

# **A Digital Forensic Readiness Framework for Ransomware Attacks on Windows-Based Operational Technology in Critical Energy Infrastructure**

**Student : 2428137**

**Name: Rekha Pambala**

## Table of content

|                                             |           |
|---------------------------------------------|-----------|
| <b>Introduction.....</b>                    | <b>2</b>  |
| Context and Background.....                 | 2         |
| Research Problem.....                       | 3         |
| Research Aim and Objectives.....            | 3         |
| Significance of the Research.....           | 4         |
| <b>Literature Review.....</b>               | <b>5</b>  |
| <b>Research Design and Methodology.....</b> | <b>8</b>  |
| Research Design.....                        | 8         |
| Research Methods and Materials.....         | 8         |
| Methods.....                                | 8         |
| <b>Expected Outcomes.....</b>               | <b>9</b>  |
| Anticipated Results.....                    | 9         |
| Implications.....                           | 10        |
| Limitations.....                            | 10        |
| <b>Timeline.....</b>                        | <b>11</b> |
| <b>Conclusion.....</b>                      | <b>12</b> |
| References.....                             | 13        |

# Introduction

## Context and Background

The dependable functioning of the critical energy infrastructure (CEI), comprising power grids, oil refineries and natural gas pipelines, is the keystone of the modern society, the basis of the national security, stable economy and community safety. In the past, the operational technology (OT) systems controlling these physical processes (including supervisory control and data acquisition (SCADA) systems and industrial control systems (ICS)) were in isolated, proprietary networks and operative in an air-gapped setting. The paradigm has changed radically and attained an efficiency, data analytics, remote management quest that has eventually led to the ubiquitous integration of information technology (IT) and OT networks. This has brought in the commercial, windows based systems such as human-machine interfaces (HMIs) and engineering workstations directly to the industrial control layer [1]. Although this convergence has the benefit of providing enormous operational advantages, it has, unwillingly, created and increased the attack surface, practically closing the gap between the corporate network and the physical controls of important industrial processes.

At the same time, the situation in the cyber threat sphere has changed its complex and malicious nature. Initially a widely-applicable tool of digital extortion, ransomware has now grown to be a strategic, planned weapon both in the hands of financially-driven offenders and state-funded agents. These opponents are currently participating in the big game hunting where they carefully choose the high value targets where failure to disrupt will mean a benefit to extortion [2]. The energy industry has become one of the main targets because of the geopolitical role and the direct, significant influence on society of any interference. The practical impact of this threat extends well beyond loss of data, as evidenced by incidents like the Colonial Pipeline attack in 2021 that launched widespread fuel shortages, which are only 2021 in date, and is not limited to effecting the availability of data [3].

It is a critical point in cybersecurity that there is an increased vulnerability of OT systems and advanced ransomware groups target them more specifically. Digital forensics as a domain needed to conduct post-incident investigation, attribution, and recovery is thus placed in an unparalleled scenario as central to the OT domain. Nevertheless, the conventional digital forensic paradigm is essentially a reactive element, which may require system isolation, thorough disk imaging, and lengthy processing which are completely contrary to the OT requirement of continuous, real-time performance in which system availability and safety are paramount [4]. This battle brings out a crisis of intensification: an ever-increasing crisis arises because the tools and methods to comprehend and recover in the aftermath of an attack are often unfeasible to implement in the most vulnerable areas. This, in turn, creates an immediate need to reconsider forensic preparedness to CEI by not only adopting a reactive stance but rather proactive one that is

cognizant of the inherent limitations of OT without sacrificing the evidence required to respond to an incident effectively must be recorded and stored once the incident takes place.

## **Research Problem**

The acute threat notwithstanding, there remains a huge defensive gap. The current paradigms of digital forensic readiness (DFR) and incident response largely apply an extrapolated analogy on information technology (IT) settings and thus is not applicable to operational technology (OT) settings. This is the result of a bottom-line clash: forensic best practices typically require system isolation or large resources, whereas in the context of OT, uninterrupted availability, real-time performance, and operational safety are considered to be of paramount importance [3], [4].

