ISSN : 2455-9679

IJRTSM
INTERNATIONAL JOURNAL OF RECENT TECHNOLOGY SCIENCE & MANAGEMENT

"SECURITY CHALLENGES IN INDUSTRIAL COMMUNICATION NETWORKS: A SURVEY ON ETHERNET/IP, CONTROLNET, AND DEVICENET"

Ruchi Patel [1]
[1]*Independent Researcher, rpnilkanth@gmail.com*

ABSTRACT

Modern industrial automation relies heavily on Industrial Communication Networks (ICNs), which provide smooth communication among sensors, controllers, as well as actuators. However, with the increasing integration of industrial networks into IT infrastructures, security vulnerabilities have emerged as a significant concern. This study offers a thorough analysis of three commonly used industrial communication protocols, Ethernet/IP, ControlNet, and DeviceNet, analyzing their characteristics, security risks, and mitigation strategies. The report emphasizes how outdated methods are unable to handle cyberthreats such denial-of-service (DoS) assaults, illegal access, and data integrity issues. Additionally, it explores emerging security solutions, including time-sensitive networking (TSN), cryptographic mechanisms, and intrusion detection systems (IDS). The review further discusses potential advancements, such as AI-driven security monitoring, blockchain-based authentication, and zero-trust security models, to enhance the resilience of industrial networks. By synthesizing insights from existing research and real-world incidents, this paper aims to bridge the gap between operational efficiency and robust security measures, offering valuable guidance.

Key Words: *Industrial Communication Networks (ICNs), Ethernet/IP, ControlNet, DeviceNet, Industrial Automation, Cybersecurity, Network Protocols, Time-Sensitive Networking.*

I. INTRODUCTION

An important pillar of a country with electricity, energy, and many diverse areas of people's employment is the modern control system (ICS). The intricate restricted communication protocols that ICS has been using [1].
Industrial automation is a system that is becoming more significant in the fourth industrial revolution. Large automated machine networking is a new area of concentration for industrial automation, and connecting to traditional automation machinery, which is only built to enable local computer connectivity, presents a problem. Industrial networks may be extremely decentralized, stiff, and difficult to administer because of the close connection between automation information and the control plane, which are often combined in equipment [2]. In the initial setup of the plant, the communication and compute nodes are frequently established separately, and the connections stay unchanged after that. Due to localized setup, the hierarchical structure of traditional industrial communication, which has three network levels and several networking technologies and protocols, which limit what can be done and make things more complicated [3].
In several commercial sectors, information and communications technology-based environments have extensively integrated cutting-edge technologies [4]. Industry adoption of information technology has become essential due to the expansion of network connection, which forces numerous organizations across a range of industries to constantly innovate.

The ICNs play a critical role in modern industrial automation, enabling seamless data exchange between sensors, controllers, and actuators [5]. Among the widely adopted industrial protocols, Ethernet/IP, ControlNet, and DeviceNet serve distinct purposes, offering varying levels of speed, topology flexibility, and data transmission methods [6][7]. These networks support industrial operations by ensuring reliable communication, real-time control, and system interoperability.

However, as industrial environments become increasingly interconnected, security challenges in ICNs have escalated, making industrial control systems (ICS) vulnerable to illegal access, cyberattacks, and possible interruptions in operations [8]. Legacy protocols such as ControlNet and DeviceNet were originally designed with minimal security considerations, making them vulnerable to modern cyberattacks. Conversely, because Ethernet/IP is IP-based, it is susceptible to the same threats as conventional IT networks, such as DoS attacks, illegal access, and protocol flaws.

Ethernet is currently the most widely used digital communication technology because of its adaptability and global reach. For this reason, Ethernet is the foundation of today's primary industrial communication protocols. Although everyone says Ethernet can accommodate many different protocols, accurate laboratory testing is the only way to confirm this claim [9][10][11]. Three protocols TCP/IP, IEC 61850, and Profilet are used in the testing, which are conducted on a hybrid network. These three protocols work together to provide a great industrial applications that combines process automation, substation automation, and general-purpose data transfer [12]. However, the industrial plant network's safety and security may decline as a result of a shared network.

