iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VI **Month of publication:** June 2026

DOI: https://doi.org/10.22214/ijraset.2026.83646

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VI June 2026- Available at www.ijraset.com

Forensic Framework for Ransomware in Industrial Internet of Things (IIoT) Systems

Merlin Jyothi M[1], Sankara Narayanan S T[2]
[1]*PG Scholar, Department of Computer Science and Engineering, Dr. M.G.R. Educational and Research Institute, Chennai, India*
[2]*Assistant Professor, Centre of Excellence in Digital Forensics, Chennai, India*

Abstract**: The rapid adoption of the Industrial Internet of Things (IIoT) in critical infrastructure such as manufacturing, energy, healthcare and transportation has significantly improved operational efficiency and automation. However, this increased connectivity has also expanded the attack surface, making IIoT environments highly vulnerable to ransomware attacks. Ransomware incidents in IIoT systems can disrupt processes, cause financial losses, and pose serious safety risks. This project proposes a Forensic Framework for Ransomware in IIoT Systems to support the systematic detection, investigations, and analysis of ransomware attacks in industrial environments. The framework integrates digital forensic principles with IIoT-specific characteristics, including real-time constraints, heterogeneous devices, limited resources, and legacy industrial protocols. It outlines a structured approach consisting of evidence identification, data acquisition, preservation, analysis, and incident reconstruction across multiple IIoT layers such as field devices, gateways, networks, and cloud platforms. The framework enables investigations to collect evidence from network traffic, device logs, memory images, and industrial controllers, followed by detailed analysis to trace infection vectors, encryption mechanisms, and lateral movement within the IIoT ecosystem. By adopting a structured forensic approach, this framework assists incident responders, forensic analysis, and industrial organization in understanding ransomware attacks and improving resilience against future threats.
Keywords: IIoT Forensics, Ransomware, Digital Forensics.

I. INTRODUCTION

A. Background

Industrial Internet of Things (IIoT) Forensics is a specialized domain of digital forensics that focuses on the investigation of cyber incidents occurring within industrial environments. IIoT systems integrate operational technology (OT) with information technology (IT), enabling real-time monitoring, automation, and data-driven decision-making in industrial processes.

Modern industries rely heavily on IIoT components such as sensors, PLCs, Distributed Control Systems (DCS), SCADA servers, edge gateways, and cloud services. While this connectivity improves efficiency and productivity, it also introduces new attack surfaces for cybercriminals. Ransomware attacks targeting IIoT systems can halt production lines, disrupt critical services, and even endanger human lives.

IIoT forensics involves the identification, acquisition, preservation, analysis, and reporting of digital evidence from industrial systems. Unlike traditional IT forensics, IIoT forensics must deal with proprietary protocols, real-time constraints, limited device resources, and safety-critical operations. A structured forensics framework is essential to ensure accurate investigation without affecting industrial continuity.

Workflow
IIoT Environment
↓
Incident Response
↓
Evidence Acquisition
↓
Forensic Analysis
↓
Attack Reconstruction
↓
Forensic Report

B. Wireshark Tool

Wireshark was used in this project for real-time network traffic monitoring and packet-level analysis within the simulated IIoT environment. The tool enabled the capture of incoming and outgoing network packets generated between connected devices. Using Wireshark, suspicious communication patterns such as repeated outbound traffic, abnormal packet frequency, and unusual IP communication were identified and analyzed.

Various filtering techniques were applied to isolate specific protocols, source and destination IP addresses, and suspicious traffic behaviour. The captured packets provided important information such as timestamps, communication sequences, packet size, and protocol details. This analysis helped in identifying anomalies that could indicate ransomware-related activities or unauthorized communication within the network.

