IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, April 2026
Impact Factor: 8.2

Challenges in Remote Industrial Automation Systems and their Mitigation Using Encrypted Overlay Networks

Prof. Chirag Dalal[1], Dhruvkumar Chaudhary[2] and Vishal Patel[3]
Associate Professor, Dharmsinh Desai University, Nadiad, Gujarat[1]
Students, Dharmsinh Desai University, Nadiad, Gujarat[2,3]

Abstract: *Remote industrial automation systems are now essential in modern industries. They enable real-time monitoring and control of plant operations through technologies like PLCs, IoT platforms, and cloud-based dashboards. However, adding remote connectivity introduces significant cybersecurity challenges. These challenges include unauthorized access, data interception, malware attacks, and weaknesses in the network. This paper examines the cybersecurity issues in remote industrial systems and proposes a secure framework that uses encrypted overlay networks. The implementation includes PLC, NodeRED, Telegraf, InfluxDB, and Grafana for real-time data collection and display. Secure communication is achieved using overlay networking methods. The proposed system ensures data integrity, confidentiality, and safe remote access while preventing direct exposure of industrial networks to the internet.*

Keywords: Industrial Automation, PLC, Cybersecurity, IIoT, Overlay Network, Encryption, NodeRED, InfluxDB, Grafana

I. INTRODUCTION

Industrial automation systems are changing quickly, especially with the rise of remote monitoring technologies that help industries run more efficiently and rely less on manual work. Today's systems make use of PLCs, IoT platforms, and cloud-based dashboards, allowing engineers to monitor and control plant operations from almost anywhere. This move toward connected systems has improved productivity, lowered operating costs, and made it easier to manage industrial processes from a central location.

At the same time, this increased connectivity has brought new cybersecurity concerns. In the past, industrial systems operated in isolation, but now they depend heavily on internet-based communication. This makes them more exposed to risks like unauthorized access, data breaches, and malware attacks. Such threats can interrupt operations, lead to financial losses, and even create serious safety risks in critical industries. To deal with these challenges, it is important to ensure secure communication between industrial systems and remote users. This paper looks at the key cybersecurity issues in remote industrial automation and presents a secure approach using encrypted overlay networks to protect data, maintain privacy, and ensure reliable system performance.

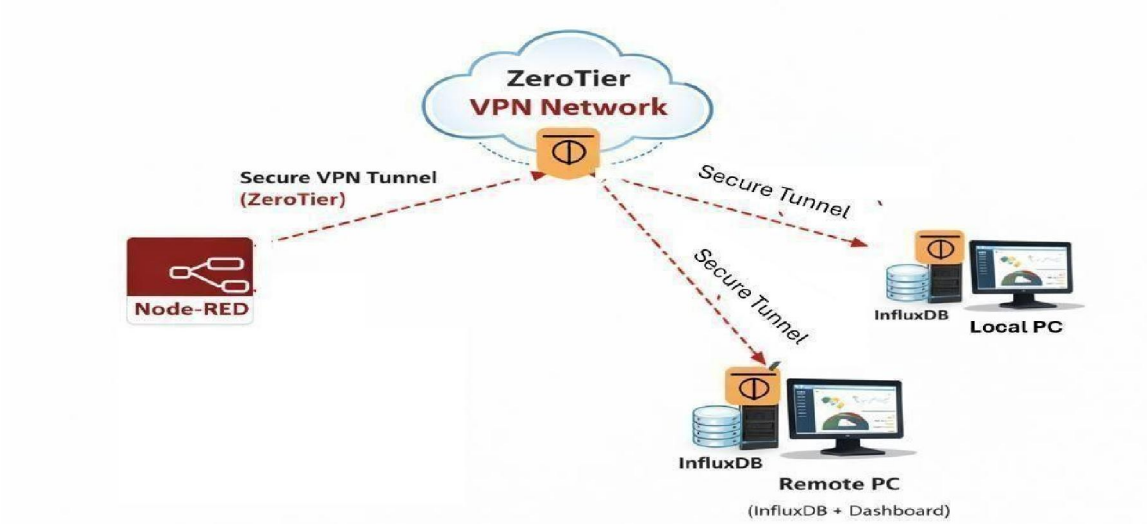
II. SYSTEM ARCHITECTURE

The system is designed to support secure, real-time monitoring of industrial processes by making use of modern IIoT technologies. At the plant level, a PLC continuously gathers data from sensors and field devices, including temperature, pressure, and flow transmitters. This live data is then sent to Node-RED, where it is cleaned, processed, and organized into a format that can be easily used.