A. Research Motivation and Significance/Aim

The increasing reliance on ICNs , particularly Ethernet/IP, ControlNet, and DeviceNet, has introduced significant security challenges as these protocols were designed for efficiency rather than security. With the rise of cyber threats targeting critical infrastructure such as manufacturing, energy, and transportation, there is an urgent need to address vulnerabilities in these legacy systems. This study aims to investigate the security risks associated with ICNs, emphasizing their main vulnerabilities, possible defenses, and attack routes. This study finds holes in current security measures and suggests ways to improve resilience against cyberattacks by analyzing existing literature and real-world occurrences. The importance of this research is in its ability to strengthen industrial networks' overall cybersecurity posture and safeguard vital infrastructure against new cyberthreats. Through this analysis, the study provides insights that can guide future developments in secure industrial communication frameworks, bridging the gap between operational efficiency and robust security measures.

B. Research Contribution

This research explores security challenges in industrial communication networks, specifically focusing on Ethernet/IP, ControlNet, and DeviceNet. The key contributions of this study include:

- **Comprehensive Analysis:** Examines various industrial communication protocols, their security vulnerabilities, and possible ways of assault. In order to reduce cyber dangers in industrial settings, it assesses the efficacy of current security measures as well as new developments.
- **Identification of Challenges:** Critical security issues, including unauthorized access, data integrity risks, and Threats to industrial control systems from cyberattacks. It also examines the limitations of traditional security mechanisms in real-time industrial networks.
- **Exploring Opportunities:** Enhancing industrial network security through time-sensitive networking (TSN), cryptographic mechanisms, and Intrusion detection systems (IDS) designed for use in industrial settings.
- **Synthesis of Literature:** Provides insights into recent advancements in industrial communication security, analyzing research on protocol vulnerabilities, real- world cyber incidents, and cybersecurity frameworks for industrial automation.
- **Future Research Directions:** Outlines potential advancements, including AI-driven security monitoring, blockchain-based authentication mechanisms, and the integration of zero-trust security models in industrial networks to strengthen resilience against cyber threats.

C. Structure of the Paper

The structure of this document is as follows: Section II overview of industrial communication protocols (ICNs). Section III discusses security challenges in industrial communication networks. The literature and case studies are reviewed in Section IV. Included are findings and suggestions for more research in Section V, Conclusions.

ISSN : 2455-9679

II. OVERVIEW OF INDUSTRIAL COMMUNICATION PROTOCOLS (ICNS)

Industrial Communication Networks (ICNs) are the backbone of modern industrial automation, enabling seamless communication between controllers, sensors, actuators, and other devices. These networks use specialized industrial communication protocols to ensure real-time, reliable, and deterministic data exchange in manufacturing, process control, and other industrial applications. Industrial communication protocols facilitate the exchange of data over a specific network and communication standard. The application determines how each communication protocol is used; each one focusses on a certain private purpose [13]. A complicated application's needs cannot be satisfied by a single protocol, therefore eventually many protocols are mixed. Data communication is the exchange of digital or analogue information or data via a connecting element between a transmitter and a receiver. In the industry, different control devices are connected via communication protocols [14].

*A. **Key Industrial Protocols***

The Industrial communication networks ICNs are essential for ensuring reliable, real-time data sharing across sensors, controllers, and industrial automation equipment. Among the various protocols used in industrial automation, Ethernet/IP, ControlNet, and DeviceNet are three of the most widely adopted. These protocols, developed by Rockwell Automation as well as managed by the Open DeviceNet Vendors Association (ODVA), facilitate communication between industrial devices such as PLCs, sensors, actuators, robotics systems, as well as Human-Machine Interfaces (HMIs) [15].

1) Ethernet/IP

Real-time data transmission across devices of different manufacturers and technologies is made possible by Ethernet/IP, an ICP based on Ethernet technology. Because of its worldwide standardization, Ethernet offers a high rate of transmission and remarkable universality. The TCP/IP and scalable SOME/IP are among the protocols it supports [16]. The contention approach, which is used in a typical Ethernet to enable numerous nodes to access a communication network, is not applicable to automobiles because of the restrictions in stability, limited latency, and real-time data processing [16].

Fig. 1. Ethernet/IP Network Architecture Diagram

Figure 1: The diagram illustrates an Ethernet/IP network architecture integrating Modbus RTU devices via a gateway, Ethernet/IP adapters, scanners, and switches, enabling seamless communication between industrial devices, controllers, and monitoring systems within a unified network infrastructure.