C. Autopsy Tool

Autopsy was used as a digital forensic investigation tool for examining and analyzing collected digital evidence related to suspicious system activity. The tool assisted in investigating system artifacts, file information, logs, and other forensic data during the analysis phase of the project. Autopsy provided a structured environment for evidence examination and helped organize forensic data systematically. The tool was used to inspect system-related information and identify traces of suspicious activity that may be associated with ransomware behaviour.

The use of Autopsy also contributed to evidence preservation by maintaining the integrity of collected data during examination. It enabled a systematic approach for forensic analysis and supported attack investigation and reconstruction activities within the proposed framework.

D. Problem Statement

Ransomware attacks in IIoT systems are increasingly sophisticated. Attackers exploit weak authentication, unpatched firmware, insecure remote access, and legacy industrial protocols to gain access to industrial networks. Once inside, ransomware can encrypt critical system files, configuration data, rendering industrial processes inoperable.

The primary challenges include:

- Limited logging and monitoring in IIoT devices
- Difficulty in acquiring live evidence without disrupting operations
- Proprietary hardware and protocols
- Distributed and heterogeneous environments
- Rapid propagation of ransomware across IT-OT networks

Traditional digital forensics techniques designed for IT systems are insufficient for IIoT environments. There is no standardized forensic framework specifically designed for ransomware investigation in IIoT systems.

Hence, the core problem addressed in this project is: The lack of a structured, IIoT-specific forensic framework to investigate ransomware attacks effectively while maintaining operational continuity and forensic integrity.

II. RELATED WORK

A. A State-of-the-Art Review of Ransomware Attacks on Internet of Things [1]

The increase of ransomware targeting the Internet of Things (IoT) is among the most significant challenges in cybersecurity. IoT devices are used extensively in healthcare, manufacturing, and smart structures due to their various functions. Thus, they are attacked because of their known vulnerabilities, such as limited resources, old firmware that has not been updated for years and poor security settings that become attractive targets for today's advanced ransomware attacks. Most importantly, the IoT involves several systems in various technologies, meaning that the controls of one device can compromise several systems, thereby disrupting IoT networks all over the globe.

B. Security Framework for the Internet of Things Applications [2]

The text highlights a comprehensive survey that focuses on all security aspects and challenges facing the Internet of Things systems, including outsourcing techniques for partial computations on edge or cloud while presenting case studies to map security challenges. It further covers three security aspects including Internet of Things device identification and authentication, network traffic intrusion detection, and executable malware files detection.

C. A Review of Internet of Things (IoT) Forensics Frameworks and Models [3]

The abundance of data generated and processed by the ubiquitous number of Internet of Things (IoT) devices around the world is a promising enabler for civil, criminal, and digital investigations. Such data can be used as valuable artefacts to support IoT forensics investigations. This paper provides a survey of IoT forensics models presenting recent advances in the field and identifying opportunities for future research.

D. A Comprehensive Survey of Cybersecurity Threats, Attacks, and Effective Countermeasures in Industrial Internet of Things [4]

This paper presents a comprehensive survey of cybersecurity threats, attacks, vulnerabilities, and countermeasures in Industrial Internet of Things (IIoT) environments. The study examines various vulnerabilities and cyber threats that can compromise the confidentiality, integrity, and availability of IIoT systems. It emphasizes the need for security measures beyond basic encryption to protect industrial infrastructures. Additionally, it evaluates current cybersecurity challenges and identifies effective defense mechanisms for securing IIoT environments.

III. PROPOSED SYSTEM

A. System Overview

The proposed system introduces a Forensic Framework for Ransomware in IIoT Systems that provides a structured and systematic approach to investigating ransomware incidents across industrial environments.

The framework integrates:

- IIoT device forensics
- Network forensics
- Malware analysis
- Incident reconstruction
- Legal and compliance considerations

The framework is designed to operate across IT, OT, edge, and cloud layers, ensuring comprehensive evidence collection and analysis.

