create a comprehensive blueprint that serves as an implementation guide, demonstrating the practical application of our research.

* Corresponding author



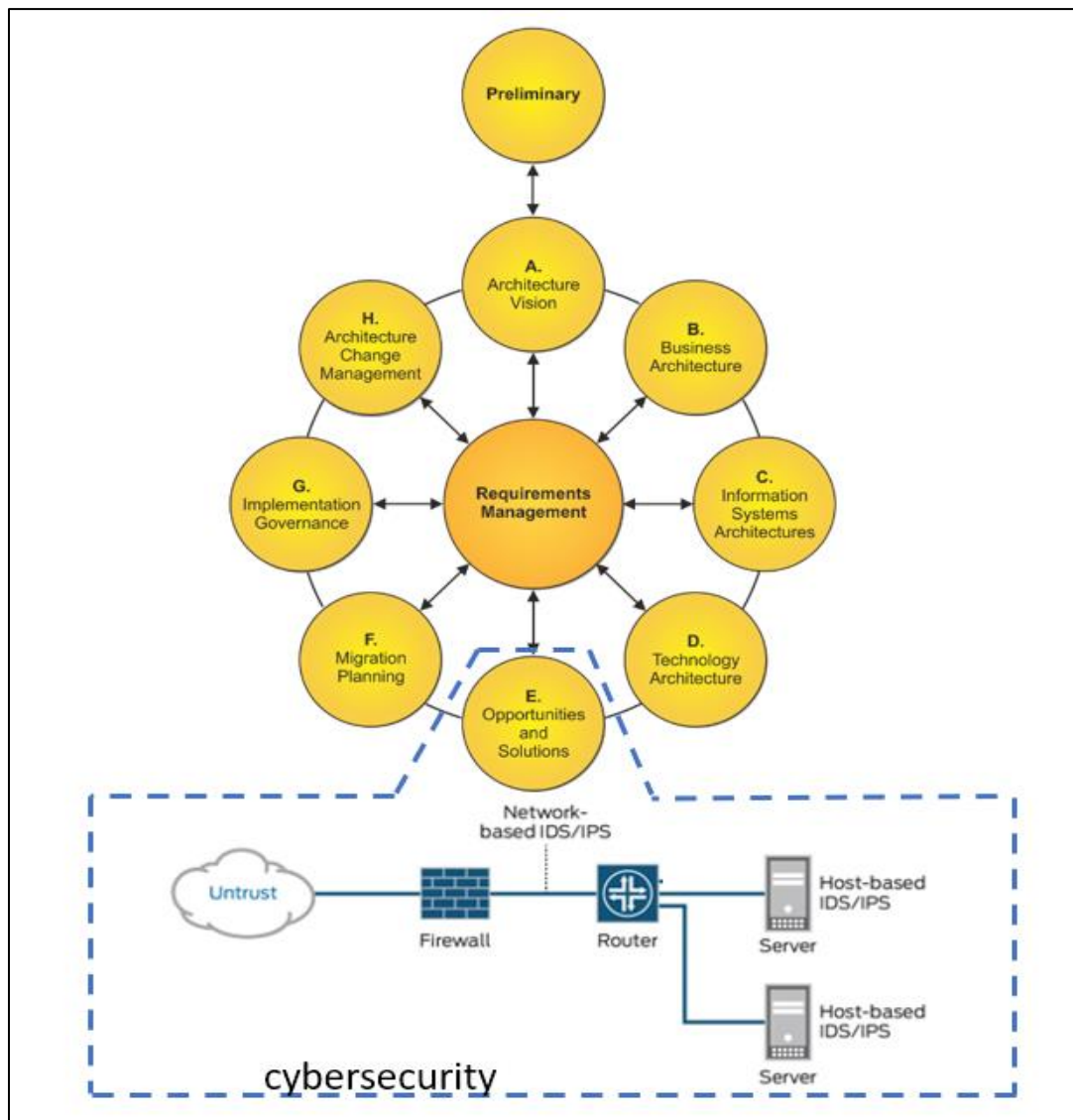


Fig.1 Proposed new method cybersecurity network and Enterprise Architecture

Figure 1 illustrates the process of developing an enterprise architecture for cybersecurity in the context of IoT infrastructure in the steel manufacturing industry. The literature review stage provides the foundation for learning about cybersecurity and enterprise architecture fundamentals, trends, and best practices. To understand a topic, a literature review searches scientific journals, books, industry reports, and conference papers. This literature review helps researchers identify and evaluate similar approaches and solutions. This process also helps identify current technologies and relevant methods for adaptation or expansion in this study. Literature reviews also identify research gaps that new studies must fill. Understanding previous research and implementation can help researchers create more specific and relevant research questions and a solid theoretical framework to support the proposed architecture model. The literature review also justifies the research and shows how it advances cybersecurity and enterprise architecture in the steel manufacturing industry. The literature review gives researchers a solid understanding of their theoretical and practical background, allowing them to move on.

Next, meet stakeholders. Collaboration is welcome from operational managers, IT teams, cybersecurity experts, and business representatives. This meeting seeks to understand IoT infrastructure cybersecurity business needs,

* Corresponding author

challenges, and expectations. Stakeholder meetings aim to unite stakeholders and advance a secure and efficient enterprise architecture. The next step was business understanding, in which the research team examined business processes. To understand how the steel manufacturing company works, the research team interviewed, observed, and analyzed documents. IoT integration's effects on supply chain management, production, and distribution were the focus. Researchers can identify IoT implementation flaws and security risks by identifying department workflows and interactions. This stage provides insight into daily operations and helps determine the company's cybersecurity needs and priorities.