2) ControlNet:

An industrial network protocol called ControlNet was created for high-speed, real-time control applications. In contexts involving industrial automation, it makes use of a deterministic token-passing protocol to provide dependable and urgent data transmission. ControlNet™ is widely used in applications requiring synchronized motion, I/O control, and peer-to-peer communication between controllers and devices. In Master Control Systems (MCS), ControlNet™ facilitates communication with internal devices and third-party systems, including FPSO's distributed control systems (DCS) [17].

3) DeviceNet:

The two primary papers that make up the DeviceNet standard as supplied by ODVA are the DeviceNet adaptation of CIP and the CIP standard [18]. The upper tiers of the protocol stack are covered in the CIP specification's main body. The communication paradigm of producers and consumers served as the foundation for the creation of CIP, an object oriented protocol. Nodes are seen as groupings o f items, and their visible network activity, is defined using object modelling.

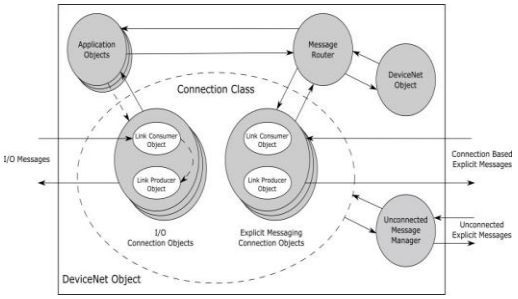

Fig. 2. The DeviceNet Object Model

A DeviceNet node's object model is shown in Figure 2, which also demonstrates the class notion by displaying object kinds and their associations. A group of objects with similar functions, characteristics, and behaviors is called a class. While attributes are an object's qualities, services are the actions that an entity may do [19]. The so-called library of objects provided by the CIP standard defines objects that cover common functionality needed by network nodes. Vendor-specific object definition is covered in the standard for any additional more specialized objects that could be required.

A. Comparison of Industrial Communication Protocols Networks

Ethernet/IP, ControlNet, and DeviceNet are widely used industrial communication protocols, each with distinct characteristics in topology, speed, and data transmission methods [20]. Understanding these differences helps in selecting the right protocol according to an industrial automation system's particular requirement.

1) Topology

Topology defines how devices connect in a network. Ethernet/IP uses star, tree, or mesh for scalability, ControlNet employs bus or ring for real-time control, and Device Net follows a bus (daisy-chain) for cost-effective sensor networking. Topology refers to how devices are connected in a network shown in Table I. Each protocol supports different topologies based on its intended use:

TABLE I. TOPOLOGY COMPARISON OF ETHERNET/IP, CONTROLNET, AND DEVICENET

Protocol	Topology	Description
Ethernet/IP	Star, Tree, Mesh	Uses standard Ethernet topologies with switches and routers. Highly flexible and scalable.
ControlNet	Bus, Ring	Operates on a token-passing network, ensuring deterministic communication. Can be implemented as a redundant ring for reliability.
DeviceNet	Bus (Daisy Chain)	Uses a trunk-line/drop-line bus topology, reducing wiring complexity. Suitable for small device networks.

2) Speed

Speed determines data transmission efficiency in industrial networks. Ethernet/IP offers the fastest communication for high-speed automation, ControlNet ensures low-latency real-time control, and DeviceNet provides sufficient speed for sensor and actuator networks. Speed determines how quickly data is transmitted between devices shown in Table II. It is a key factor in selecting the right protocol for industrial automation:

TABLE II. SPEED COMPARISON OF ETHERNET/IP, CONTROLNET, AND DEVICENET

Protocol	Speed	Latency
Ethernet/IP	10 Mbps – 1 Gbps	Variable, depending on network congestion.
ControlNet	5 Mbps	Low latency due to scheduled communication.
DeviceNet	125 Kbps – 500 Kbps	Higher latency compared to Ethernet/IP and ControlNet.

ISSN : 2455-9679

3) Data Transmission Method

Data transmission methods affect reliability and performance. Ethernet/IP supports real-time and non-real- time messaging, ControlNet ensures deterministic data transfer, and DeviceNet uses cyclic and event-driven messaging to optimize bandwidth shown in Table III. The way data is transmitted in an industrial network impact's reliability, latency, and performance [21].