B. System Architecture

The proposed system architecture for the forensic framework in IIoT systems is designed to support ransomware detection, forensic investigation, and incident recovery in a structured manner. The architecture integrates network monitoring, evidence handling, forensic analysis, and reporting processes to improve cybersecurity investigation capabilities within industrial environments.

The framework begins with continuous monitoring of network communication within the IIoT environment. Suspicious activities and abnormal traffic patterns are identified through anomaly detection techniques using network analysis tools such as Wireshark. Once suspicious behaviour is detected, the affected system is isolated to prevent further spread of ransomware activity.

Digital evidence including network packets, logs, timestamps, and communication records is then collected and preserved securely for forensic investigation. The collected evidence is analyzed using forensic tools such as Autopsy to identify malicious behaviour, reconstruct attack events, and determine possible indicators of compromise.

Finally, the framework generates investigation reports and supports recovery procedures to restore normal system operations. The architecture provides a systematic workflow for ransomware investigation and improves forensic readiness in IIoT environments.

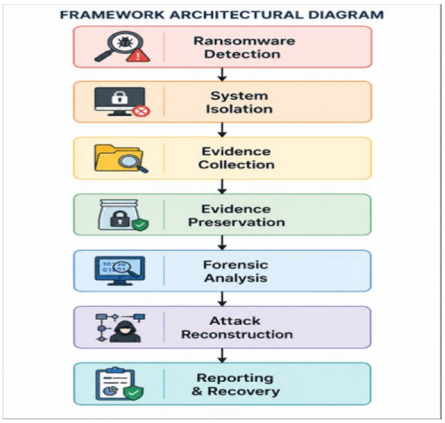


Figure 1. System Architecture

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VI June 2026- Available at www.ijraset.com

IV. METHODOLOGY

A. Environmental Setup

The implementation of the proposed framework was carried out in a controlled and simulated IIoT environment. A personal computer system with standard network connectivity was used to monitor and analyze network traffic. The environment was designed to replicate basic communication behaviour between devices in an IIoT network.

B. Ransomware Detection

The first stage of implementation focused on detecting suspicious activities within the simulated IIoT environment. Network traffic was continuously monitored using Wireshark to capture incoming and outgoing communication between devices. During monitoring, abnormal traffic behaviour such as repeated outbound requests, unusual communication frequency, and unknown IP connections were identified as potential indicators of ransomware activity.

Packet filtering techniques were applied to inspect suspicious protocols, communication patterns, and packet structures. The detection process helped identify deviations from normal network behaviour and triggered further forensic investigation.

C. System Isolation

After identifying suspicious activity, the affected system was logically isolated from the network environment to prevent further spread of the suspected ransomware attack. Isolation was performed to contain the abnormal communication and maintain the integrity of the remaining network systems.

This stage also ensured that forensic evidence was preserved without contamination or modification during the investigation process.

D. Evidence Collection

Digital evidence related to the suspicious activity was collected from both network and system sources. Evidence included captured network packets, IP addresses, timestamps, communication logs, protocol information, and system-related artifacts.

Wireshark was used to collect packet-level evidence, while additional system information was gathered for forensic examination. The collected data was stored securely for further analysis and investigation.

E. Evidence Preservation

The collected evidence was preserved carefully to maintain its integrity and reliability throughout the investigation process. Proper evidence handling procedures were followed to avoid tampering, modification, or accidental loss of data.

The evidence was securely stored and organized to support future forensic analysis and attack reconstruction activities.

F. Forensic Analysis

The forensic analysis stage involved detailed examination of the collected evidence using Autopsy and Wireshark. Packet-level analysis was conducted to inspect suspicious communication behaviour, repeated outbound traffic, and irregular network patterns.

Autopsy was used to analyze system artifacts, logs, metadata, and other digital evidence associated with suspicious activity. Timeline analysis and evidence categorization helped identify traces of malicious behaviour and possible indicators of compromise. The combined use of Wireshark and Autopsy improved the effectiveness of the forensic investigation process.