The business understanding stage gathers information to create a business model with business architecture, technology architecture, and application architecture. Organizational structure, key business processes, and departmental relationships are defined by business architecture. We examine how IoT supports business goals and core processes and defends them with cybersecurity. Technology architecture, which encompasses IoT devices, networks, and control systems, enables business processes. It also covers infrastructure security measures like firewalls, intrusion detection, and encryption. Application architecture describes daily-use applications and their interactions. Each IoT application needs adequate security to prevent unauthorized access and maintain data integrity. Integrated and structured businesses can create a comprehensive and effective cybersecurity strategy to protect IoT infrastructure.

Implementing Zero Trust Security (ZTS) in enterprise architecture requires extensive testing and security technology deployment. This involved reconfiguring devices and systems for micro segmentation and end-to-end data encryption. All users and devices used multi-factor authentication (MFA) for layered verification before access. An IDPS was added to the network to monitor and respond to threats in real time. We also implemented dynamic security policies that adjust access and protection based on context and conditions. To solve technical issues and integrate with operations, IT teams and stakeholders worked closely together during implementation. Testing and validation were done in stages to ensure each component worked adequately and provided the expected security. After all elements were implemented and tested, the system was ready for a thorough evaluation to ensure cybersecurity improvement in steel manufacturing.

After creating the business model, evaluate it. We assess this architecture model for its ability to combat cybersecurity threats and improve operational efficiency. The evaluation process uses practical trials in simulated environments to mimic real-world operational conditions and risk analysis to identify security gaps. The research team can simulate a cyberattack to test the system's response and security controls. However, risk analysis helps assess and quantify threats to the IoT system and business operations. The evaluation results are crucial to improving the architecture model. Pilot test and risk analysis results help researchers improve security technologies and operational procedures. If data encryption fails to protect sensitive data, researchers can use a stronger encryption method. If network monitoring finds vulnerabilities that attackers can exploit, we may need more advanced detection and response systems. This evaluation and customization process ensures that the architecture model is theoretical, practical, and field-ready, protecting the steel manufacturing industry's IoT infrastructure.

Final step: enterprise architecture blueprint. This blueprint details every aspect of the designed architecture model, including organizational structure, technologies, and applications. The blueprint provides detailed steps for an enterprise to implement the proposed architecture model, focusing on cybersecurity integration. To ensure that all implementation parties understand and can follow the guide, we clearly explain each architecture element, from hardware and software configuration to security policies and procedures. There was a good cybersecurity strategy at the steelmaker. This blueprint unifies every part of the system to stop cyberattacks. The strategy calls for incident response, real-time network monitoring, and data encryption. The plan calls for training and awareness of employee security to guarantee cybersecurity awareness. These recommendations guarantee operational continuity, defend IoT infrastructure against cyberattacks, and increase security and efficiency.

4. RESULT

Application Architecture

In the implementation of application architecture (Hindarto et al., 2023) for the steel manufacturing industry, support applications play an important role in ensuring operational security and efficiency. These support applications include various systems and technologies designed to monitor and secure all production activities, from monitoring steel raw materials to shipping finished products. The process of monitoring steel raw materials involves the use of Internet of Things (IoT) devices equipped with sensors to collect real-time data on the quality and quantity of raw materials

* Corresponding author



available. The control center then receives this data for analysis, which serves as a foundation for decision-making in inventory management and production planning. In addition, the support application includes a monitoring system for the manufacturing process of steel products that uses robotics and IoT technology to ensure that each stage of production runs according to set standards. Sensors attached to machines and production devices continuously monitor data regarding temperature, pressure, and other operational conditions, enabling quick intervention in case of anomalies.

Data security is a crucial aspect of the integration of IoT technology and robotics in the steel manufacturing industry. IoT devices must secure the data they collect, which includes sensitive information about production processes and operational conditions, against potential cyber threats. Strong encryption algorithms must encrypt the data sent from IoT devices to the central server. Data encryption (Permana & Pratiwi, 2022) ensures that information remains protected during transmission, preventing unauthorized access and manipulation of data by potentially harmful third parties. The central server performs a decryption process once the data arrives, restoring it to its original form for further processing and analysis. This encryption and decryption process ensures data integrity and security, which is crucial to supporting accurate and efficient decision-making in production management. Thus, the support application not only serves to monitor and manage the production process but also plays a vital role in maintaining information security, which ultimately supports the smooth operations and business sustainability of steel manufacturing companies. Table 1 describes Application Architecture.

Table 1
Application Support for IoT Steel Manufacturing

Code	Control IoT Application	Code	Secure Application
CI01	Supervisory Control and Data Acquisition	SA01	Security Information and Event Management
CI02	MES (Manufacturing Execution System)	SA02	Firewall
CI03	Enterprise Resource Planning	SA03	Antivirus and Anti-Malware Software
CI04	Warehouse Management System	SA04	Data Encryption Software
CI05	Predictive Maintenance System	SA05	Intrusion Detection Prevention System
CI06	Quality Management System	SA06	Virtual Private Network
CI07	Supply Chain Management	SA07	Access Control Systems
CI08	Data Encryption and Security System	SA08	Backup and Recovery Solutions
CI09	Remote Monitoring and Control System	SA09	Multi-Factor Authentication
CI10	Asset Management System	SA10	Data Loss Prevention Solutions

Technology Architecture

Technology architecture is a framework that defines the infrastructure and technologies that support information systems and business operations in an organization, including in the steel manufacturing industry. In this context, the technology architecture includes the network infrastructure that connects various IoT devices, sensors, machines, and control systems. This infrastructure includes local networks, wide-area networks, and wireless networks that enable data communication between devices across manufacturing facilities, complemented by network security such as firewalls, intrusion detection systems, and virtual private networks to protect data from cyber threats.

The production environment uses IoT devices and sensors to collect real-time data, including temperature, humidity, pressure, and machine operational status, and then sends this data over the network to a central system for analysis. Advanced data processing systems, including cloud computing technology, enable the storage and processing of large amounts of data, supporting real-time data analytics for quick and informed decision-making. Cybersecurity is a critical component, with the use of data encryption, multi-factor authentication (MFA) (Almadani et al., 2023), (Chen et al., 2023), and antivirus and anti-malware software to protect systems and data from cyber threats.

Figure 3 depicts the technological framework for intelligent steel production, which combines different technologies to guarantee efficient operations, safety, and dependability. The smart steel manufacturing system is centrally located and connected to various components through routers that handle data traffic. The main components of this architecture are a smart steel foundry, asset management, smart preemptive maintenance, and planning and design. Edge computing supports these components, facilitating swift and effective processing of local data. Edge computing, present in all components, enables data processing to take place near the origin, resulting in decreased latency and enhanced system responsiveness. An intelligent steel foundry system actively monitors and regulates the

* Corresponding author



steel casting process in real-time, while an asset management system oversees and manages production assets to ensure maximum efficiency and utilization. Intelligent proactive maintenance uses sensor data to forecast and avert machine failures in advance, minimizing periods of inactivity and maintenance costs. Data encryption is a critical component of this architecture, wherein the information gathered by IoT sensors is encrypted prior to transmission over the network to guarantee data security and privacy. The data center then decrypts the encrypted data to perform further analysis. A router-connected intrusion detection and prevention system ensures that network data is protected against cyber threats and unauthorized entry. Furthermore, the planning and design process incorporates data gathered from all systems to enhance the efficiency of production processes and the creation of new products. The image also illustrates the correlation between the company's internal systems and the external, untrusted cloud, emphasizing the significance of security in the transmission of data over networks that may be susceptible to risks

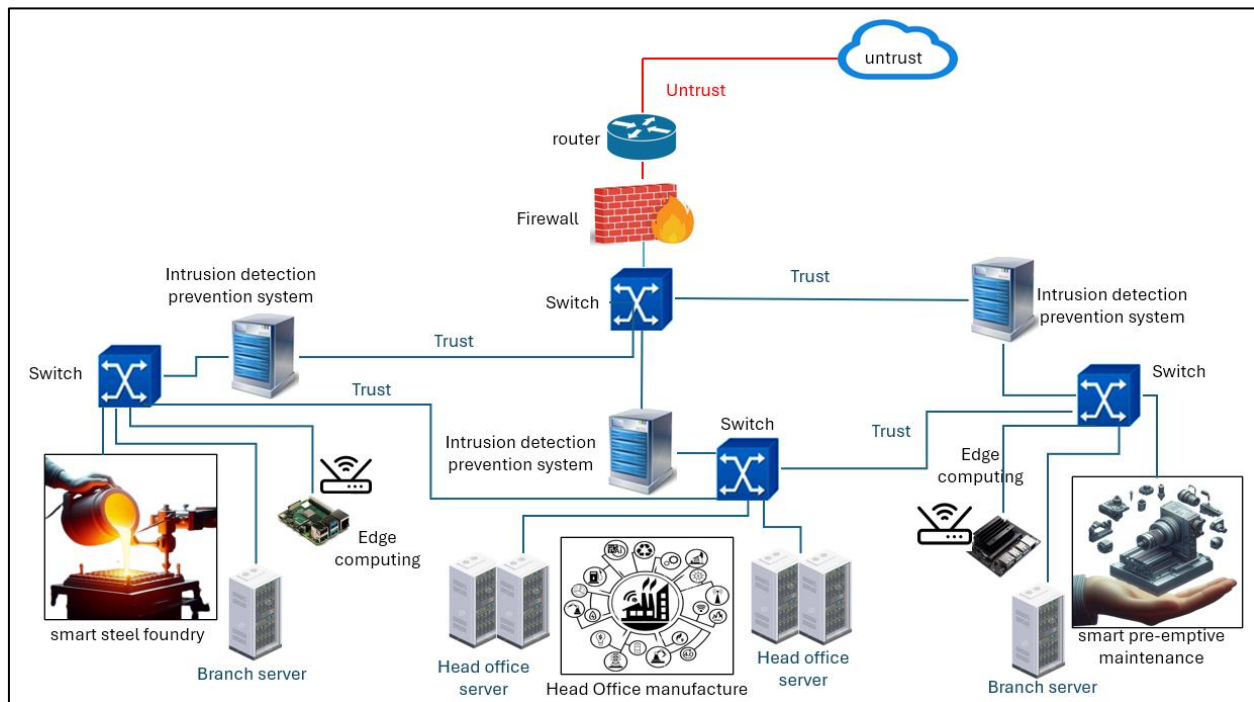


Fig. 2 Zero Trust Security Architecture Steel Manufacture

Figure 2, a combination of a strong firewall and an Intrusion Detection and Prevention System (IDPS) can guarantee the safety of servers in both the main office and any of the branch offices. As the initial line of defense, firewalls regulate authorized network traffic and block suspicious connections. However, intrusion detection and prevention systems (IDPS) allow for real-time attack detection and prevention and the monitoring of suspicious activity that may indicate a threat. Both servers can be safeguarded from a wide range of cybersecurity threats with the help of an advanced intrusion detection system (IDPS) and a robust firewall. Updating the IDPS system with the most recent threats and regularly updating the firewall rules are also crucial. Further measures to enhance network security include the introduction of stringent security policies and the implementation of regular staff training. Branch and head office servers can have their security well-maintained with these measures.

DISCUSSIONS

What is cybersecurity, and how can we improve IoT data security in steel manufacturing? (RQ.1)
Cybersecurity safeguards systems, networks, and data against digital attacks that aim to access, alter, or damage sensitive data, disrupt business operations, or extort users. Firewalls, encryption, multifactor authentication, and continuous network monitoring detect and respond to threats. With the rapid digitalization of manufacturing, the need for a robust cybersecurity plan has never been more urgent. As technology advances rapidly, more processes are

* Corresponding author



becoming digital. This trend underscores the critical importance of robust cybersecurity measures. Several steps can improve IoT data security for steel manufacturing. End-to-end encryption prevents eavesdropping, while a segmented network restricts sensitive data access to authorized devices and users, reducing security risks. Security measures like digital certificates and multifactor authentication can also prevent unauthorized access. However, it's important to note that a comprehensive approach, including IoT device monitoring and regular software updates, is necessary to close security gaps and ensure the ongoing security of the system. This comprehensive approach, when implemented, can provide a robust shield against potential threats, making the audience feel secure and well-protected.

Prior to implementing the Zero-trust System approach in steel manufacturing, as depicted in Figure 3. Figure 2 shows the structure of the IoT-enabled steel production network. In this figure, multiple IoT devices are connected through switches and routers, with data being forwarded to an intrusion detection and prevention system. Communication paths marked as “untrust” indicate that the data does not have sufficient security protection while in transit between devices. The implementation of edge computing on both sides, i.e., in an innovative steel foundry and smart pre-emptive maintenance, shows that data processing is done near the data source to reduce latency. However, these networks are still vulnerable to cybersecurity threats due to the absence of a Zero Trust Security approach that can ensure that every entity on the network is verified before being granted access. This figure illustrates the urgent need to enhance security by applying zero-trust principles to secure the entire IoT ecosystem in the steel manufacturing industry. The integration of more advanced security technologies will be critical to protecting industrial data and operations from potential threats.

Security and operational efficiency improved after the Zero Trust System was implemented in the steel manufacturing network architecture. Zero Trust verifies every network entity, internal and external, before granting access to resources or data. This architecture application connects all IoT devices, including intelligent steel foundry and smart pre-emptive maintenance, via encrypted communication. Remote Monitoring and SSL/TLS protect device-server data from unauthorized access. Multi-factor authentication (MFA) provides additional security by restricting system access to authorized users and devices. Thus, internal and external cyber threats can be reduced. Zero Trust System implementation uses advanced Intrusion Detection and Prevention Systems (IDPS) that are deeply integrated into the network architecture in addition to encryption and authentication. IDPS watches and analyzes network traffic all the time, looking for threats and stopping them before they do any harm. The IDPS, with its AI-based security analytics, can detect suspicious behavior and anomalies faster, thanks to its ability to learn and adapt to new threats.

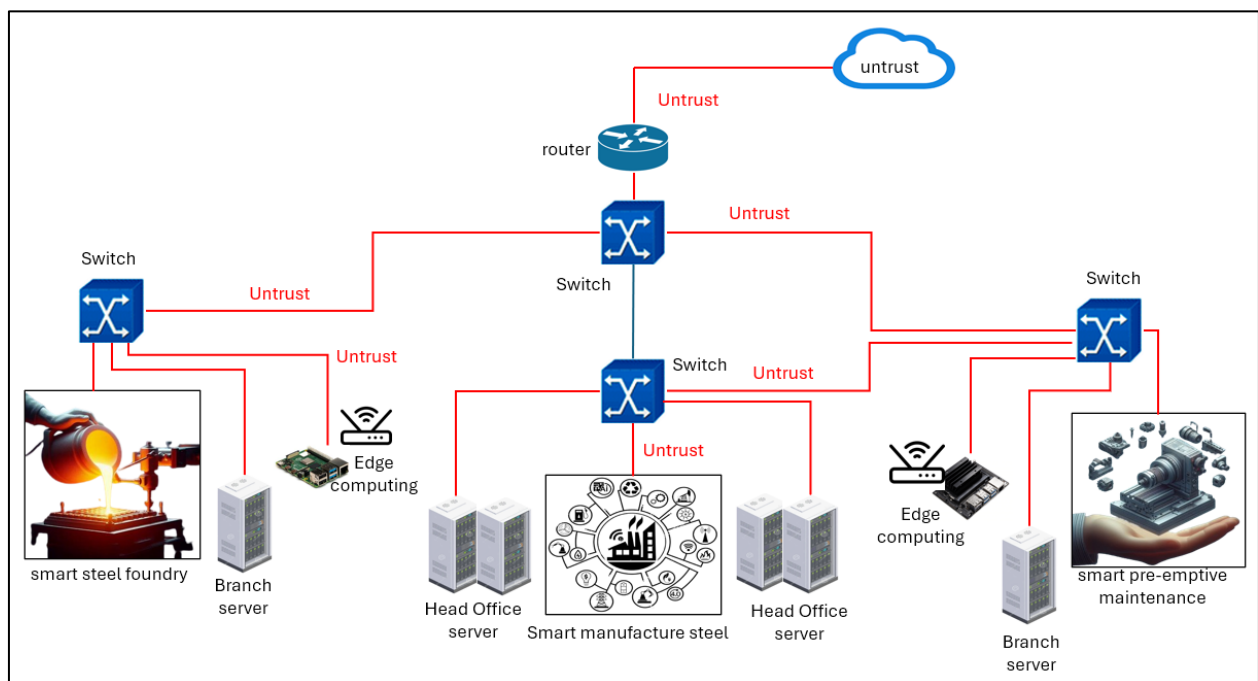


Fig. 3 Previous work without the addition of Zero Trust Security

* Corresponding author



Zero Trust Security (ZTS) in the steel manufacturing industry uses micro-segmentation, multi-factor authentication, and identity and access management to verify each entity before granting access, changing “untrust” to “trust”. Data is encrypted during transmission, and intrusion detection and prevention systems (IDPS) monitor the network in real time to prevent threats. Comprehensive visibility and forensic analysis are possible with centralized monitoring and logging. Security in the steel manufacturing industry's IoT ecosystem is improved by dynamic security policies based on the current context, boosting trust and efficiency. The proposed architecture application and technology must be implemented to create a trustworthy steel manufacturing network.

Can the use of IDPS devices and firewalls improve the security of Internet of Things data? (RQ.2)

Indeed, Intrusion Detection and Prevention System (IDPS) devices and firewalls can improve IoT data security. Firewalls, as the initial line of defense, filter network traffic and prevent unauthorized access to IoT devices. These firewalls, when configured, can effectively prevent attacks from untrusted external sources and permit only legitimate communication between IoT devices and central systems. Therefore, the firewall protects the confidentiality and integrity of data transmitted within the IoT ecosystem, giving users a sense of security. Meanwhile, IDPS functions as an additional, more advanced layer of security. IDPS can detect suspicious or unusual activity in an IoT network and prevent attacks before they cause more damage. IDPS devices employ a variety of methods, including behavioral analysis and attack signatures, to detect threats that firewalls may not detect. Moreover, IDPS can generate comprehensive reports on network activity, providing security administrators with a wealth of information to comprehend attack patterns and rectify systemic deficiencies. By incorporating firewalls and IDPS, IoT security systems can more effectively detect, prevent, and respond to threats, thereby enhancing their overall resilience to cyber threats. Given the volume and sensitivity of data managed by IoT devices, the implementation of IDPS and firewalls is of paramount importance, especially in the context of manufacturing industries, such as steel manufacturing. Attackers often target operational data collected by sensors and IoT devices to disrupt production or steal valuable information. By securing IoT networks with IDPS and firewalls, companies can protect their critical operations, reduce the risk of downtime, and ensure improved business continuity. In essence, firewalls and IDPS are indispensable components of a comprehensive cybersecurity strategy designed to protect IoT data, particularly in the unique security landscape of manufacturing industries.

5. CONCLUSION

This research shows that the integration of cybersecurity and the Internet of Things (IoT) in the steel manufacturing industry is essential to protect the data generated by IoT devices. Currently, although most important industries have adopted IoT technology, many steel manufacturing companies are still vulnerable to cyberattacks. Data that is not protected by security devices becomes a prime target for attackers, so a combination of cybersecurity and IoT strategies is indispensable. In addition, employees' awareness and understanding of data security play an essential role in the effectiveness of cybersecurity strategies. Security training and raising employee awareness are crucial steps in improving the effectiveness of cybersecurity strategies. This research successfully developed an effective enterprise architecture model for IoT cybersecurity risk management. The model, which focuses on threat identification, risk mitigation, and efficient security control implementation, is not just theoretical but practical. Firewall and IDPS implementation have proven effective in improving protection against cyber threats, thereby improving trust traffic to trust. This research also offers practical guidance for steel manufacturing companies to implement comprehensive and integrated security measures, instilling confidence in their ability to improve protection against cyber threats and maintain the company's operational sustainability. For future research, it is crucial to conduct a long-term evaluation of the effectiveness of the proposed architecture model and examine its impact on the company's operational performance. Additionally, there is a pressing need for further research to develop more effective employee training strategies to increase cybersecurity awareness. This call for further research engages us in the ongoing efforts to improve cybersecurity in IoT infrastructure in the steel manufacturing industry and provides strategies that can be implemented to enhance data security and operational efficiency.

6. REFERENCES

- Abawajy, J., Darem, A., & Alhashmi, A. A. (2021). Feature subset selection for malware detection in smart iot platforms. *Sensors (Switzerland)*, 21(4), 1–19. <https://doi.org/10.3390/s21041374>
- Almadani, M. S., Alotaibi, S., Alsobhi, H., & Hussain, O. K. (2023). Blockchain-based multi-factor authentication :

* Corresponding author



[Creative Commons Attribution-NonCommercial-ShareAlike 4.0
International License.](https://creativecommons.org/licenses/by-nc-sa/4.0/)

- A systematic literature review. *Internet of Things*, 23(June). <https://doi.org/10.1016/j.iot.2023.100844>
- Amalia, N., & Hindarto, D. (2024). Enterprise Architecture for Efficient Integration of IoT Lighting System in Smart City Framework. *Sinkron*, 8(2), 1091–1099. <https://doi.org/10.33395/sinkron.v8i2.13591>
- Babu, T., Roopa, H., Kumar, A., David, D. S., Jayadatta, S., & Rajesh, A. S. (2022). Internet of things-based automation design and organizational innovation of manufacturing enterprises. *Materials Today : Proceedings*, 56, 1769–1775. <https://doi.org/10.1016/j.matpr.2021.10.459>
- Brandín, R., & Abrishami, S. (2024). IoT-BIM and blockchain integration for enhanced data traceability in offsite manufacturing. *Automation in Construction*, 159(January). <https://doi.org/10.1016/j.autcon.2024.105266>
- Chen, Z., Cheng, Z., Luo, W., Ao, J., Liu, Y., & Sheng, K. (2023). FSMFA : Efficient firmware-secure multi-factor authentication protocol for IoT devices. *Internet of Things*, 21(December 2022). <https://doi.org/10.1016/j.iot.2023.100685>
- Hindarto, D., & Djajadi, A. (2023). *Android-manifest extraction and labeling method for malware compilation and dataset creation*. 13(6), 6568–6577. <https://doi.org/10.11591/ijece.v13i6.pp6568-6577>
- Hindarto, D., Indrajit, R. E., & Dazki, E. (2021). Sustainability of Implementing Enterprise Architecture in the Solar Power Generation Manufacturing Industry. *Sinkron*, 6(1), 13–24. <https://doi.org/10.33395/sinkron.v6i1.11115>
- Hindarto, D., Program, I. S., Technology, I., & Nasional, U. (2023). Exploring YOLOv8 Pretrain for Real-Time Detection of Indonesian Native Fish Species. *Sinkron*, 8(4), 2776–2785. <https://doi.org/10.33395/sinkron.v8i4.13100>
- Karthick, M. K., Kiruthiga, G., Ms Saraswathi, P., Dhiyanesh, B., & Radha, R. (2022). A Subset Scaling Recursive Feature Collection Based DDoS Detection Using Behavioural Based Ideal Neural Network For Security In A Cloud Environment. *Procedia Computer Science*, 215, 509–518. <https://doi.org/10.1016/j.procs.2022.12.053>
- Lee, I. (2021). Internet of Things The Internet of Things for enterprises : An ecosystem, architecture, and IoT service business model. *Internet of Things*, 7(2019). <https://doi.org/10.1016/j.iot.2019.100078>
- Permana, A. A., & Pratiwi, L. A. (2022). Implementation of the advanced encryption standard (AES) algorithm for digital image security. *Jurnal Teknik Informatika*, 15(1), 44–51. <https://doi.org/10.15408/jti.v15i1.25735>
- Rani, S., & Srivastava, G. (2024). Secure hierarchical fog computing-based architecture for industry 5.0 using an attribute-based encryption scheme. *Expert Systems With Applications*, 235(August 2023). <https://doi.org/10.1016/j.eswa.2023.121180>
- Saxena, R., Arora, D., & Nagar, V. (2023). Classifying Transactional Addresses using Supervised Learning Approaches over Ethereum Blockchain. *Procedia Computer Science*, 218(2022), 2018–2025. <https://doi.org/10.1016/j.procs.2023.01.178>
- Sze, E., Hindarto, D., & Wirayasa, I. K. A. (2022). Performance Comparison of Ultrasonic Sensor Accuracy in Measuring Distance. *Sinkron: Jurnal Dan Penelitian Teknik Informatika*, 7(4), 2556–2562. <https://doi.org/10.33395/sinkron.v7i4.11883>
- Unal, D., Al-ali, A., Catak, F. O., & Hammoudeh, M. (2025). A secure and efficient Internet of Things cloud encryption scheme with forensics investigation compatibility based on identity-based. *Future Generation Computer Systems*, 125(2021), 433–445. <https://doi.org/10.1016/j.future.2021.06.050>