TABLE III. DATA TRANSMISSION METHODS OF ETHERNET/IP, CONTROLNET, AND DEVICENET

Protocol	Data Transmission Method	Message Type
Ethernet/IP	TCP/IP (explicit messaging) and UDP/IP (implicit messaging)	Real-time versus non- real-time information.
ControlNet	Token-passing mechanism	Deterministic, scheduled data transmission.
DeviceNet	CAN-based bus communication	Cyclic and event-driven messaging.

III. SECURITY CHALLENGES IN INDUSTRIAL COMMUNICATION NETWORKS

Industrial Communication Networks (ICNs) face significant security challenges due to their integration with IT systems, legacy protocols, and increasing cyber threats. Unlike traditional IT networks, ICNs prioritize real-time performance and reliability, often at the expense of built-in security features. The key security challenges include:

A. General Threats to ICNs

Threats to the security of ICNs can cause operational disruptions, damage data integrity, and pose safety or financial hazards. The most frequent dangers are:

1) Man-in-the-Middle (MITM) Attack

The ability of the MITM attacker to intercept, alter, replace, or manipulate the communication traffic of the target victims sets them apart from a mere eavesdropper. Additionally, victims don't know who is intruding, so they think the route of contact is safe [22]. MITM attacks may be carried out using a variety of communication channels, including Wi-Fi, Bluetooth, Near Field Communication (NFC), UMTS, GSM, and Long-Term Evolution (LTE). The secrecy as well as integrity of the data itself are also targets of the assault, in addition to the actual data that moves between endpoints [23].

2) Denial-of-Service (DoS) Attacks

In particular, DoS attacks that interfere with communication between smart metering devices and control centers can prevent signals from arriving at their intended locations on time. This can hinder the control center's ability to maintain a strong situational awareness of the grid's state, which can result in grid instability. To execute a Distributed DoS assault, the attackers may use a large number of machines (including botnets) and fake IP addresses to conceal their identity [24].

3) Malware Attack

Malware, an acronym for malicious software, is any invasive software created by hackers with the intention of stealing data and causing harm or destruction to computers and computer systems. Furthermore, badware is the aggregate word for malware and inadvertently damaging software [25]. Malware may be broadly classified into several types, such as ransomware, rootkits, botnets, Trojan horses, worms, viruses, and more.

4) Insider Threats

The possibility of an insider using an internal danger is a system that has the ability to harm people or steal information. Because employees are viewed as trustworthy individuals with vast abilities that may be easily abused, these threats are especially concerning [7]. An insider threat involves individuals within an organization who may intentionally or unintentionally leak data. Characteristics include those who leak data either on purpose or by mistake, and anyone with access to confidential information.

5) Supply Chain Attacks

Attacks against supply chains use third-party resources or services, Often called a "supply chain," it compromises a target's network or system. These assaults are often referred to as "third-party attacks" or "value-chain attacks." Supply

chain attacks are by definition indirect, concentrating on the third- party dependencies that their ultimate targets usually rely on without realizing it [26]. A piece of code or software that enhances an application's functionality and is frequently written in JavaScript is called a dependent [27].

B. Vulnerabilities in Industrial Protocols

Industrial communication protocols like Ethernet/IP, ControlNet, and DeviceNet were designed primarily for efficiency and interoperability, often lacking built-in security features. This makes them vulnerable to various cyber threats, including:

1) Vulnerabilities in Ethernet/IP

The vulnerability arises when the listener at the Ethernet/IP TCP port (default 44818) incorrectly interprets the extra parameters in the TCP ACK message [28]. The device reboots instantly and goes into "Major Fault" status if the NOP option is used incorrectly [29]. This needs to be fixed manually. There must be more than one choice and the NOP option must be selected first in order to activate the vulnerability.

2) Vulnerabilities in ControlNet

ControlNet, a real-time industrial communication protocol, has several security weaknesses that can be exploited by attackers [30]:

- **Lack of Encryption and Authentication:** ControlNet does not support encryption, increasing the possibility that hostile actors may collect or alter data through eavesdropping and spoofing attacks.
- **Susceptibility to Network Attacks:** The token- passing protocol can be exploited for Denial-of- Service (DoS) attacks, disrupting communication and causing system downtime [31].
- **Legacy System Risks:** Many ControlNet implementations are more susceptible to malware, illegal access, and a lack of security fixes since they are based on outdated hardware and software.
- **Physical Security Concerns:** Unauthorized physical access to network cables or devices can allow attackers to inject malicious commands or disrupt operations [32].