G. Attack Reconstruction

Attack reconstruction was performed to understand the sequence of events that occurred during the simulated ransomware activity. By analyzing timestamps, packet flow, communication behaviour, and system artifacts, the investigation recreated the progression of suspicious activities within the IIoT environment.

This process helped identify how the abnormal communication originated, how it propagated through the network, and how it affected the system environment.

H. Reporting and Recovery

The final stage involved documenting the findings obtained during the forensic investigation process. Investigation reports were prepared based on the observed anomalies, evidence analysis, and attack reconstruction results.

Recommendations were provided to improve IIoT security, enhance forensic readiness, and reduce future ransomware risks. Recovery procedures were also discussed to restore normal system operation and strengthen incident response capabilities within industrial environments.

V. RESULTS AND DISCUSSION

The implementation of the proposed forensic framework successfully identified suspicious activities within the simulated IIoT environment. Network traffic monitoring and packet analysis revealed several abnormal communication patterns that were inconsistent with normal system behaviour.

Using Wireshark, repeated outbound traffic, unusual communication frequency, and connections to unknown external IP addresses were observed during the anomaly simulation process. Packet analysis showed repetitive communication behaviour and irregular traffic patterns, which were treated as potential indicators of ransomware-related activity.

The framework also supported systematic evidence collection and preservation. Captured network packets, communication logs, timestamps, and protocol information were successfully collected and stored for forensic investigation purposes.

Through forensic analysis using Autopsy, system artifacts and collected evidence were examined to identify suspicious traces associated with abnormal activities and digital evidence such as captured files, logs, and forensic artifacts were verified using SHA-256 hash values to ensure data integrity and authenticity. The hashing process helped confirm that the collected evidence remained unchanged throughout the investigation process and was not modified or tampered with during storage or analysis.

Timeline analysis and evidence categorization helped reconstruct the sequence of events that occurred during the simulated attack scenario. The attack reconstruction process successfully recreated the flow of suspicious communication within the network environment, enabling better understanding of the possible attack behaviour and its impact on the system.

Overall, the proposed framework demonstrated the capability to support ransomware detection, forensic investigation, evidence handling, and attack analysis within a controlled IIoT environment.

TABLE I Comparative Analysis of Traditional and Proposed Forensic Framework for IIoT

Phase	Traditional Forensic Framework	Proposed Forensic Framework for IIoT
Incident Response	Reactive approach with delayed response to cyber incidents	Faster response through anomaly detection and immediate system isolation
Evidence Acquisition	Manual evidence collection with limited automation	Structured evidence acquisition using Wireshark and system monitoring tools
Evidence Integrity	Basic evidence handling procedures	Secure evidence preservation using SHA-256 hashing and forensic preservation techniques
Forensic Analysis	Limited network and system-level investigation	Comprehensive packet-level and artifact analysis using Wireshark and Autopsy
Attack Reconstruction	Partial reconstruction based on available logs	Detailed reconstruction using timestamps, packet flow, and communication behaviour

The comparative analysis highlights the differences between traditional forensic approaches and the proposed forensic framework designed for IIoT environments. Traditional forensic frameworks mainly focus on post-incident investigation and often follow a reactive approach, whereas the proposed framework integrates detection, investigation, and recovery processes into a structured workflow.

In the incident response phase, traditional methods usually depend on manual identification of cyber incidents, which may delay response time. In contrast, the proposed framework improves response efficiency through anomaly detection and immediate system isolation within the IIoT environment.

During evidence acquisition, traditional frameworks often rely on manual collection procedures with limited automation and monitoring capabilities. The proposed framework enhances evidence acquisition by using tools such as Wireshark for packet capture and network traffic monitoring, allowing systematic collection of communication data and suspicious network activity.

The proposed framework also improves evidence integrity through secure preservation methods such as SHA-256 hashing, which ensures that collected evidence remains authentic and unaltered during the investigation process. Traditional approaches may not always include structured integrity verification mechanisms.

