International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 04 | April - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

A Comprehensive Survey of Security Challenges and Solutions of Industrial Internet of Things (IIoT) Networks

Anusha Kumari*[1], Dr. Siddalingappagouda Biradar[2]

[1]Under Graduate Student, Department of Electronics and Communication, Dayananda Sagar Academy of Technology and Management, Bangalore, Karnataka, India

[2]Associate Professor, Department of Electronics and Communication, Dayananda Sagar Academy of Technology and Management, Bangalore, Karnataka, India

*Corresponding Author: kumari.anusha1503@gmail.com

Abstract

Despite the transformative potential of the Industrial Internet of Things (IIoT) in optimizing industrial operations, significant security and privacy challenges persist, underscoring the need for comprehensive solutions. This paper addresses this research gap by presenting a thorough survey of the security challenges and solutions in IIoT networks. Drawing from the extensive literature on IIoT, we identify and categorize key threats such as malware attacks, data breaches, and supply chain vulnerabilities. Additionally, we explore privacy concerns arising from the vast amounts of sensitive data collected and transmitted by IIoT devices. This analysis highlights the critical importance of encryption mechanisms, access controls, and authentication protocols as fundamental security measures. By synthesizing current research, this paper provides insights to guide the development of robust security strategies for IIoT deployments. Addressing these challenges is crucial to maintaining the reliability and integrity of industrial operations, and safeguarding against production disruptions, financial losses, and safety hazards. Through robust security measures and privacy-enhancing technologies, IIoT deployments can foster trust, compliance, and innovation in industrial settings, driving the evolution towards smart factories and connected enterprises.

Keywords – Industrial Internet of Things, Cyber Security, Network Security, Threats.

I. Introduction

The Industrial Internet of Things (IIoT) refers to the integration of interconnected devices, sensors, and software within industrial infrastructure, enabling the collection, exchange, and analysis of data to optimize operations and drive innovation. In essence, IIoT harnesses the power of internet connectivity to enhance the efficiency, productivity, and safety of industrial processes. By facilitating real-time monitoring and control of machinery, equipment, and assets, IIoT enables predictive maintenance, minimizing downtime and reducing operational costs. Moreover, IIoT fosters the automation of workflows and the optimization of resource utilization, leading to improved scalability and agility in industrial operations. Beyond operational enhancements, IIoT generates valuable insights from vast amounts of data, empowering organizations to make data-driven decisions and uncover new business opportunities. Consequently, IIoT holds profound significance in industrial settings, revolutionizing traditional manufacturing, energy production, transportation, and infrastructure management, and driving the evolution towards smart factories and connected enterprises.

Security and privacy concerns loom large in deploying Industrial Internet of Things (IIoT) systems, posing significant challenges to their widespread adoption. With the interconnection of numerous devices, sensors, and networks, IIoT environments become vulnerable to various cyber threats, including unauthorized access, data breaches, and malicious attacks. Moreover, the heterogeneous nature of IIoT devices, coupled with legacy systems and disparate protocols, exacerbates security vulnerabilities. Concerns regarding data privacy also arise due to the massive volumes of sensitive data collected and transmitted by IIoT devices, raising issues of data ownership, consent, and compliance with regulations such as GDPR and industry-specific standards. Additionally, the potential for data interception or manipulation during transmission poses risks to the integrity and confidentiality of information within IIoT ecosystems. Addressing these security and privacy concerns is crucial to fostering trust and confidence in IIoT deployments, necessitating robust encryption mechanisms, access controls, authentication protocols, and privacy-enhancing technologies to safeguard sensitive data and ensure the integrity and security of IIoT networks.

Addressing security and privacy concerns within Industrial Internet of Things (IIoT) deployments is paramount for ensuring the reliability and integrity of industrial operations. The interconnected nature of IIoT networks means that any breach in security or privacy could have far-reaching consequences, potentially leading to system downtime, production disruptions, financial losses, or even safety hazards. By safeguarding against cyber threats and unauthorized access, organizations can maintain the continuous operation of critical industrial processes, mitigate risks of equipment failure, and uphold the safety of personnel and assets. Moreover, ensuring the privacy of sensitive data collected by IIoT devices is essential for preserving the trust of stakeholders, including customers, partners, and regulatory authorities. By prioritizing security and privacy measures, organizations can bolster the resilience of their IIoT ecosystems, minimize the likelihood of security incidents, and uphold the integrity of industrial operations, thereby fostering sustainable growth and innovation in the digital era.

II. Overview of Security Threats in IIoT

Cyber-Physical Attacks:

Cyber-physical attacks represent a potent fusion of digital infiltration with physical consequences, exploiting vulnerabilities in interconnected systems to compromise physical infrastructure or assets. These assaults target the interface between the cyber and physical realms, leveraging digital pathways to manipulate or disrupt physical components. From tampering with critical infrastructure like power grids or transportation systems to compromising industrial machinery or medical devices, cyber-physical attacks pose significant risks to public safety, national security, and economic stability. The convergence of cyber and physical domains amplifies the impact of these attacks, demanding integrated defence strategies and heightened vigilance in safeguarding both digital and physical infrastructures.

Cyber Attacks

- **Cloud malware injection**: Cloud malware injection involves an attacker inserting malicious code or a worm onto a Virtual Machine (VM) in a cloud system, enabling it to spread and infect other targets within the cloud. Implementing service instance integrity checks before processing incoming requests can effectively thwart this attack. [1]
- **Authentication attacks**: The majority of cloud services still rely on single-factor knowledge-based authentication, which consists of a simple username and password. This attack can be avoided by

multi-factor authentication, delayed response, and account lockdown. [1]

- **Man-in-the-Middle Cryptographic Attack**: In this type of attack, the attacker inserts himself into the communication line between two users (MitM) to intercept or change their exchanges. Mutual authentication or OTP (one-time password) can stop such attacks. [1]
- **Attacks on mobile devices**: Malware, data exfiltration, data manipulation, and data loss are examples of attack vectors for mobile devices. Make sure the program only receives the appropriate rights, and make sure it doesn't have any backdoors by looking up trusted signatures, to stop these attacks on mobile devices. [1]
- **Phishing attacks**: These are cyberattacks in which perpetrators deceive victims into interacting with phony emails or webpages to obtain sensitive personal information. Creating awareness about these types of attacks is the most effective deterrent against phishing. [1]
- **SQL Injection**: An injection attack known as SQLi occurs when an attacker inserts malicious input into a database to retrieve sensitive information, erase the database, and get around authentication. By utilizing stored procedures and parameterized queries, SQLi can be avoided. [1]
- **Malware**: If the IT systems are not patched and no security strategy is put in place, harmful code can spread to the OT network by delivering malicious payloads to the lower-layer devices. Malware operates at layer IV. Malware can be found using security firewalls and antivirus software that receives frequent updates. [1]

Physical Attack

- **Tampering**: The act of physically altering a communication link or device (such as an RFID) is referred to as tampering. [2]
- **Malicious Code Injection**: In this technique, an attacker compromises a physical device to introduce malicious code, which may enable them to conduct more assaults. [2]
- **RF Interference/Jamming**: To initiate DoS attacks against the RFID tags/sensor nodes and impede communication, the attacker generates and transmits noise signals over the Radio Frequency (RF)/WSN signals. [2]
- **Fake Node Injection**: To manipulate data flow between two genuine network nodes, an attacker inserts a fake node in between them. [2]
- **Sleep Denial Attack**: The attacker uses a sleep deprivation technique to keep battery-operated gadgets awake by feeding them incorrect input. Their batteries run out of power as a result, shutting down. [2]
- **Side Channel Attack**: In this attack, the attacker uses timing, power, fault, and other techniques to target system devices and obtain the encryption keys. This key allows it to encrypt and decrypt private information. [2]

Real-world Incidents of Cyber-Physical Attacks

- A DDoS attack was launched against Dyn, a DNS service provider, in October 2016 (C. Analysis). The attack, which impacted Twitter, GitHub, and other sites, lasted for a few hours. Also hindered was access to well-known websites like PayPal, the BBC, and others. [2]

- A European gang used Man-in-the-Middle (MiTM) attacks in 2015 to snoop on and intercept email payment requests (SOPHOS, 2015). According to the investigations, the group was carrying about 6 million euros. They were keeping an eye out for payment requests and sniffing around for them, which gave them unauthorized access to company email accounts. [2]
- The Mirai Botnet: Using an Internet of Things botnet, the biggest DDoS attack against DNS provider Dyn was launched in October 2016. A virus known as Mirai, which caused the shutdown of significant sections of the Internet, including Twitter, Netflix, and other sites, allowed the botnet to operate. [2]
- The Jeep Hack: Using a software upgrade vulnerability, a group of researchers was able to take control of the car via the Sprint cellular network in July 2015. It turned out that they could steer the vehicle off the road and adjust its speed. [2]
- An insider unapproved access assault occurred against Sage, a UK-based provider of accounting and HR software, in 2016. [2]
- An employee of the business gained unauthorized access to steal sensitive customer data, including pay and bank account information. [2]
- Private data on over 50 million Facebook users was compromised by Cambridge Analytica in March 2018. [2]

Data Breaches and Unauthorized Access:

Vulnerabilities

The Edge

At the edge of an IIoT system lies the field level, where devices equipped with sensors, actuators, and controllers are directly linked to the Internet or through a gateway. These edge devices, comprising machines, sensors, actuators, controllers, and intelligent nodes, can be wired or wirelessly connected via Bluetooth, WIFI, NRF, or LiFi. Machine-to-machine communication occurs at this level, even without an Internet connection, with many devices deployed on low-power networks. Despite the emphasis on cyber threats, the primary security concerns for edge devices are electronic disruptions like jamming or physical attacks due to their remote deployment and limited accessibility. [3]

Wireless Sensor Networks

Wireless Sensor Networks (WSN) form a critical component of the edge layer in IIoT systems, providing extensive insight into industrial operations across vast geographical areas. These networks consist of numerous low-power sensors deployed for various purposes such as quality control, traffic monitoring, and disaster response. Advancements in communication technologies like Zigbee and Bluetooth Low Energy have facilitated the integration of WSNs into IIoT systems, although their vulnerability to attacks due to open wireless channels and resource limitations remains a concern.

WSNs face both passive and active attacks, including monitoring, impersonation, and sinkhole attacks, which require proximity to the targeted devices. Passive attacks can lead to subsequent active attacks, posing significant risks to the integrity and security of WSNs. Gateways play a crucial role in WSN communication, aggregating data from the edge layer before passing it on to higher levels of the IIoT system for processing. Meanwhile, fog computing, positioned between the edge and cloud layers, enables efficient data processing and storage closer to the data sources, ensuring low latency and effective management of time-sensitive data within IIoT systems. [3]

SCADA & PLCs

Supervisory Control and Data Acquisition (SCADA) systems serve as the central nervous system of industrial control systems, allowing operators to monitor and manage processes from control room consoles. Traditionally, SCADA networks have relied on proprietary protocols and isolation from other networks for security. Attacks targeting protocols such as Modbus, DNP3, and IEC-60870-5-014 have been documented, raising concerns as IIoT devices are integrated into industrial processes, shifting towards IP-based cyber-physical systems.

Embedded within IIoT systems like "Smart Train" or "Smart Grid," SCADA systems feature lower-layer sub-controllers known as programmable logic controllers (PLCs), which revolutionized industrial automation following Dick Morley's invention in 1968. PLCs, integrated with remote terminal units (RTUs) and human-machine interfaces, form the backbone of SCADA systems, responsible for command disaggregation within industrial processes. Attacks against PLCs may exploit vulnerabilities in communication protocols or target command disaggregation, allowing attackers to manipulate control processes for malicious purposes. [3]

The Cloud

Before the advent of IIoT, businesses turned to cloud storage as a cost-efficient alternative to on-premise solutions, sparing them from the burdens of hardware upgrades, software maintenance, and dedicated administrators. Despite its central role in IIoT, the cloud presents a significant security vulnerability as the responsibility for data security is shifted to cloud service providers (CSPs), whose track record in data security is less than perfect.

Cloud-based services encompass not only data storage but also software applications, platforms, and virtual infrastructure. Even SCADA systems can operate in the cloud, posing risks particularly concerning communication with controlled devices, which may occur via unsecured satellite or radio channels. [3]

Attacker's areas of attack

This risk involves an attacker using industrial IoT devices as the door into the central network where important and sensitive data is stored. Because the attack surface is very large for many industrial IoT devices, due to the legacy technology concerns we mentioned above, it makes them a prime target to use as the "doorway" to larger corporate networks.

Attackers can simply use them as a way to gain entry to your enterprise network and gain access to data you are looking to keep protected, including:

- **Client or partner data:** Any information about your clients or partners, including their passwords, their customers, or their internal systems.
- **Personally identifiable information:** This can be personal or identifying data about your customers or other employees.
- **Intellectual Property or Trade secrets:** Anything that is vital to how your company or its customers or partners work that would be negative if it found itself in the hands of your competitors.
- **Health data:** Any health or personal data protected by HIPAA regulations.
- **Financial data:** Information about finances for your company, your clients, partners, or your customers including bank details and login information.

Denial-of-Service (DoS) Attacks:

Denial of Service (DoS) attacks pose a significant threat to networks by restricting servers from serving legitimate clients, typically targeting network bandwidth or services. In Cloud environments, DoS attacks are particularly damaging, often involving innocent hosts in the network sending demands, thus earning the moniker "Cloud Zombie Attack." Firewalls play a crucial role in managing access to requests, while Intrusion Detection Systems (IDS) aid in detecting such attacks. Additionally, implementing robust authentication and

authorization systems can help mitigate the risk of DoS attacks.

These attacks can severely disrupt services for legitimate users, rendering systems inaccessible due to the flooding of malicious requests. In industrial environments, such disruptions can be especially detrimental, potentially preventing stakeholders from accessing critical data. Another variant, Permanent Denial of Service (PDoS) or phishing, involves the destruction of IoT devices through hardware sabotage, such as destroying firmware or uploading corrupted BIOS using malware. Furthermore, Distributed Denial of Service (DDoS) attacks compound the threat by leveraging multiple compromised nodes to flood messages or connection requests, effectively overwhelming and crashing system servers or network resources. [1],[2]

Protection Mechanism from Denial of Service (DoS)

Prevention using filters

To stop harmful traffic, it's crucial to filter it out. These filtering methods primarily stop attacks and prevent unwittingly participating in them. Generally, routers use filtering to allow only valid traffic to reach a system. Here, we'll discuss various filtering methods described in studies, including how effective they are at preventing DDoS attacks. [4]

Ingress/egress filtering

One common filtering technique is called ingress/egress filtering. These methods stop traffic with fake IP addresses from getting into or out of a protected network. Ingress filtering blocks bad traffic heading into a local network, while egress filtering stops bad traffic from leaving a local network. Ingress filtering, as defined in RFC 2267, only lets traffic into the network if it matches a certain range of domain prefixes. So, if an attacker uses a fake IP address that doesn't match this range, it gets blocked by routers. These filters are effective against many DDoS attacks that use fake IPs. However, they're not as helpful if attackers use valid IPs from botnets. Also, these filters rely on knowing the expected range of IPs for a given port, which can be tricky in complex network setups. Plus, if an attacker uses fake IPs within the valid range, the filters won't catch the bad traffic. Mobile IP users also need special tunneling setups to avoid being filtered by ingress/egress filters. Overall, because ISPs don't always enforce these filters, they're only partly used in networks. [4]

Martian address filtering and source address validation

Martian address filtering, as described in RFC 1812, helps block fake IP addresses that come from a limited range. This filtering stops routers from forwarding packets with invalid source or destination IP addresses, including reserved, special, or unassigned ones. It also ensures that packets with the destination IP address 255.255.255.255/32 are rejected by the router.

Source address validation, also in RFC 1812, is another method used by routers. Here, the router checks if the source address of a packet matches the interface it's received on. If not, the packet is discarded, helping to catch packets with fake source IPs. However, this method can lead to many legitimate packets being wrongly discarded, especially in the asymmetric routes of the Internet, where interfaces might not always match up. Unfortunately, not all routers on the Internet use these filtering techniques. [4]

Route-based packet filtering

Route-based packet filtering (RPF) is a method that stops packets with fake source IP addresses. It's like an expansion of ingress filtering but for core routers. RPF checks the route information of each packet as it moves through the core router links. If a packet's source address doesn't match the limited set allowed on that link, it's seen as fake and discarded. However, to use RPF, routers need detailed Border Gateway Protocol (BGP) routing info.

Researchers found that for RPF to work well, around 18% of the internet's autonomous systems (AS) need to use it. But in reality, this isn't practical. Also, adding source addresses to BGP messages, as RPF requires, increases message size and processing time. If routers don't stay updated, RPF might mistakenly discard legitimate packets due to route changes. Plus, attackers can manipulate BGP sessions to bypass RPF. Another issue is that if attackers use IP addresses that don't look like fake ones, RPF won't catch them. Duan et al. propose a solution that uses local BGP update messages to spot fake IPs, making it easier to deploy and reducing false positives. [4]

History-based filtering

This filtering method relies on packet marking and uses past normal traffic to identify and block malicious traffic. Here, the target of an attack keeps a record of IP addresses commonly seen in its traffic. When facing a bandwidth attack, it only accepts IP addresses found in its database and rejects all others. However, if an attacker can make its attack traffic look like normal traffic, this method won't be able to spot and block the harmful flow effectively. [4]

III. Mitigation Strategies and Best Practices

Physical Damage Attacks−Countermeasures:

- Installation of strong fences around critical equipment and infrastructure.
- Use of anti-theft and tracking devices to deter potential attackers.
- Deployment of motion detection cameras and alarm systems for real-time alerts
- Regular inspection and assessment of equipment for signs of tampering or damage.
- Adoption of anti-tampering and anti-counterfeiting technologies
- Utilization of technologies to detect attempts to tamper with or counterfeit components
- Ensuring authenticity and reliability of IIoT devices [5]

Tampering Attacks−Countermeasures:

- Adoption of anti-tampering and anti-counterfeiting technologies.
- Utilization of technologies to detect attempts to tamper with or counterfeit components.
- Implementation of secure boot and code signing to prevent unauthorized code changes.
- Use of cryptographic techniques to preserve data integrity.
- Making it harder for attackers to modify data during transit or storage. [5]

Ransomware Attacks−Countermeasures:

- Implementation of cyber threat hunting (CTH) to proactively identify and mitigate threats.
- Regular application of firmware and device patches to address known vulnerabilities.
- Minimization of attack surface for ransomware
- Introduction of more robust and secure endpoints to enhance device security.
- Reduction of likelihood of successful ransomware infiltrations.
- Adoption of countermeasures to bolster resilience against ransomware attacks.
- Safeguarding critical industrial operations and data from potential harm through these measures. [5]

Malware−Countermeasures:

- Implementation of sophisticated cybersecurity frameworks for comprehensive protection.

- Employment of dependable authentication methods such as multifactor authentication (MFA) during updates.
- Reduction of risk of malware infiltration by limiting access to authorized personnel.
- Utilization of the interplanetary file system (IPFS) for data storage and retrieval to enhance data integrity and availability.
- Mitigation of potential malware-induced data loss through IPFS
- Creation of regular backups of data on devices to safeguard against data loss or corruption
- Fortification of the IIoT perception layer against malware attacks
- Enhancement of resilience and safeguarding of integrity and availability of essential industrial processes and data through these measures

Patch Management Techniques

- Many IIoT device manufacturers do not regularly provide security updates, leaving devices vulnerable to known vulnerabilities.
- Timely patching is crucial to secure IIoT systems and reduce the risk of attacks on industrial processes.
- Internal mechanisms for patching vulnerabilities should be reinforced in firms to ensure timely updates.
- Manufacturers need to consistently provide security fixes for their devices throughout their lifespan.
- Automated patch installation can simplify the process for a large number of IIoT devices.
- However, patching industrial systems requires thorough testing to ensure compatibility with existing configurations.
- NIST recommends regression testing as part of a systematic patch management approach to enhance safety and minimize process downtime.
- The IETF offers an automatic firmware upgrade method for resource-constrained IoT devices, ensuring secure end-to-end transfer of new firmware.
- Active methods for detecting security problems in IIoT installations include evaluating devices during idle moments and assessing vulnerabilities using network graphs.
- These methods help identify security flaws and their impact on systems, allowing for appropriate actions to be taken, such as isolating vulnerable devices. [6]

Cryptography and Authentication Mechanisms

- Encryption is crucial for maintaining data secrecy and providing authentication in IIoT systems.
- Resource constraints in many IIoT devices require lightweight symmetric-key encryption methods.
- Symmetric key cryptography can lack a secure and scalable management infrastructure, making participant secrecy challenging.
- Both public-key and symmetric key cryptographic methods can introduce unacceptable delays in safety-critical procedures.
- The increasing data transmission and reliance on cloud services in IIoT systems require robust security measures against unauthorized access.
- Therefore, specialized encryption and authentication technologies tailored to the IIoT environment are needed.
- These technologies must address the resource constraints of IIoT devices while ensuring secure and efficient data transmission.
- Implementing such technologies will enhance data security and protect IIoT systems from potential threats.
- It is essential for IIoT systems to adopt encryption and authentication solutions that meet their specific requirements and challenges.

- By prioritizing security measures, IIoT stakeholders can safeguard sensitive data and maintain the integrity of industrial operations. [6]

DEA Method

- The Data Envelopment Analysis (DEA) is an economic method used to measure efficiency.
- Efficiency is the ratio of output to the effort or resources invested.
- DEA measures efficiency relative to the highest level of efficiency.
- It involves non-parametric estimation of the relationship between input and output data.
- DEA can handle various input and output factors without assuming a specific functional relationship.
- It allows for different scales of input and output elements.
- By using existing data, DEA eliminates the need for creating separate data for performance measurement.
- It evaluates the relative performance of decision-making units (DMUs).
- DMUs need to be homogeneous for accurate comparison.
- DEA analysis methods include the Charnes, Cooper, and Rhodes (CCR) and Banker, Charnes, and Cooper (BCC) approaches. [7]

IV. Future Directions and Research Challenges

Emerging Threats and Vulnerabilities:

Emerging threats and vulnerabilities in Industrial Internet of Things (IIoT) environments present formidable challenges to the security and integrity of industrial operations. One such threat is the proliferation of sophisticated malware specifically designed to target IIoT devices and networks. These malicious programs can infiltrate systems, compromise sensitive data, and disrupt critical infrastructure, leading to significant financial losses and operational downtime. Additionally, the increasing use of edge computing and cloud services introduces new attack vectors, as these technologies create additional points of entry for cyber attackers. Furthermore, the diverse array of IIoT devices, often characterized by resource constraints and outdated firmware, poses a significant vulnerability, as these devices may lack robust security features and receive infrequent updates, making them susceptible to exploitation. Moreover, the convergence of operational technology (OT) and information technology (IT) networks in IIoT deployments blurs the traditional boundaries between industrial control systems and enterprise IT environments, creating potential pathways for attackers to breach critical infrastructure. To address these emerging threats and vulnerabilities effectively, organizations must adopt a proactive approach to cybersecurity, encompassing comprehensive risk assessments, ongoing monitoring, and the implementation of robust security controls and best practices throughout the IIoT ecosystem.

Some of these research gaps include:

- **Scalability and Interoperability:** While many IIoT solutions have been developed, scalability and interoperability remain significant challenges. There is a need for research into scalable architectures that can support the increasing number of devices and data generated by IIoT systems. Additionally, interoperability standards are essential for the seamless integration of diverse IIoT devices and platforms, warranting further investigation.
- **Security and Privacy**: Despite efforts to enhance security in IIoT deployments, cybersecurity threats continue to evolve. Research is needed to develop more robust security mechanisms to protect IIoT systems from emerging threats, such as zero-day attacks and supply chain vulnerabilities. Similarly, addressing privacy concerns related to data collection, sharing, and storage in IIoT environments requires further investigation.
- **Edge Computing and Data Analytics**: Edge computing plays a crucial role in

IIoT by enabling real-time data processing and decision-making at the edge of the network. Research gaps exist in optimizing edge computing architectures for IIoT applications, as well as developing efficient algorithms for data analytics and machine learning at the edge to extract actionable insights from sensor data.

- **Reliability and Resilience**: Ensuring the reliability and resilience of IIoT systems is essential for mission-critical industrial operations. Research is needed to develop fault-tolerant architectures and redundancy mechanisms to minimize downtime and system failures. Additionally, investigating resilience strategies to withstand cyber-physical attacks and natural disasters is crucial for maintaining continuous operation in IIoT environments.
- **Energy Efficiency**: Energy consumption is a significant concern in IIoT deployments, particularly in remote or resource-constrained environments. Research gaps exist in developing energy-efficient communication protocols, low-power hardware designs, and optimization techniques for reducing the energy footprint of IIoT devices while maintaining performance.
- **Human-System Interaction**: The human-machine interface plays a critical role in IIoT applications, influencing user acceptance and effectiveness. Research is needed to design intuitive interfaces, develop adaptive automation systems, and address human factors considerations to enhance the usability and user experience of IIoT technologies in industrial settings.

V. Conclusion

In summary, the literature review highlights the critical need for robust security measures and privacy considerations in IIoT deployments. Continued collaboration among industry, policymakers, and researchers is essential to address emerging threats effectively. This research has direct implications for industry practitioners, policymakers, and researchers alike, emphasizing the importance of advancing IIoT security and privacy technologies. By working together, we can foster trust, compliance, and innovation in IIoT ecosystems, ultimately ensuring the integrity and reliability of industrial operations while safeguarding sensitive data.

VI. References

[1] A. C. Panchal, V. M. Khadse and P. N. Mahalle, "Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures," *2021 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*, Lonavala, India, 2018, pp. 124-130, doi: 10.1109/GCWCN.2018.8668630

[2] Jayasree Sengupta, Sushmita Ruj, Sipra Das Bit, A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT, Journal of Network and Computer Applications, Volume 149, 2020, 102481, ISSN 1084-8045

[3] Hoffman, Fred. "INDUSTRIAL INTERNET OF THINGS VULNERABILITIES AND THREATS: WHAT STAKEHOLDERS NEED TO CONSIDER." *Issues in Information Systems* 20.1 (2019)

[4] Mahjabin T, Xiao Y, Sun G, Jiang W. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks*. 2017;13(12). doi:10.1177/1550147717741463

[5] A. H. Eyeleko and T. Feng, "A Critical Overview of Industrial Internet of Things Security and Privacy Issues Using a Layer-Based Hacking Scenario," in *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 21917-21941, 15 Dec.15, 2023, doi: 10.1109/JIOT.2023.3308195.

[6] H. Sarjan, A. Ameli and M. Ghafouri, "Cyber-Security of Industrial Internet of Things in Electric Power Systems," in *IEEE Access*, vol. 10, pp.

92390-92409, 2022, doi: 10.1109/ACCESS.2022.3202914

[7] Park, S. and Lee, K., 2021. Improved Mitigation of Cyber Threats in IIoT for Smart Cities: A New-Era Approach and Scheme. *Sensors*, *21*(6), p.1976.

[8] T. Gebremichael *et al*., "Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges," in *IEEE Access*, vol. 8, pp. 152351-152366, 2020, doi: 10.1109/ACCESS.2020.3016937

[9] Dhirani LL, Armstrong E, Newe T. Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap. *Sensors*. 2021; 21(11):3901. https://doi.org/10.3390/s21113901

.