3) Vulnerabilities in DeviceNet:

DeviceNet an industrial network protocol used for communication between controllers and field devices, has several security weaknesses that can be exploited by attackers [33]:

- **Lack of Encryption and Authentication:** DeviceNet does not support encryption or authentication, leaving it open to spoofing, eavesdropping, and MitM attacks, which allow malevolent actors to alter or intercept data [34].
- **Denial-of-Service (DoS) Risks:** The Master-Slave communication model can be overloaded with malicious traffic, causing delays or device failures, disrupting critical industrial processes.
- **Physical Security Weaknesses:** Since DeviceNet relies on physical cabling, unauthorized physical access to network connections can allow attackers to inject malicious commands, disable devices, or disrupt production.
- **Legacy System Vulnerabilities:** Many DeviceNet- enabled devices are outdated and lack firmware updates, making them susceptible to malware, unauthorized modifications, and protocol exploits.

IV. LITERATURE REVIEW

In this section, previous research on Ethernet IP-based ICNs, controlNet and DeviceNet. Table IV provides a structured comparison of previous research, focusing on Ethernet/IP, ControlNet, and DeviceNet within ICNs and their security challenges.

Kada, Alzubairi and Tameem (2019) examine IoT enablers and industrial communication topologies that demand low latency. They came to the conclusion that the next difficult emphasis in terms of latency and security will be wireless gateways. current communication technology advancements and how they affect industry and industrial automation in general. Ethernet, wireless networks, and web technologies are examples of digital communication networks that have improved the dependability, flexibility, and comprehensiveness of information flow and interchange within dispersed automation systems. The information and communication technology (ICT) offer high performance, increased controllability, and flexibility, as well as inherent advantages in monitoring, control, and supervision as well as assistance for industrial automation [35].

Chang (2015) effectiveness and performance of the communication system will be assessed to make sure it is suitable

for the industrial network. The factory's control systems, including the industrial motion control system, must have precise control and quick communication since the industrial communication system needed real-time communication. Therefore, in order to attain performance and reliability in ICNs, they suggested a connection security system that complements visible light communication and wireless networks. In the near future, they will think about. using industrial wireless Ethernet to accomplish this method [36].

Junfeng et al. (2020) presents the EtherNet/IP protocol's applicability to combination switches used by miners. Based on this protocol stack, Tests show that by completing data exchange and keeping a consistent communication connection via an EtherNet/IP host, an EtherNet/IP gateway can meet the technical criteria of EtherNet/IP communication. To overcome the limitations of the mine-used combination switch's outdated communication method and inadequate protocol generality. The article introduces the combination switch application idea and goes over the basics of the EtherNet/IP protocol [37].

Makrakis et al. (2021) provide a thorough and current analysis of the main dangers and attacks on industrial control systems, key infrastructures, and the equipment and communication protocols utilized there. According to their study, the frequency of attacks against critical infrastructure has increased as a result of the dissemination of commodities that may be used in the early or late stages of attacks. Additionally, their investigation reveals that there are flaws in the architecture and operation of a number of Devices and network protocols unique to OT that might readily provide attackers a substantial impact on operational procedures [38].

Nguyen and Jeon (2020) proposes a smart manufacturing gateway built on DeviceNet and EtherCAT. DeviceNet is utilized as a secondary protocol, while EtherCAT is selected as the primary protocol. The gateway's exceptional characteristics allow it to accommodate a large number of devices and improve the network's quality of service (QoS). An embedded programmable logic controller (ePLC) can take the role of a hardware programmable logic controller with proposal gateway. Tests demonstrate that this gateway meets the real-time needs of a production system while also offering a high quality of service [39].