In terms of forensic analysis, traditional systems provide limited support for combined network and system-level investigation. The proposed framework integrates Wireshark and Autopsy to perform detailed packet analysis, artifact examination, timeline analysis, and anomaly investigation. Attack reconstruction is more structured in the proposed framework because communication behaviour, timestamps, packet flow, and system artifacts are analyzed together to recreate the sequence of attack events.

V. ADVANTAGES AND LIMITATIONS

A. *Advantages*

- The framework helps identify abnormal communication patterns and suspicious behaviour at an early stage within the IIoT environment, improving cybersecurity monitoring.
- The project combines ransomware detection, evidence collection, forensic analysis, and attack reconstruction into a single structured framework.
- Digital evidence is securely preserved using SHA-256 hashing techniques, ensuring the integrity and authenticity of forensic data during investigation.
- Industry-recognized tools such as Wireshark and Autopsy were used for network traffic monitoring and digital forensic analysis.
- The framework follows a systematic process including detection, isolation, evidence collection, analysis, reporting, and recovery.

B. *Limitations*

- The project was conducted in a simulated IIoT environment, not a real-world deployment.
- The dataset used was limited and may not represent all types of cyberattacks.
- The anomaly detection approach is conceptual and not fully AI-driven.
- Real-time large-scale implementation was not performed.

VI. FUTURE WORK

1) Integration of machine learning algorithms for automated anomaly detection
2) Deployment in real-world IIoT environments
3) Development of a real-time alert and response system
4) Integration with SIEM (Security Information and Event Management) tools
5) Expansion of dataset for improved accuracy and reliability

VII. CONCLUSION

This project presented a framework for anomaly detection and forensic analysis in an Industrial Internet of Things (IIoT) environment. By monitoring network traffic and identifying abnormal communication patterns, the system demonstrated the ability to detect potential security threats at an early stage.

The integration of forensic analysis techniques further strengthened the investigation process by providing insights into suspicious behaviour.