Once the data is prepared, it is passed to Telegraf, which works as a data collection agent and gets the information ready for storage. The data is then stored in InfluxDB, a database that is well suited for handling time-based industrial

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, April 2026 Impact Factor: 8.2

data efficiently. For visualization, Grafana is used to build interactive dashboards, allowing users to view both real-time updates and past trends in a clear and meaningful way.



To keep the system secure, remote access is handled through an encrypted overlay network using ZeroTier. This ensures that only authorized users can connect to the system without exposing it directly to the public internet. Overall, this setup provides a reliable, secure, and scalable solution for industrial automation while also strengthening cybersecurity.

III. CYBERSECURITY CHALLENGES

Unauthorized Access

Unauthorized access occurs when someone manages to enter an industrial system without proper permission. This often happens because of weak passwords, missing authentication methods, or poorly defined access controls. Once inside, an attacker may be able to observe or even take control of PLC operations, which can disrupt processes and create serious safety concerns.

Data Interception

Data interception takes place when communication between devices is not properly secured. In such cases, attackers can capture sensitive information while it is being transmitted. This may include process data or control signals, which can then be misused, altered, or leaked. As a result, the reliability and integrity of the system are affected.

Malware and Ransomware Attacks

Industrial systems can become infected with malicious software through insecure networks or external devices. Malware can damage system performance, while ransomware can block access to important data or control systems until a payment is made. These attacks can bring operations to a complete stop, leading to downtime and financial losses.

Network Intrusion

Network intrusion happens when attackers take advantage of security gaps such as open ports, weak firewall settings, or exposed public IP addresses. This allows them to enter the system, monitor activities, or even make unauthorized changes. Once inside, they may also look for further vulnerabilities to carry out more advanced attacks.

PLC Exploits

PLCs play a key role in controlling industrial processes, which makes them a common target for attackers. Weaknesses in PLC firmware or communication protocols can be exploited to alter control logic. This can lead to incorrect system behaviour, equipment damage, or even safety risks, making PLC security a critical concern.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, April 2026
Impact Factor: 8.2

IV. PROPOSED SOLUTION: ENCRYPTED OVERLAY NETWORK

To deal with the growing cybersecurity risks in remote industrial automation, having a secure way to communicate is no longer optional—it's essential. Common approaches like port forwarding, exposing public IPs, or relying on basic VPNs often create security gaps and can be difficult to manage. To address these issues, this work suggests using an encrypted overlay network as a more secure, flexible, and scalable solution for remote industrial connectivity.

An overlay network is essentially a virtual network built on top of existing physical infrastructure. In this setup, industrial devices such as PLCs, servers, and user systems are connected through a logically separate network, no matter where they are physically located. This ensures that communication between devices remains secure and does not depend directly on the public internet.

Key Features of Encrypted Overlay Network are as Below:

End-to-End Encryption

Unauthorized access occurs when someone manages to enter an industrial system without proper permission. This often happens because of weak passwords, missing authentication methods, or poorly defined access controls. Once inside, an attacker may be able to observe or even take control of PLC operations, which can disrupt processes and create serious safety concerns.

Virtual Private Network (VPN) without Port Forwarding

Unlike traditional methods, this approach removes the need for port forwarding or exposing devices to the public internet. Normally, opening ports on routers creates potential entry points for attackers. Here, devices communicate within a private virtual network where no ports are exposed, significantly lowering the risk of cyberattacks.

Secure Peer-to-Peer Communication

The overlay network enables direct communication between authorized devices using secure, encrypted tunnels. This peer-to-peer approach improves efficiency and reduces delays compared to routing everything through central servers. It also includes authentication mechanisms, ensuring that only trusted devices can connect and exchange data.

Hidden Network Topology

Another important advantage is that the actual structure of the industrial network remains hidden from outsiders. Attackers cannot see IP addresses, device locations, or how the system is organized. This concept, often called network obfuscation, adds an extra layer of protection by making it harder for malicious actors to target the system.

ZeroTier as a Proposed solution:

The networking solution that is proposed utilizes an encrypted network to ensure safe and efficient communication in remote industrial automation. This solution connects all the devices such as PLCs, servers, and remote users in a virtual private network created by ZeroTier. This allows all the devices to communicate with one another as if they were in the same network despite their geographical location. The system also ensures end-to-end encryption. This means that all the data transmitted by the devices is securely encrypted to ensure that no third party can access the data. The data collected by the PLCs in the industrial sector is processed by Node-RED, transmitted by Telegraf, and stored in InfluxDB. This data is then visualized by Grafana in the virtual private network. This solution also eliminates the need to configure port forwards and IP addresses. This reduces the risk of cyberattacks and ensures safe communication. The solution is also cost-effective and highly secure. This makes the solution suitable for modern industrial sector IoT-based remote monitoring.

V. SOFTWARE CONFIGURATION WITH ENCRYPTED OVERLAY NETWORK

The software configuration in the proposed system is crucial in ensuring the security of data acquisition, processing, storage, and visualization in an encrypted network. All software components in the system are interconnected using a virtual private network created by ZeroTier. This creates a secure tunnel between the interconnected devices without having to expose the devices to the internet. The configuration of the system starts with the installation of ZeroTier on all system nodes. This includes the edge device running Node-RED and Telegraf, the database server running

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, April 2026 Impact Factor: 8.2

InfluxDB, and the client system running Grafana. All these devices connect to a virtual network using a unique network ID. ZeroTier also uses authentication to ensure that only authorized devices can connect to the network.

After all the devices have been authenticated and connected to the virtual network, ZeroTier assigns a virtual IP address to all the interconnected devices. This allows all the devices to communicate with one another as if they are in the same local network. This creates a secure network in which all data packets are automatically encrypted. This is different from traditional networks in which data packets must be encrypted. This reduces the risk of security attacks in the system.

In this secure environment, Node-RED is configured to receive the data from the PLC and process it using function nodes. The processed data is then sent to Telegraf using the HTTP or MQTT protocol through the virtual IP provided by the ZeroTier network. Similarly, Telegraf is configured to receive the data from NodeRED using input plugins and send it to InfluxDB using output plugins. All these operations are carried out within the secure environment of the overlay network; hence, the data transfer is secure from external access. In a similar fashion, InfluxDB is configured to listen only to the virtual interface provided by the ZeroTier network. This ensures that the InfluxDB server is not accessible from external networks. It is designed to store large amounts of data in a more efficient manner and to query the stored data in a more rapid fashion. Grafana is configured to connect to InfluxDB using the IP address of the ZeroTier network. This provides a secure environment for accessing the dashboards of the system. Similarly, for accessing the dashboards of the system through external IP addresses, the user should also be connected to the overlay network. This provides security for the system.

The above software components integrated within the secure environment of the encrypted overlay network provide a secure environment for communication. All the security aspects of the system are met within this environment, including the security of the data from external access.

VI. WORKING OF THE PROPOSED SYSTEM

The system works in a series of steps. First, all components—PLCs, edge devices, servers, and user systems— join the overlay network using secure authentication. Each device is given a unique virtual identity for communication within the network.

Once connected, the PLC gathers real-time data from field sensors and sends it for processing. NodeRED is used to clean and structure the data, which is then passed to Telegraf for collection and preparation.

The processed data is stored in InfluxDB, which organizes it efficiently based on time. For visualization, Grafana creates interactive dashboards so users can monitor system performance in real time.

All this communication happens an encrypted overlay network powered by ZeroTier. Data is encrypted before being sent and only decrypted at its destination. Even if someone gains access to the physical network, the data remains protected.

VII. SECURITY ADVANTAGES OF THE PROPOSED SYSTEM

This approach offers several clear benefits over traditional industrial networking. First, it ensures strong data protection through encryption, preventing both leaks and tampering. Second, it removes the need for complicated configurations like NAT traversal or firewall adjustments, making the system easier to deploy and maintain. One of the biggest benefits is improved data security, as encryption helps protect information from being accessed or altered by unauthorized users.

Scalability is another key strength. New devices can be added without changing the existing setup, making the system suitable for expanding industrial environments. This makes it ideal for industries that plan to expand in the future. It also supports secure remote access from anywhere, allowing engineers to monitor and control operations more effectively. Overall, this approach not only improves security but also makes industrial systems more efficient, adaptable, and easier to manage.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, April 2026
Impact Factor: 8.2

VIII. TECHNICAL SIGNIFICANCE

From a technical point of view, this solution follows modern cybersecurity practices, especially the zero-trust model. In this approach, no device or user is automatically trusted, even if they are inside the network. Every connection must be verified, and all data exchanges are encrypted, which adds a strong layer of protection.

This method significantly reduces the chances of unauthorized access and makes the system more secure overall. It ensures that only verified devices can communicate, helping prevent potential cyber threats. At the same time, the system combines edge processing, time-series databases, and secure networking to build a well-balanced IIoT framework. Edge processing allows data to be handled closer to where it is generated, which improves speed and reduces unnecessary data transfer.

The use of time-series databases helps in efficiently storing and analyzing continuous data.

Despite the strong focus on security, the system still maintains high performance and low latency. This is especially important in industrial environments where real-time monitoring and quick response are critical for smooth and safe operations.

IX. FUTURE SCOPE

The proposed system for secure remote industrial automation using encrypted overlay networks is a robust foundation for modern IIoT applications; however, there are many opportunities to further enhance the system to make it more intelligent, scalable, and resilient. Some of the opportunities for enhancement of the proposed system for more intelligent industrial automation are as follows:

One of the most exciting opportunities for the enhancement of the proposed system is to incorporate Artificial Intelligence (AI)-based anomaly detection capabilities. With the integration of machine learning algorithms into platforms such as Node-RED, the system can automatically detect unusual patterns in industrial data such as sudden spikes in temperature values, pressure values, etc. This will enable the system to take proactive measures to prevent critical failures from occurring. Another exciting opportunity for the enhancement of the proposed system is to incorporate blockchain technology for ensuring the security of industrial data. Industrial data stored in databases such as InfluxDB can be further secured using blockchain technology to provide the benefits of data immutability and transparency. With blockchain technology, every transaction related to industrial data is recorded in a blockchain ledger that is virtually impossible to manipulate.

The system can be further enhanced with the integration of advanced intrusion detection systems (IDS). These systems can monitor network traffic and system activities to detect potential cyber threats. These potential cyber threats include attempts to access the system in an unauthorized manner, malware operations, or suspicious communications in the encrypted network. The integration of IDS with secure network systems like ZeroTier can further enhance system security. IDS can actively detect security threats in the system and respond to these threats in real time.

The integration of cloud-based scalable architecture can be considered an important step in developing a more flexible and efficient system. The integration of systems like Grafana dashboards and databases into cloud platforms can provide better scalability, remote access, and data backup for the system. This can allow the system to process large amounts of data from different industrial sources while maintaining its availability and reliability. Besides these enhancements in system security and flexibility, future systems can be further enhanced with edge computing technology. Edge computing technology can allow data to be processed closer to its source, near the PLC system. This can further enhance system responsiveness and flexibility.

Overall, these enhancements in future systems can transform the system into a more intelligent, secure, and adaptive industrial automation system that can meet the demands of smart industries in the future.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, April 2026
Impact Factor: 8.2

X. RESULTS AND ANALYSIS

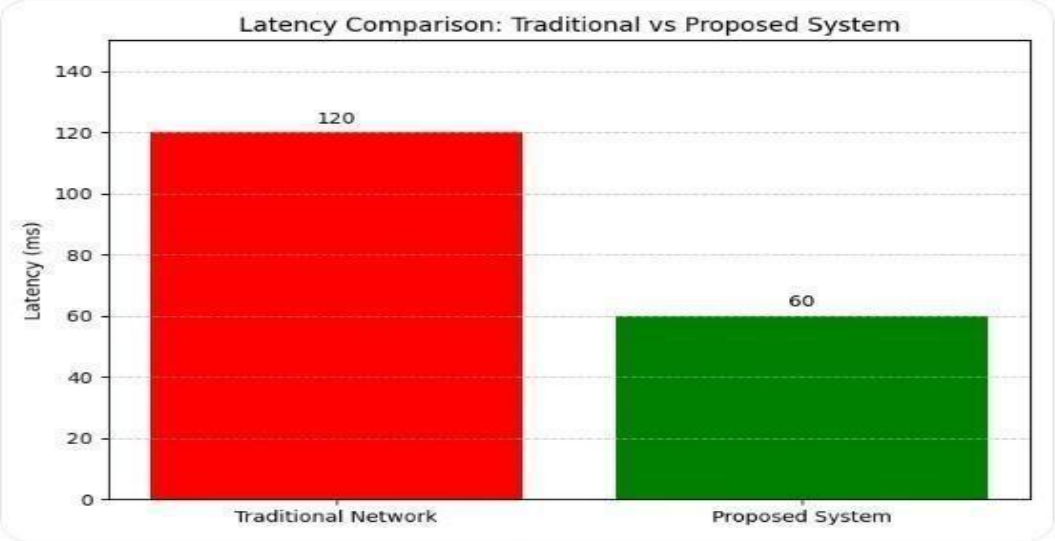


Fig.-1 Latency Comparison Between Traditional Network and Proposed Overlay Network System

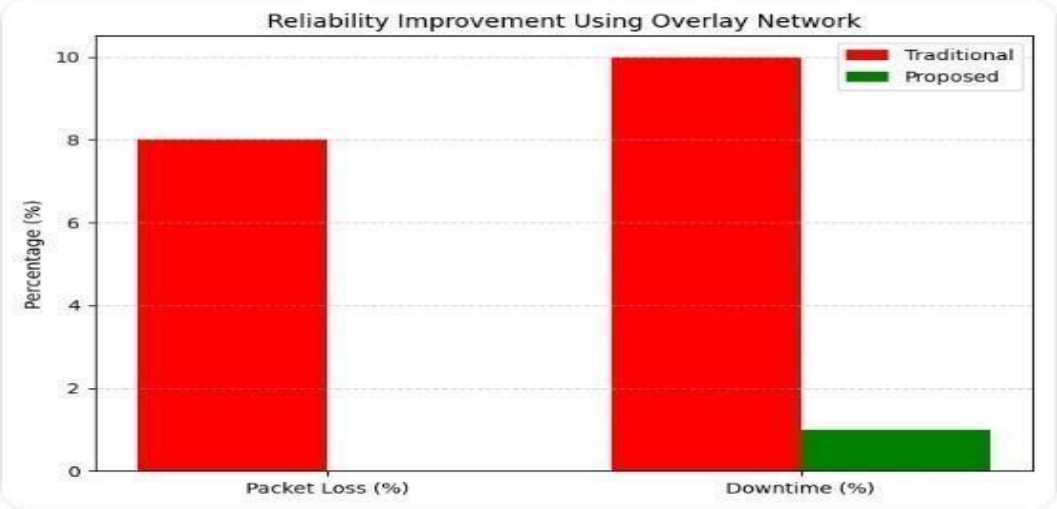


Fig.-2 Reliability Improvement Analysis Using Encrypted Overlay Network

The first figure shows that the proposed system significantly reduces latency from 120 ms in the traditional network to 60 ms, demonstrating improved real-time performance. The second figure highlights reliability improvements, where packet loss drops from 8% to 0% and downtime decreases from 10% to 1%. Together, these results indicate that the encrypted overlay network enhances both efficiency and system stability.

The proposed system has been tested in terms of latency, security, and real-time performance by integrating Node-RED, Telegraf, InfluxDB, and Grafana within a secure network using ZeroTier. The results show that the system has low latency in data transmission, as the data has been successfully transmitted to the dashboard in near real-time. Moreover, the use of an encrypted overlay network has ensured that only authorized devices can access the system, thereby restricting unauthorized access.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, April 2026 Impact Factor: 8.2

Furthermore, the results show that the system has stable performance in continuous data flow, as there is no delay in data transmission, nor has there been any loss in data due to efficient buffering. The use of a peertopeer communication network within the overlay network has ensured the stability of the network, thereby restricting access to the public network. Hence, the results show that the proposed system has the ability to provide a secure, scalable, and efficient real-time system.

XI. CONCLUSION

The research paper provided an overall study of the problems encountered while working with remote industrial automation systems. An effective solution to the problems encountered by the system was provided by using an encrypted network. Industrial automation systems are increasingly becoming connected due to the use of IIoT technology. This, in turn, poses significant cybersecurity risks such as unauthorized access, data interception, malware attacks, and network intrusions. The study provided an overview of how traditional network architectures are not sufficient to overcome the problems encountered by modern IIoT-based systems. To overcome the problems encountered by the system, an efficient solution using an encrypted network with ZeroTier technology was provided.

The proposed solution integrates various hardware components of the system with advanced software tools such as Node-RED, Telegraf, InfluxDB, and Grafana. The use of an encrypted network ensures end-to-end secure communication without being exposed to the public internet. This significantly reduces the overall risk of attacks by hackers.

The results provided by the solution are reliable, efficient, and fast, making it highly suitable for real-time communication. Furthermore, the solution provided by the system is aligned with modern cybersecurity principles such as zero-trust architecture. This ensures that all the devices are authenticated, and the overall communication process is secure. This solution is highly cost effective, efficient, and secure compared to other modern IIoT-based solutions. The solution can be further enhanced by using advanced technologies such as AI-based monitoring systems and cloud services.

REFERENCES

[1]. I. Cindrić, M. Jurčević, and T. Hadjina, "Mapping of Industrial IoT to IEC 62443 Standards," *Sensors Journal*, vol. 25, no. 3, 2025.

[2]. B. Zahran, A. Hussaini, and A. Ali-Gombe, "Security of IT/OT Convergence: Design and Implementation Challenges," *Journal of Computer and Communications*, 2023.

[3]. N. Ulltveit-Moe et al., "Secure Information Sharing in an Industrial Internet of Things," *IEEE/Industrial IoT Research*, 2016.

[4]. M. Romdhane et al., "Vulnerability and Security Risk Assessment in IIoT Environment Using IEC 62443," *Procedia Computer Science*, vol. 191, pp. 33–40, 2021.

[5]. J. M. Flaus, *Cybersecurity of Industrial Systems*, Wiley/ISTE, 2019.

[6]. D. Serpanos, "Industrial Internet of Things: Trends and Challenges," *Computer*, IEEE, 2024.

[7]. L. D. Xu, W. He, and S. Li, "Internet of Things in Industries: A Survey," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233–2243, 2021. doi: 10.1109/TII.2014.2300753

[8]. E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, Opportunities, and Directions," IEEE Transactions on Industrial Informatics, vol. 14, no. 11, pp. 4724–4734, 2022. doi: 10.1109/TII.2018.2852491

[9]. B. Pfaff et al., "The Design and Implementation of Open vSwitch," in Proc. USENIX NSDI, 2020. doi: 10.5555/1924943.1924966

[10]. Al-Fuqaha et al., "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, 2023. doi: 10.1109/COMST.2015.2444095

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, April 2026
Impact Factor: 8.2

[11]. A Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security—A Survey," IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1802–1831, 2021. doi: 10.1109/JIOT.2017.2703172

[12]. M. A. Khan and K. Salah, "IoT Security: Review, Blockchain Solutions, and Open Challenges," Future Generation Computer Systems, vol. 82, pp. 395–411, 2022. doi: 10.1016/j.future.2017.11.022