Nyasore et al. (2020) investigate and talk about the usage of industrial firewalls with DPI and IDPS that can identify and thwart highly specialized assaults that are concealed deep inside the communication flow. According to the study's findings, Real-time communication requirements in many industrial & automation control devices may be difficult to meet when DPI is used due to the delay and jitter that IDPS as well as DPI industrial firewalls produce. Decades ago, when the protocol was developed, no security precautions were taken [40].
Table IV summarizes key studies on ICNs, highlighting wireless gateways, hybrid communication models, and EtherNet/IP for enhanced performance. It reviews security challenges in OT protocols, proposes integrated gateways for smart factories, and evaluates DPI-based intrusion detection. The studies underline trade-offs between security, latency, and real-time performance.

Table IV. Comparative analysis of communication-related literature on industrial networks

Reference	Focus Area	Key Findings	Challenges	Key Contribution
Kada, Alzubairi and Tameem (2019)[35]	Industrial communication topologies, IoT enablers	Wireless gateways will be a major focus for low latency and security	Latency issues in wireless industrial networks	Highlights the role of wireless gateways in industrial communication
Chang (2015)[36]	Industrial communication system performance	Connection protection mechanism using wireless and visible light communication	Real-time communication reliability in industrial motion control	Proposes a hybrid wireless and visible light communication approach for reliability
Junfeng et al. (2020)[37]	EtherNet/IP in mining applications	EtherNet/IP gateway ensures stable communication with host devices	Legacy communication protocols in mining applications	Demonstrates successful implementation of EtherNet/IP in mine-used switches
Makrakis et al. (2021)[38]	Security threats in industrial control systems (ICS)	Increasing threats due to commodity attack tools	Vulnerabilities in OT-specific protocols	Provides an in-depth survey of security threats in ICS
Nguyen and Jeon (2020)[39]	EtherCAT and DeviceNet gateway for smart factories	Embedded PLCs enhance network performance	Real-time performance constraints in factory automation	Proposes a high-QoS gateway integrating EtherCAT and DeviceNet
Nyasore et al. (2020)[40]	Intrusion detection and prevention in ICNs	DPI-based IDPS can detect specialized attacks	Latency and jitter in real-time communication	Evaluates DPI-based security measures and their impact on real-time ICS communication

V. CONCLUSION & FUTURE WORK

The ICNs play a vital role in modern automation systems, but their security challenges pose significant risks to critical infrastructure. This paper has explored the vulnerabilities of Ethernet/IP, ControlNet, and DeviceNet, highlighting risks including unauthorized access, Attacks that cause denial of service and breaches of data integrity. The increasing interconnectivity of industrial systems, combined with legacy protocols that lack robust security mechanisms, makes these networks prime targets for cyber threats. Despite advancements in industrial cybersecurity, challenges remain,

particularly in ensuring low-latency, real-time communication while maintaining strong security protections. Future studies should use AI for proactive threat detection and include blockchain for safe, decentralized recordkeeping. Time- Sensitive Networking (TSN) guarantees safe, real-time data transfer, while quantum cryptography can defend against potential quantum assaults. Network defenses will be strengthened by SDN, Zero Trust Architecture, and standardized security frameworks. Securing low-latency, dispersed communication will be essential for robust, next- generation industrial networks as edge computing and 5G grow.

REFERENCES

[1] K. Imtiaz and M. J. Arshad, "Security Challenges of Industrial Communication Protocols: Threats, Vulnerabilities and Solutions," *Int. J. Comput. Sci. Telecommun.*, vol. 10, no. 4, 2019.

[2] Y. Kang, S. Lee, S. Gwak, T. Kim, and D. An, "Time-Sensitive Networking Technologies for Industrial Automation in Wireless Communication Systems," *Energies*, vol. 14, no. 15, 2021, doi: 10.3390/en14154497.

[3] K. Ahmed, J. O. Blech, M. A. Gregory, and H. W. Schmidt, "Software Defined Networks in Industrial Automation," *J. Sens. Actuator Networks*, vol. 7, no. 3, 2018, doi: 10.3390/jsan7030033.

[4] H. Yu and H. Chang, "A Meta-Analysis of Industrial Security Research for Sustainable Organizational Growth," *Sustainability*, vol. 12, no. 22, 2020, doi: 10.3390/su12229526.

[5] D. Cavalcanti, J. Perez-Ramirez, M. M. Rashid, J. Fang, M. Galeev, and K. B. Stanton, "Extending accurate time distribution and timeliness capabilities over the air to enable future wireless industrial automation systems," *Proc. IEEE*, vol. 107, no. 6, pp. 1132–1152, 2019.

[6] A. V. Hazarika, G. J. S. R. Ram, and E. Jain, "Performance Comparision of Hadoop and Spark Engine," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, IEEE, Feb. 2017, pp. 671–674. doi: 10.1109/I- SMAC.2017.8058263.

[7] S. Pandya, "Predictive Analytics in Smart Grids : Leveraging Machine Learning for Renewable Energy Sources," *Int. J. Curr. Eng. Technol.*, vol. 11, no. 6, pp. 677–683, 2021.

[8] A. M. Romanov, F. Gringoli, and A. Sikora, "A precise synchronization method for future wireless TSN networks," *IEEE Trans. Ind. Informatics*, vol. 17, no. 5, pp. 3682–3692, 2020.

[9] L. Rocca, "IEC 61850 : A Safety and Security Analysis in Industrial Multiprotocol Networks," University of Genoa, 2019.

[10] A. Balasubramanian, "AI-Enabled Demand Response: A Framework for Smarter Energy Management," *Int. J. Core Eng. Manag.*, vol. 5, no. 6, pp. 96–110, 2018, doi: 10.5281/zenodo.14741022.

[11] A. Gogineni, "Observability Driven Incident Management for Cloud-native Application Reliability," *Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci.*, vol. 9, no. 2, 2021.

[12] G. Modalavalasa, "Towards Sustainable Development Based on Machine Learning Models for Accurate and Efficient Flood Prediction," vol. 8, no. 2, pp. 940–944, 2021.

[13] H. Peng, W. Tärneberg, E. Fitzgerald, and M. Kihl, "Is cloud RAN a feasible option for industrial communication network?," *J. Commun. Softw. Syst.*, 2021, doi: 10.24138/JCOMSS-2021-0017.

[14] A. Kocamuftuoglu, O. Akbay, and S. Kaba, "A Comparative Study on Industrial Communication Protocols Using IoT Platforms," *Eurasia Proc. Sci. Technol. Eng. Math.*, vol. 14, pp. 57–65, 2021, doi: 10.55549/epstem.1050178.

[15] S. Shah and M. Shah, "Deep Reinforcement Learning for Scalable Task Scheduling in Serverless Computing," *Int. Res. J. Mod. Eng. Technol. Sci.*, vol. 3, no. 12, Jan. 2021, doi: 10.56726/IRJMETS17782.

[16] H.-J. Kim, M.-H. Choi, M.-H. Kim, and S. Lee, "Development of an Ethernet-Based Heuristic Time-Sensitive Networking Scheduling Algorithm for Real-Time In-Vehicle Data Transmission," *Electronics*, vol. 10, no. 2, Jan. 2021, doi: 10.3390/electronics10020157.

[17] J. Pimentel and G. Schneider, "Network Topology Protocol Change from ControlNet to Ethernet/IP for a Master Control Station in a Subsea Production System." 2016.

[18] P.-S. Murvay and B. Groza, "A brief look at the security of DeviceNet communication in industrial control systems," in *CECC 2018: Proceedings of the Central European Cybersecurity Conference 2018*, 2018, pp.

1–6. doi: 10.1145/3277570.3277575.

[19] S. S. S. Neeli, "Ensuring Data Quality: A Critical Aspect of Business Intelligence Success," *Int. J. Lead. Res. Publ.*, vol. 2, no. 9, 2021.

[20] A. Immadisetty, "Real-Time Data Analytics in Customer Experience Management: A Framework for Digital Transformation and Business Intelligence," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 10, no. 6, pp. 1280–1288, 2021.

[21] N. Patel, "Sustainable Smart Cities : Leveraging IoT and Data Analytics for Energy Efficiency and Urban Development," *J. Emerg. Technol. Innov. Res.*, vol. 8, no. 3, 2021.

[22] R. Tarafdar, "Algorithms on Majority Problem," *Univ. Missouri- Kansas City*, 2017.

[23] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man in the Middle Attacks," *IEEE Communications Surveys and Tutorials*. 2016. doi: 10.1109/COMST.2016.2548426.

[24] B. Jaya, Y. Yuhandri, and S. Sumijan, "Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS)," *J. Sistim Inf. dan Teknol.*, 2020, doi: 10.37034/jsisfotek.v2i4.32.

[25] A. Qamar, A. Karim, and V. Chang, "Mobile malware attacks: Review, taxonomy & future directions," *Futur. Gener. Comput. Syst.*, 2019, doi: 10.1016/j.future.2019.03.007.

[26] Abhishek and P. Khare, "Cloud Security Challenges: Implementing Best Practices for Secure SaaS Application Development," *Int. J. Curr. Eng. Technol.*, vol. 11, no. 06, pp. 669–676, Nov. 2021, doi: 10.14741/ijcet/v.11.6.11.

[27] J. Thomas, "The Effect and Challenges of the Internet of Things (IoT) on the Management of Supply Chains," *Int. J. Res. Anal. Rev.*, vol. 8, no. 3, pp. 874–878, 2021.

[28] J. Pavesi, T. Villegas, A. Perepechko, E. Aguirre, and L. Galeazzi, "Validation of ICS Vulnerability Related to TCP/IP Protocol Implementation in Allen-Bradley Compact Logix PLC Controller," 2019, pp. 355–364. doi: 10.1007/978-3-030-33229- 7_30.

[29] A. Balasubramanian and N. Gurushankar, "AI-Powered Hardware Fault Detection and Self-Healing Machanisms," *Int. J. Core Eng. Manag.*, vol. 6, no. 4, pp. 22–30, 2019.

[30] S. Sen, "ControlNet," in *Fieldbus and Networking in Process Automation*, CRC Press, 2014, pp. 233–243. doi: 10.1201/b16891- 16.

[31] V. S. Thokala, "A Comparative Study of Data Integrity and Redundancy in Distributed Databases for Web Applications," *Int. J. Res. Anal. Rev.*, vol. 8, no. 4, pp. 383–389, 2021.

[32] Goyal, "Enhancing Engineering Project Efficiency through Cross-Functional Collaboration and IoT Integration," *Int. J. Res. Anal. Rev.*, vol. 8, no. 4, pp. 396–402, 2021.

[33] P. S. Murvay and B. Groza, "A brief look at the security of DeviceNet communication in industrial control systems," in *ACM International Conference Proceeding Series*, 2018. doi: 10.1145/3277570.3277575.

[34] V. Kolluri, "A Pioneering Approach To Forensic Insights: Utilization AI for Cybersecurity Incident Investigations," *Int. J. Res. Anal. Rev.*, vol. 3, no. 3, 2016.

[35] B. Kada, A. Alzubairi, and A. Tameem, "Industrial Communication Networks and the Future of Industrial Automation," in *2019 Industrial and Systems Engineering Conference, ISEC 2019*, 2019. doi: 10.1109/IASEC.2019.8686664.

[36] S. H. Chang, "A Visible Light Communication Link Protection Mechanism for Smart Factory," in *Proceedings - IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, WAINA 2015*, 2015. doi: 10.1109/WAINA.2015.41.

[37] D. Junfeng, R. Xiang, Y. Shuohang, and W. Lipeng, "Design of Mine-Used Combination Switch Gateway Based on EtherNet/IP," in *2020 5th International Conference on Power and Renewable Energy, ICPRE 2020*, 2020. doi: 10.1109/ICPRE51194.2020.9233221.

[38] G. M. Makrakis, C. Kolias, G. Kambourakis, C. Rieger, and J. Benjamin, "Industrial and critical infrastructure security: Technical analysis of real-life security incidents," *Ieee Access*, vol. 9, pp. 165295–165325, 2021.

[39] V. Q. Nguyen and J. W. Jeon, "Develop an EtherCAT and DeviceNet Gateway for a Smart Factory," in *2020 IEEE International Conference on Consumer Electronics - Asia, ICCE- Asia 2020*, 2020. doi: 10.1109/ICCE-Asia49877.2020.9277185.

[40] O. N. Nyasore, P. Zavarsky, B. Swar, R. Naiyeju, and S. Dabra, "Deep Packet Inspection in Industrial Automation Control System to Mitigate Attacks Exploiting Modbus/TCP Vulnerabilities," in *2020 IEEE 6th*

Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), IEEE, May 2020, pp. 241–245. doi: 10.1109/BigDataSecurity-HPSC-IDS49724.2020.00051.