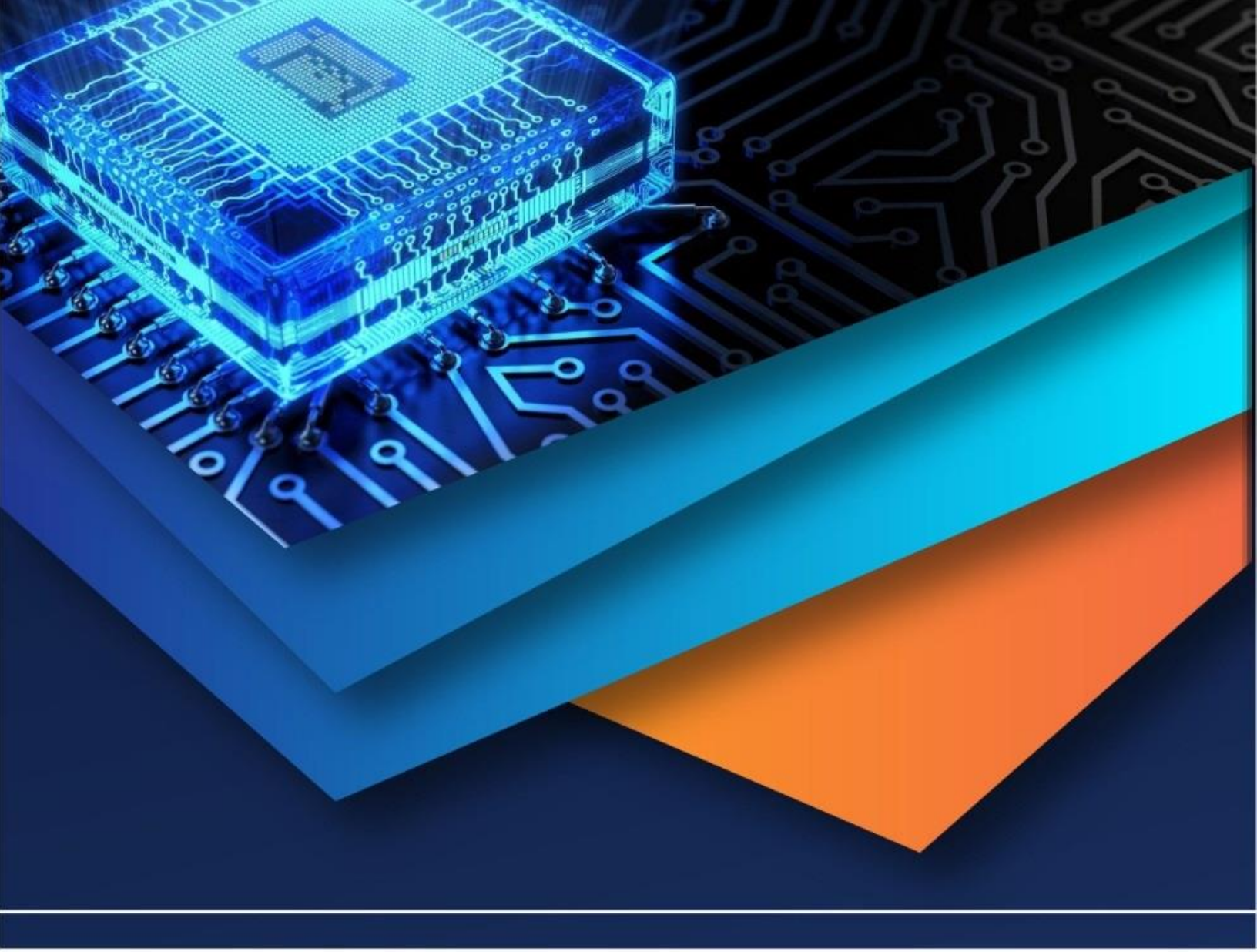
Although the study was conducted in a simulated environment, the results highlight the potential of combining anomaly detection with digital forensics to enhance IIoT security. The proposed approach can serve as a foundation for future research and real-world implementation in securing critical IoT infrastructures.

VIII. ACKNOWLEDGMENT

The authors thank Dr. P. Dinesh Kumar, Head of the Department of Cyber Security, and the management of Dr. M.G.R. Educational and Research Institute for their support. Every target scanned in this project was either under direct author control or scanned with explicit written permission obtained in advance.

REFERENCES

[1] Journal of Information Engineering and Applications. (2019). International Institute for Science, Technology and Education.
[2] Hamad, S. A., Sheng, Q. Z., & Zhang, W. E. (2024). Security framework for the internet of things applications. CRC Press.
[3] Al-Hussaeni, K., Brits, J., Praveen, M., Yaqoob, A., & Karamitsos, I. (2023). A review of internet of things (IoT) forensics frameworks and models. In Lecture Notes in Business Information Processing (pp. 515–533). Springer Nature Switzerland.
[4] Alnajim, A., Habib, S., Islam, M., Thwin, S., & Alotaibi, F. (2023). A comprehensive survey of cybersecurity threats, attacks, and effective countermeasures in Industrial Internet of Things. Technologies, 11(6), 161. https://doi.org/10.3390/technologies11060161
[5] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Academic Press, 3rd Edition, 2011.
[6] W. Stallings, Network Security Essentials: Applications and Standards, Pearson Education, 6th Edition, 2017.
[7] K. Kent, S. Chevalier, T. Grance, and H. Dang, Guide to Integrating Forensic Techniques into Incident Response, NIST Special Publication 800-86, 2006.
[8] Wireshark Foundation, Wireshark User Guide and Documentation, Available online.
[9] Basis Technology, Autopsy Digital Forensics Platform Documentation, Available online.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY