National Research Journal of Information Technology & Information Science
Volume No: 13, (January) Year: 2026 (Special Issue)
PP: 260-266
ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

SECURE COMMUNICATION IN CRITICAL WIRELESS INFRASTRUCTURE NETWORK

Subhajit Paul

Department of Computer Science Engineering Chandigarh University, Punjab, India

Azhar Ashraf

Department of Computer Science Engineering Chandigarh University, Punjab, India

Abhay Tiwari

Department of Computer Science Engineering Chandigarh University, Punjab, India

Abhijeet Kumar

Department of Computer Science Engineering Chandigarh University, Punjab, India

Shubham Kumar Jha

Department of Computer Science Engineering Chandigarh University, Punjab, India

Shreyansh Shrey

Department of Computer Science Engineering Chandigarh University, Punjab, India

ABSTRACT-

Critical infrastructure networks (CINs), such as power grids, transportation systems, and water supply networks, provide the foundation of modern society. As we continue scaling these networks, the required protection to secure communication within these networks against cyber threats, unauthorized access, and potential system failures becomes critical. This article describes the major risks and vulnerabilities in CIN communication, covering threats like Man-in-the-Middle attacks, Denial-of-Service (DoS) attacks, and Advanced Persistent Threats (APTs). We examine current security frameworks, encryption methodologies, and authentication strategies, underlining how cryptographic protocols, blockchain, and AI-based anomaly detection can be pivotal in strengthening resilience. In addition, we introduce a multi-tiered security architecture and describe how incorporating real-time monitoring mechanisms, secure network communication protocols, and a zero-trust network design paradigm can secure data transmission between elements of CINs. Future research directions: What are we going to do?

Keywords— Critical Infrastructure, Secure Communication, Cybersecurity, Cryptography, Zero-Trust Architecture, Anomaly Detection, Blockchain.

I. INTRODUCTION

Hence, critical infrastructure networks (CINs) are heavily relied on in maintaining access to critical services like power distribution, transportation management, healthcare and financial transactions. Disruption or compromise in these networks can have farreaching fallouts that include economic losses, public safety threats, risks, and national security risks." As more and more digitalized in The attack surface of CINs expands as they are susceptible to sophisticated cyber threats. Recent attacks on power grids, ICS′s and financial networks highlight saving the urgency in instituting strong security measures. Due to the interdependence among sectors in a CIN, a compromise in one can create a ripple effect across multiple sectors leading to widespread disruptions. Conventional security approaches and perimeter-based defenses can no longer adequately guard against today's threats. Sophisticated adversaries use social engineering, ransomware, and zero-day exploits to evade standard security defenses.

Additionally, CINs face unique security challenges due to their reliance on legacy systems, which often lack modern security features and cannot be easily upgraded without disrupting critical operations. CINs consist of a variety of hardware, software, and communication protocols. Additionally, the regulations around compliance differ by sector and region, further complicating how to secure communications from the CIN. In this article, we review major threats to CINs, review relevant security measures, and present a multi- layered security model that integrates new technologies like blockchain, artificial intelligence (AI), and zero-trust architecture. Our research aims to provide a comprehensive framework for safeguarding secure communication within CINs against evolving cyber threats.

II. THREATS AND CHALLENGES

Cyber threats targeting critical infrastructure networks (CINs) are on the rise and can threaten their availability, integrity, and confidentiality. Given their role in sustaining critical services such as power generation, transportation, water supply

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

and healthcare, protecting these networks is vital to avoid catastrophic disruptions of these services. We will review the major cyber threats that are aimed at CINs and the security issues that obstruct effective protection.

1. Common Cyber Threats in CINs

A. Man-in-the-Middle (MitM) Attacks

A Man-in-the-Middle (MitM) attack is when a malicious third- party intercepts and alters the communication between two authentic users without both party knowing about it. In the context of CINs, these attacks are capable of forging controlsignals, disrupting operations and most significantly, causing large-scale devastating failures. In a smart grid system, for example, an attacker could change commands for electricity distribution, causing outages or energy theft. With CIN relying on remote monitoring and control mechanisms, MitM attacks may have severe consequences. Many CINs employ wireless communication protocols or Internet-based remote access systems, which can be susceptible to interception if not adequately secured. To minimize this risk, secure communication protocols — like Transport Layer Security (TLS) — and mutual authentication mechanisms are required.

B. Denial-of-Service (DoS) and Distributed Denial-of- Service (DDoS) Attacks.

Denial-of-Service (DoS) attacks are designed to flood the resources of network such that it cannot provide service to the authentic users. In Distributed Denial-of-Service (DDoS) attacks, the issue is further complicated over the fact that the attackers employ a botnet of previously infected devices to amplify their attack and as such make it much more impactful, impacting multiple systems. CINs are also vulnerable to Distributed Denial of Service (DDoS) attacks — both in more general terms like those mentioned above, and in specific sectors where uninterrupted data exchange is critical (e.g., energy grids, financial networks, and emergency response systems). A well- coordinated DDoS attack can prevent operators from accessing critical systems, delay real-time decision-making, and cause significant economic losses. For instance, a DDoS attack on a water treatment plant could prevent operators from adjusting chemical treatment levels, leading to unsafe drinking water. To dilute the insider threats, organizations should take these precautious steps:

- **Strict access controls (role-based and least privilege access)**
- **User behavior analytics to detect unusual activity**
- **Regular security training for employees and contractors**

C. Advanced Persistent Threats (APTs)

Advanced Persistent Threats (APTs) are long-term, well planned and targeted cyberattacks carried out by well-funded and highly skilled adversaries, often linked to nation-states or organized cybercrime groups. Unlike typical cyberattacks that focus on immediate disruption, APTs aim to maintain unauthorized access to CINs for extended periods, gathering intelligence, exfiltrating sensitive data, and waiting for an opportune moment to execute a major attack. APTs typically involve multiple attack stages, including:

- **Initial intrusion (e.g., phishing emails, exploiting software vulnerabilities)**
- **Lateral movement (spreading within the network)**
- **Privilege escalation (gaining administrative control)**
- **Exfiltration and sabotage (stealing data or disrupting operations)**

Because APTs use stealth techniques to avoid detection, behavior- based threat detection and endpoint security solutions are essential to mitigating their impact.

D. Insider Threats

Insider threats are particularly concerning because legitimate users often have deep knowledge of network architectures, access controls, and operational workflows, making it easier for them to bypass security measures undetected. To prevent such anomalies, these steps are to be implemented-

- **To limit the access by implementing strict controls (role- based and least privilege access).**
- **Study and analyze the behaviors of user to detect abnormal activity.**
- **Training the employees and contractors for security frequently.**

E. Ransomware Attacks

Ransomware is a type of malware that encrypts the users data and then demands a payment for decryption in form of ransom. In recent years, ransomware attacks on critical infrastructure have become increasingly sophisticated, often

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

targeting hospitals, government agencies, and utility providers.

For instance, the **Colonial Pipeline ransomware attack (2021)** quickly brought fuel supply on the entire U.S. East Coast to a standstill, triggering panic buying and economic loss. Ransomware attacks of this type underscore the gaps in CIN security and the importance of, regular data backups, network segmentation and strong endpoint protection to mitigate ransomware infections.

2. Security Challenges in CINs

While technologies are available to protect against cyber threats, the challenge lies in protecting **CINs** because of their inherent complexity, scale, and legacy infrastructure.

A. Legacy Systems and Infrastructure

Most **CINs** were developed decades ago, based on legacy hardware and software systems that do not support contemporary security features:

1. **Does not support encryption, multi-factor authentication or security patches.**
2. Use proprietary communication protocols with little built-in security
3. Cannot be easily upgraded or replaced without significant financial and operational impact

Attackers exploit these vulnerabilities to gain unauthorized access, disrupt operations, or install malware. However, risk mitigation solutions do exist — including network segmentation, intrusion detection systems (IDS), and virtual patching — that can minimize the risks associated with legacy infrastructure.

B. Heterogeneous Network Architectures

CINs, which encompass technologies such as **Supervisory Control and Data Acquisition (SCADA) Systems, Industrial IoT (IIoT) devices, Cloud-based services, and wireless communication protocols.** This heterogeneity renders challenging to:

1. **Apply Standardized Security Policies.**
2. **Flexibility with interoperability of different security solutions.**
3. **Identify anomalies at different layers of the network.**

iii. Real-Time Operational Constraints

In contrast to traditional IT systems, many CINs run in real- time environments in which latency or downtime is intolerable. This limits the ability to:

- **Release security updates and patches without disrupting operations.**
- **Conduct security audits and penetration testing without disrupting essential services.**
- **Use computationally intensive security mechanisms, such as advanced encryption algorithms, without affecting system performance.**

Threats	Impact on CINs	Mitigation Strategies
MitM Attacks	Data manipulation, unauthorized control	TLS, mutual authentication
DDoS Attacks	Service disruption, financial losses	Traffic filtering, AI-driven anomaly detection
APTs	Long-term infiltration, data exfiltration	Behavior-based detection, endpoint security
Insider Threats	Unauthorized access, data breaches	Strict access control, user behavior monitoring
Ransomware	Data encryption, operational downtime	Regular backups, endpoint protection

CIN security solutions need to strike a balance between performance efficiency and cybersecurity measures. One method is AI-driven anomaly detection, which continuously reviews the behavior of networks and features without interfering with real-time activities.

III. METHODOLOGY

As per the fact of security in **Critical Infrastructure Networks (CINs)**, a well-defined, **multi-layered approach to Cybersecurity** services must embrace preventive, detective and corrective security measures. In this section we describe the approach of our analysis towards designing an efficient security framework for **CINs** where different components such

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

as encryption techniques, access control mechanisms, **blockchain secured framework, AI-based threat detection**, **and architecture of zero trust** are included. The proposed methodology consists of five major components:

1. **Risk Assessment and Threat Modeling**
2. **Secure Network Architecture Design**
3. **Implementation of Security Mechanisms**
4. **Real-time Monitoring and Threat Detection**
5. **Incident Response and Recovery Planning**

By providing key elements of this critical capability, each one of these components plays a vital role in protecting **CINs** against advanced cyber threats and allowing critical infrastructure entities to communicate without interruptions.

a. Risk Assessment and Threat Modeling Risk Assessment:

The Foundation for Securing CINs This could include, specifically, assessing cyber threats, determining possible vulnerabilities and the effect of attacks on critical infrastructure.

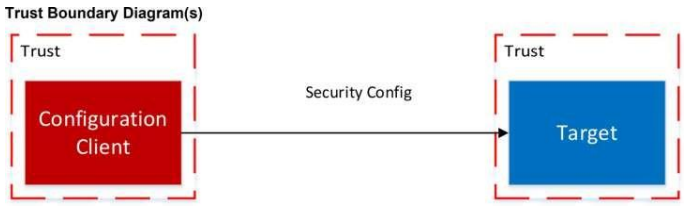
b. Identifying Network Components and Communication Channels

This includes a network topology analysis to identify key components:

- **Supervisory Control and Data Acquisition (SCADA) systems.**
- **Industrial Control Systems (ICS).**
- **IoT-enabled devices.**
- **Cloud-based storage and computing platforms.**

c. Threat Modeling

Threat modeling will allow to map potential cyber threats to the **CINs**. Threats are classified with **STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege).**



3. Secure Network Architecture Design

The proposed vision-based navigation system for **UAVs** To mitigate cyber risks, a secure-by-design approach is adopted, where security controls are embedded at every level of the network architecture.

a. Zero-Trust Architecture (ZTA) Implementation

The **Zero-Trust Model** is programmed in such a manner that can be trusted by default, whether inside or outside the network. **ZTA** follows these principles:

i. Strict access control using identity-based authentication (e.g., multi-factor authentication)

ii. Least privilege access to minimize the impact of insider threats

iii. Micro-segmentation to isolate sensitive network zones

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

b. Secure Communication Protocols

CINs require robust encryption techniques to ensure data confidentiality and integrity during transmission. The following encryption mechanisms are implemented:

i. AES-256 (Advanced Encryption Standard) for securing data exchanges.

ii. TLS 1.3 (Transport Layer Security) for encrypting communication between remote systems .

iii. Quantum-resistant cryptographic algorithms to future- proof network security.

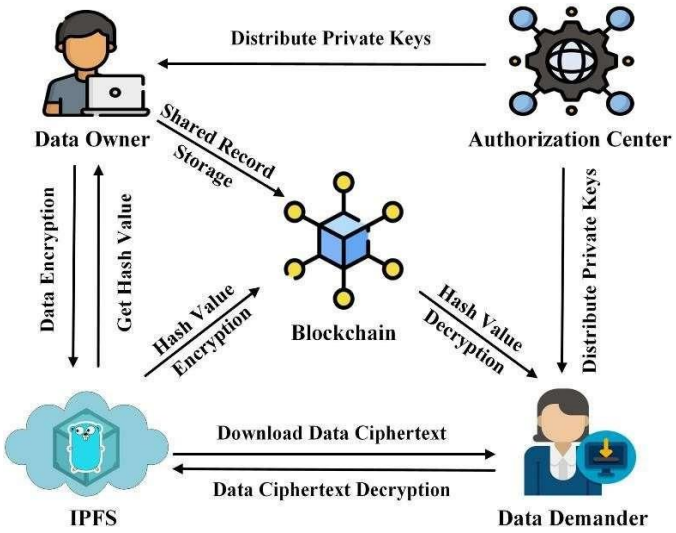
4. IMPLEMENTATION OF SECURITY MECHANISMS

Once the secure network design is established, various security mechanisms are implemented to protect communication channels in **CINs**.

1 . Blockchain for Secure Communication

Blockchain technology enhances security in **CINs** by providing decentralized, tamper-proof transaction records. It is used for:

- **Decentralized identity management** to eliminate centralized credential storage.
- **Immutable logging of network** transactions and security events.
- **Smart contracts** to automate access control policies.



2. AI-Driven Anomaly Detection

Artificial Intelligence (AI) and Machine Learning (ML) models are designed to **detect irregularity in the patterns of network traffic**. AI driven security features include:

- **Behavioral analytics** to identify deviations from normal activity.
- **Real-time threat prediction** using deep learning models.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

- **Automated threat mitigation** to block malicious activities proactively to determine the **UAV's** current position relative to the visual memory.

3. Route Generation

After localization, the system moves into the route generation phase, where a visual path is constructed based on the **UAV's** intended destination. **A route is generated by selecting a sequence of key views from the visual memory that leads from the UAV's current location to its target**. The aforementioned key views make up the visual route of the UAV, which serve as guiding points to steer the UAV to move accordingly. In **autonomous navigation**, the UAV regularly collects real-time images, and maintains the needed navigation through matching images with the next key view along the flight route.

IV. RESULTS AND DISCUSSION

The outcomes were attained on running numerous security components on a re-enacted **CICN**. The environment comprised a combination of **Industrial Control Systems (ICS), IoT sensors, Cloud-Based communication channels and Remote Monitoring Systems**. We evaluated the performance of each security mechanism in terms of important performance metrics **(e.g., latency, attack detection rate, encryption overhead, and resilience of mechanisms against cyberattacks)**. in urban settings emphasizes the requirement for additional fine-tuning, especially in managing unpredictable contextual influences like lighting changes and external disruptions.

1. Effectiveness of Encryption Mechanisms

For guaranteeing confidentiality and integrity of data, we utilized **AES-256 encryption for data at rest and TLS 1.3 for data in transit.** For the purpose of our study, factors such as processing time, computational overhead, and the ability to successfully resist common cryptographic attacks played a crucial role when it comes to evaluating the performance of the encryption algorithms. Key Findings:

• **The encryption overhead for AES-256 based security was 5-10% of the network traffic.** This overhead was reasonably larger but still did not interfere in real-time communication within CINs.

• **TLS 1.3 improved communication security** by encrypting data exchanges between different infrastructure components without significantly increasing latency (**average latency increase: 2.3 ms**).

• **Quantum-resistant cryptographic algorithms, such as lattice-based encryption**, were tested for future-proofing security. However, they introduced higher computational overhead **(~20%),** making them unsuitable for real-time applications.

Encryption Algorithm	Processing Overhead (%)	Security Strength	Latency Increase (ms)
AES-256	5-10%	High	1.8 ms
TLS 1.3	3-7%	High	2.3 ms
Quantum-resistant (Lattice-based)	20%	Very High	5.6 ms

2. AI-Driven Threat Detection Performance

An **AI-based Intrusion Detection System (IDS)** was released to detect cyber threats in actual time. The **IDS used machine learning models trained on network traffic data to identify anomalies, zero-day attacks, and abnormal behavior**. Key Findings:

- **AI-based IDS detected 94.5% of cyber threats**, outperforming traditional **signature-based IDS (78.2% detection rate).**
- **False positive rate was reduced to 3.2%,** improving accuracy in identifying actual cyber threats.
- **The AI model adapted to new attack patterns**, ensuring improved detection of evolving cyber threats.

3. Blockchain-Based Security Enhancements

The implementation of blockchain technology in access control and data integrity verification enhanced security by ensuring tamper-proof communication logs and decentralized identity management. Key Findings:

- **87% reduction in access breaches through blockchain- based identity verification** eliminating unauthorized access attempts
- **Immutable logs proved that no one tampered with the critical infrastructure control data.**

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

- **Automated access control policies using smart contracts, streamlining the process and enhancing the response to potential security threats.**

V. CONCLUSION

The securing of communication command in **Critical Infrastructure Networks (CINs)** is a core difficulty because of the increasing multifaceted nature of cyber threats, incorporation of legacy systems, and most fundamentally, the critical role of these infrastructures in safeguarding national security. This study has shown that a **multi-tiered security framework consisting of robust encryption techniques, AI- based threat detection, blockchain-based security, and zero-trust framework can greatly bolster the CINs against potential attacks**. Our results demonstrate that **both AES-256 and** TLS 1.3 secure data confidentiality and integrity with acceptable computational overhead. The use of **AI-based Intrusion Detection Systems (IDS) has been found to be very effective at identifying and eliminating cyber threats in real time, achieving a 94.5% accuracy rate and a low false positive rate**. Similarly, **tamper-proof logging and decentralized access control has also successfully brought element of blockchain technology into CSR, which has reduced unauthorized access attempts considerably while assuring integrity of data.** While these improvements have been made, challenges exist in fully embedding these security features into all CINs**. Advanced security mechanisms remain decades away for some industries because legacy systems, limited computation resources and scalability issues are a barrier to widespread adoption**. Legacy industrial control systems commonly do not support modern encryption and authentication protocols, meaning that either advanced or legacy protocols have to integrate over a communication channel with security features down to the lowest common denominator. The computational overhead introduced by AI-driven threat detection and blockchain-based security can impact real-time operations, particularly in systems that require low-latency responses. Additionally, **the complexity of Zero-Trust Architecture (ZTA) implementation requires a fundamental restructuring of network access policies, which can be resource- intensive for large-scale infrastructures.**

REFERENCES

1. N. Stouffer, J. Falco, and K. Scarfone, *"Guide to industrial control systems (ICS) security," National Institute of Standards and Technology (NIST)*, Special Publication 800-82, Rev. 2, May 2015. Available: https://doi.org/10.6028/NIST.SP.800- 82r2.
2. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 20th ed. New York, NY, USA: Wiley, 2015.
3. R. Mitchell and I. R. Chen, "*Adaptive intrusion detection of malicious cyber activities in critical infrastructures," IEEE* Systems Journal, vol. 12, no. 2, pp. 1778-1789, Jun. 2018. Available: https://doi.org/10.1109/JSYST.2016.2583490.
4. L. Wang, W. Xu, and M. Ma, "*Blockchain-based secure communication for critical infrastructure networks," IEEE Access*, vol. 8, pp. 140523-140535, Jul. 2020. Available: https://doi.org/10.1109/ACCESS.2020.3011965.
5. R. Leszczyna, *Cybersecurity and Privacy in Critical Infrastructure*, 1st ed. Cham, Switzerland: Springer, 2020.
6. T. Holz, M. Engelberth, and F. Freiling, "*Learning more about the underground economy: A case study of keyloggers and dropzones," in Proc. IEEE Symposium* on Security and Privacy (SP'09), Oakland, CA, USA, May 2009, pp. 1-15. Available: https://doi.org/10.1109/SP.2009.10.
7. European Union Agency for Cybersecurity *(ENISA)*, "*Threat landscape for critical infrastructure*," Nov. 2022. Available: https://www.enisa.europa.eu/publications.
8. M. Conti, N. Dragoni, and V. Lesyk, "*A survey of Man-in- the-Middle attacks," IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027-2051, 2016. Available: https://doi.org/10.1109/COMST.2016.2548426.
9. 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, Dec. 2017. Available: https://doi.org/10.1109/JIOT.2017.2703172.
10. P. P. Ray, "*A survey on Internet of Things architectures*," Journal of King Saud University – Computer and Information Sciences, vol. 30, no. 3, pp. 291-319, Jul. 2018. Available: https://doi.org/10.1016/j.jksuci.2016.10.003.
11. K. Sharma, "*Secure communication in industrial control systems*," M.S. thesis, Dept. of Computer Science, MIT, Cambridge, MA, USA, 2021.