The incompatibility is also worsened by the lack of a strictly theoretically based, standards-based, DFR framework specially formulated to fit the Windows based OT system within the framework of CEI. Consequently, energy infrastructure operators do not have an active, organized roadmap of the collection of forensically viable evidence during a ransomware attack, which negatively affects the investigation of the incident and increases recovery and response time. The study attempts to fill the conceptual gap of proactive forensic preparedness in OT through the following research question: How can a DFR framework be theorized to serve as an effective mechanism of gathering evidence given the special conditions of a ransomware attack on Windows based CEI systems?

## **Research Aim and Objectives**

The main purpose of the research involves developing and conceptually justifying a holistic Digital Forensic Readiness Framework that is explicitly tailored to respond to ransomware attacks against Windows-based OT systems of critical energy infrastructure. The latter objective will be sought by the means of the following specific objectives:

1. To systematically review the current literature, the study summarizes a theoretical framework that provides an explanation of the primary artifacts found in the Windows Registry and volatile memory that reflects ransomware intrusion in operational technology (OT) systems.
2. To outline an overall theoretical design of a digital forensic readiness (DFR) architecture, detailing its modules and logical procedural steps to achieve automated evidence acquisition upon trigger and clearly includes design limitations regarding the OT performance and availability.
3. To develop an abstract model of the inter-relationship within the framework mechanisms, and thus is able to verify the integrity of evidence, and the safe storage of data as well as establish a legally admissible chain of custody.

4. To engages in a theoretical assessment and verification of the framework structure and the working processes of the suggested framework with the provisions and stipulations of the ISO/IEC 27043 standard of incident investigation.
5. To theorizes possible approaches to the problem, within the capability of the framework, to proactively extract ransomware decryption keys in volatile memory, and paves a way to subsequent empirical investigation.

### **Significance of the Research**

This research has triple the importance. To the scholarly community, it adds a new conceptual framework at the meeting point of occupational therapy cybersecurity and digital forensics, thus filling an otherwise well-defined gap in the available literature. It contributes to the theoretical understanding by exploring the adaptation of proactive forensic principles to the high-availability high-safety situations. To practitioners in the industry and operators of CEIs, the study provides a strictly validated standards-compliant blue plan. It provides a practical approach to improving cyber resilience, which could perhaps reduce mean time to recover (MTTR) after an attack and provide the orderly gathering of data that could be the basis of legal action or insurance claims. After all, the social effect is enormous. This research supports the continuity of vital services by contributes to the hardening of the critical energy infrastructure, which protects the citizens of a secure environment and economic stability against the disruptive cyber aggression.

# **Literature Review**

## **Introduction to the Literature Review**

The present review will be based on the recent academic and industrial literature between 2020 and 2025 to build the background context and the urgent need of the proposed study. The analysis is themed to explore the growing ransomware threat to Critical Energy Infrastructure (CEI), the technical vulnerabilities of the technological platform of this assault, the inherent weaknesses of the current investigative methodology, and the conceptual gap the paper attempts to fill. This review establishes the current work as a necessary and immediate reaction to an evident gap in theoretical framework and practical framework on cyber-physical system defense.

## **The Escalating and Targeted Ransomware Threat**

Modern reportages by leading cybersecurity agencies and researchers have consistently described ransomware as an existential threat to national critical infrastructure and thus not being viewed as an opportunity-seeking cyber-crime but an organized, strategically planned wave of attack generally known as a big game hunting [1]. The energy industry is over involved due to the essential role that it plays in the work of society; even temporary and temporary failures in the operation can lead to a chain of economic and safety disasters, which in turn increases the extortion pressure of the adversary. Industry reports supported by hard evidence confirm a sharp rise in attack rate over years with a 2025 forecast showing a 34 per cent rise in attacks on sectors of critical infrastructure, thus highlighting the continuation and acceleration of the threat [2].

Such attacks have been advancing as much as they are being experienced. Attacker organizations are employing more techniques like the doubling extortion where sensitive information is stolen before the system is encrypted and tailoring malware to interfere with or disrupt industrial operations [3]. These attackers methodically bypass the traditional corporate IT security boundaries to attack the operational technology (OT) crown jewels because they understand that the urgency of the services provided in the critical and essential infrastructure (CEI) puts the operators under significant pressure to meet ransom demands in a very short period. It is a strategic development that illustrates the lack of effectiveness of the traditional perimeter-sensitive security architecture and reactive incident-response models in the face of a dedicated and process-conscious adversarial force.

## **Systemic Vulnerability of Windows-Based OT**

The reliance of commercial Windows operating systems in industrial control systems is a documented weakness that is exploitable in CEI. Digital transformation efforts have eroded the historically isolated air-gap that had been between OT networks, creating a dramatically interconnected and expanded attack surface in which IT vulnerabilities have a direct impact on physical process [4]. The legacy OT components such as important Human-Machine interfaces (HMIs) and engineering workstations continue to use out-of-date and unpatronized versions of

Windows, which do not have any modern security patches or embedded defenses, making them highly vulnerable to exploitation when connected to modern network architectures [5].

Furthermore, ransomware has proven itself to have OT-specific skills, which represent an advanced knowledge of the industrial environment. Malware family analyses of the Snake/EKANS indicate the presence of malware codes that will question and end particular SCADA and IC S processes prior to commencing the encryption of files, thus ensuring the highest possible operational disruption [6]. Besides process targeting, the windows registry still remains a key area of forensic investigation. Registry keys are becoming valuable to threat actors as persistence, configuration data, and the ability to execute fileless attack methods, which live in memory, thus bypassing traditional file-scanning security platforms and making post-incident investigations difficult [7]. These results support the need to have a forensic preparedness model that lays committed focus on such stable and unstable data sources.

### **The Inadequacy of Reactive Forensic Models**

The direct implementation of traditional reactive digital forensic techniques in operational technology (OT) situations is the subject of critical analysis in academic and professional literature, which demonstrates a conflict between essential principles. Normal forensic best practices, which were initially designed in the context of information technology (IT) settings, frequently focus on integrity of evidence by taking actions such as immediate system isolation and extensive disk imaging. Such operations require disabling of systems and this is precisely the opposite of what the OT requires of full availability and continuous operation [8]. The empirical researches prove that a notable majority of industries control surroundings cannot be offlined even to have a regular security patching process, and not to mention the long hours or days needed to conduct a complete forensic analysis [5].

It is not only operational philosophy that is technically incompatible. This fundamental vulnerability of most OT systems suggests that the use of active scan tools or traditional IT forensic software agents can inadvertently cause a crash or breakage of the system or dangerous operational conditions, which is likely to cause the very physical safety events that cybersecurity efforts are meant to prevent [9]. Studies that concentrate on forensic acquisition of a device, like Programmable Logic Controllers (PLCs), further highlight the view that traditional approaches are often simply not applicable as they do not have a standardized debugging interface, proprietary communication protocol, or the requirement that realtime control loops be maintained when investigating the device [10]. This body of evidence indicates a pressing necessity of an evidence -collection model that should be developed based on first principles in the limitations of OT settings.

### **The Critical Role of Volatile Memory Forensics**

The spread of so-called fileless malware and sophisticated persistent threats which mainly reside in the Random Access Memory (RAM) of a system have significantly broadened the importance

of volatile memory analysis in modern digital forensics. These attacks have minimal traces on persistent storage unlike conventional malware which captures activity on disk; this means that memory is the key and sometimes the only reliable source of evidence in identification of malicious activity, the explanation of attack vectors, and determination of attacker tools [11]. To incident responders of the Canadian Energy Industries (CEI), the ability to purchase and examine memory in real time, without need of system reboot, which would destroy this volatile information, is an essential facility.

Despite this significance, there is still a significant level of capability gap, especially in the operational technology (OT) contexts. Although there are academic research efforts into memory forensics of a specific industrial controller, including a particular programmable logic controller (PLC) model, these are still confined to individual vendor research and are mostly of a demonstration character [12]. An obvious lack of a unified theoretical basis or a practical benchmark of automated, low impact memory acquisition in the heterogeneous ecosystem of Windows based-OT assets that most energy infrastructure consists of is a deterrent. This gap is a direct contribution to the research goal of theorizing proactive memory evidence gathering mechanisms, which may support retrieval of vital artifacts, such as encryption keys, and reveal malicious in-memory loads.

### **The Gap in Standardized Digital Forensic Readiness**

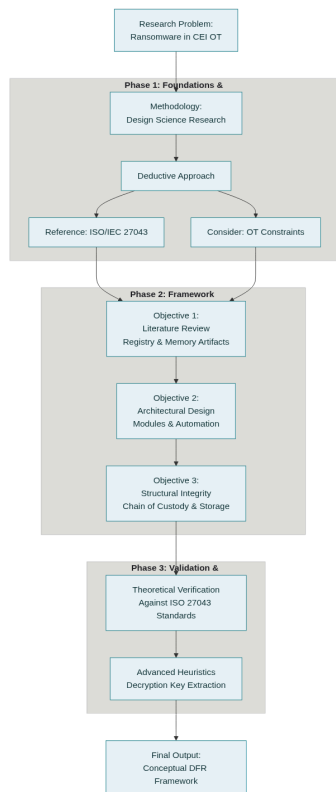
One of the key academic confirmations of the current study will be the established agreement on the lack of a theoretically and practically viable Digital Forensic Readiness (DFR) framework specific to Operational Technology (OT), specifically one in line with the international requirements. As much as standards like ISO/IEC 27043 offer a high level of foundation to incident investigation principles and processes, they are often characterized in the literature as being idealized and generic, and they often omit the proactive preparedness activities as optional and do not offer the specific guidance that OT needs to meet its unique safety and availability goals needed [13]. This gives an interruption between the abstract principle and practical implementation.

In turn, the recent academic efforts to develop DFR notions, as important as they may be, are mostly limited to Information Technology settings, e.g., cloud environments or database systems [14]. These models are not suitable for OT since they lack design constraints to the real-time performance, compatibility with legacy systems and the safety of operation. The absence of forensically ready systems and standard processes is also mentioned repeatedly by experts as one of the biggest setbacks, which forces incident responders to use ad-hoc, reactive responses that often fail to ensure the preservation of admissible evidence or enable quick recovery of vital operations [15], [16].

This is particularly noticeable in such multifaceted, interrelated settings as the Industrial Internet of Things (IIoT), which complicate both the issue of jurisdiction and technical side of digital inquiries even further [4].

# Research Design and Methodology

## Research Design



The current paper is based on the paradigm of Design Science Research (DSR), which is a methodology system developed to conceive, build, and test artefacts that would solve particular organizational issues [20]. The main artefact of this research is the proposed DFR framework which is central to this investigation.

Considering the critical, sensitive and resource-intensive environment of live operational technology (OT) spaces in CEI, a purely theoretical and conceptual query is not only methodologically warranted but also ethically and practically essential. At this stage, physical implementation or empirical validation would be logistically impossible and would have unacceptable risk. In this regard, the study is placed as a background theoretical research, with an emphasis on formulating the framework design, specification, and conceptual validation of the architecture. A deductive approach will be utilized, according to which the specific elements and procedures of the framework will be based on the existing theoretical basis in digital forensics principles that are enshrined in the ISO/IEC 27043 standard and on the specifications that OT cybersecurity requires.

## Research Methods and Materials

### Methods

The study will follow a qualitative and non-empirical approach that will focus on theoretical research and design conceptualization. The primary data will be in the form of current knowledge that will be obtained through academic and industrial literature. The theoretical Analysis and Conceptual Framework Development is the main strategy. The method allows building and testing a new theoretical framework systematically in the absence of primary data gathered on live systems. The main steps in this plan are a Systematic Literature Review (SLR) to develop the artifact model of the design, Conceptual Design to design the framework, Formal Concept



Analysis to approximate the forensic controls model, and Conformance Analysis to provide ISO/IEC 27043 conformity. This multidimensional strategy alleviates the risks of testing with critical infrastructure, and it makes the theoretical background needed to the future application research.

The central output is the theoretical structure of the DFR structure. The design will be informed by the principles of Proactivity, OT-Awareness, and built-in Forensic Soundness. The architecture shall be broken down into logical components such as Lightweight Monitoring Agent, Rule-Based Trigger Engine, performance-throttled Evidence Collector and Integrity and Secure Storage Module. Data flow Diagrams (DFD) and component architecture diagrams will be used to formally model the interactions and the data flows among these components to give a clear and standardised visual representation. Two main approaches will be involved in data analysis and assessment. The literature collected in the SLR will undergo thematic analysis to code data and determine the themes and synthesize Theoretical Artifact Model. The main evaluation tool will be Conformance Analysis that is a strict, clause-by-clause evaluation of the design of the framework against the ISO/IEC 27043 standard with an aim to identify points of coincidence and discrepancy, which will culminate in a formal Conformance Report.

## Materials

The study will solely rely on the secondary data materials in the scholarly publications, industry reports and international standards. There will be no live or simulated systems that will be the primary sources of data. The process of collecting said information is Structured Literature Review or SLR which is performed through the use of digital scholarly databases and search engines like IEEE Xplore, ACM Digital Library, Scopus, etc. This is a reasonable method due to the possibility to synthesize the existing knowledge in a complete form without facing the risk of primary data creation in the background of critical infrastructure, more detail of the material are given in the table.

| Category          | Description / Specification                                                                                        | Justification / Purpose                                                                                                            |
|-------------------|--------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Research Approach | Secondary Data Only<br>Use of scholarly publications, industry reports and international standards.                | Reduces the risk posed by accessing or testing on live critical infrastructure systems which is high.                              |
| Data Source       | Structured Literature Review (SLR)<br>Databases: <i>IEEE Xplore</i> , <i>ACM Digital Library</i> , <i>Scopus</i> . | Provides the opportunity to derive the existing theoretical knowledge into a comprehensive framework without needing primary data. |

|                       |                                                                                                                                                                                                                                                           |                                                                                                                                                |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Software Requirements | <ul style="list-style-type: none"> <li>- Zotero: To organise the references and produce IEEE citations.</li> <li>- Microsoft word: Writing general documentation and thesis.</li> <li>- Lucidchart: Data flow diagrams (DFD) and architecture.</li> </ul> | Basic capabilities of theoretical modeling, documentation and academic formatting; no forensic specialized software is needed.                 |
| Hardware Requirements | Standard Personal Computer<br>Simple computer performance with stable Internet connection..                                                                                                                                                               | The fact that the research is theoretical does not require the use of high-performance computing (HPC), servers, or cloud computing resources. |
| Exclusions            | No Live/Simulated Systems<br>None of the primary data collection in the working environments.                                                                                                                                                             | Eliminates logistical problems and safety issues that come with Operational Technology (OT) testing                                            |

## Expected Outcomes

### Anticipated Results

The main deliverable of this study will be an architectural blueprint of a proactive Digital Forensic Readiness (DFR) Framework specifically tailored to the windows based Operational Technology (OT) ecosystem in Critical Energy Infrastructure (CEI). This blueprint will specify formally the main elements of the framework, including a lightweight monitoring agent, a rule based trigger engine and a forensically viable evidence collector, and their interactions, in more detail, by a series of visual models, such as Data Flow Diagrams (DFDs). This architectural requirement will give a clear conceptual roadmap to convert proactive forensic principles to a formal design that does not violate OT constraints such as the maximum availability and real-time performance requirements.

One of the most crucial deliverables with the blueprint will be an elaborate Conformance Report. The following report will capture the findings of a strict, line by line analysis of mapping the processes and controls of the proposed framework to the demands of ISO/IEC 27043 international standard on incident investigation. This validation will be important evidence of the conceptual nature of the framework and its professional applicability. Moreover, the study will provide a theoretical formulation of the approach of using automated determination of

ransomware decryption keys in volatile memory as an investigative methodology that can be used in the future, offering a prospective research methodology to spur and inform future practical study in the field of forensic recovery.

## **Implications**

The theoretical implication of this study is important, because it provides a new conceptual framework to the overlapping field of OT cybersecurity and digital forensics. The study fulfills an identified gap in the literature by strictly detailing the ways that proactive evidence collection can be built into safety-critical high-availability environments, thus refuting the current reactive paradigm. This contribution serves the contribution to the academic discourse through the introduction of a structured and standards-compatible theory that may be used to guide future empirical research, simulation-based testing, and the creation of new forensic preparedness measurements that can be introduced to industrial controls systems.

Practically and in a professional point of view, the study is an authenticated practical roadmap to industry practitioners, CEI operators, and cybersecurity professionals. This framework presents an ordered approach towards improving the organizational forensic preparedness which may potentially decrease the mean time to recovery (MTTR) after a ransomware attack by making key evidence gathering proactive. Socially, via its role in strengthening critical energy infrastructure, the research advances more general objectives of national resilience and civic security, whereby it assists in protecting vital services against disruptive cyber-aggression that may have economic and social cascades.

## **Limitations**

The main drawback of this study can be attributed to its hypothetical and non-improved design. Although conceptual validity is defined and determined as the architectural blueprint and conformance analysis, it cannot be used to understand the actual performance implication, the efficiency of operations of the forensic triggers and many problems of implementation in the heterogeneous and legacy-filled environments characteristic of CEI. The design of the framework is based on ideal conditions and cannot take into consideration all possible technical interoperability problems or other unexpected interactions with proprietary industrial software that might only manifest itself on physical deployment or in a simulation based test in a controlled laboratory setting.

Moreover, even though compliance with the ISO/IEC 27043 standard acts as a strong proxy in determining validity, the standard does not offer detailed technical advice based on OT, but instead offers high-level concepts. This is to say that the conformance analysis confirms that the framework is going to conform to the general best practices of forensics and investigations, but does not ensure that it is best suited to each individual OT situation. This study explicitly identifies these limitations, and makes the output not a complete solution to the problem, but the

basis theory, and design specification that must be logically developed into on which further applied research, such as the creation of a prototype, sandbox testing, and the analysis of a case study must be established.

## Timeline

The research and writing process for this dissertation will be conducted over a proposed three-month period. The timeline below outlines the major high-level activities and milestones, organized in two-week blocks, to ensure a structured and timely completion.

| Time Period | Major Tasks and Milities                                                                                                                                                                                                                                                      |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Week 1-2    | Primary Research and Scoping. <ul style="list-style-type: none"> <li>● Preliminary research and literature review.</li> <li>● Conclude the scope of the research and the problem statement.</li> <li>● Design the first project plan and frame work.</li> </ul>               |
| Week 3-4    | Swept Literature Review. <ul style="list-style-type: none"> <li>● Systematic search of scholarly databases.</li> <li>● Critically evaluate and synthesize the existing research.</li> <li>● Find major themes and gaps and theory.</li> </ul>                                 |
| Week 5-6    | Design and Development of Frameworks. <ul style="list-style-type: none"> <li>● Design the first framework design and elements.</li> <li>● Define the principles and working processes.</li> <li>● The initial diagrams and conceptual models should be created.</li> </ul>    |
| Week 7-8    | Analysis and Validation <ul style="list-style-type: none"> <li>● Deep analysis of the framework that is proposed.</li> <li>● Carry out conformity checks with the applicable industry standards.</li> <li>● Modify and design the framework according to analysis.</li> </ul> |
| Week 9-10   | Drafting Core Chapters <ul style="list-style-type: none"> <li>● Prepare the introduction and literature review chapters.</li> <li>● Prepare the elaborate methodology and design chapter.</li> <li>● Start to gather results and analysis segments.</li> </ul>                |

|            |                                                                                                                                                                                                                                                           |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Week 11-12 | The Last Compilation and Drafting. <ul style="list-style-type: none"> <li>● Finalize the entire dissertation.</li> <li>● Incorporate all sections, references, and appendices.</li> <li>● Have coherence and logical flow in all the chapters.</li> </ul> |
| Week 13-14 | Final Review and Submission <ul style="list-style-type: none"> <li>● Full-scale proofreading and editing.</li> <li>● The last stage: formatting and compliance check.</li> <li>● Turning in of the final dissertation</li> </ul>                          |

## Conclusion

To sum up, this research proposal is a timely and critical issue that deals with ransomware preparedness in Critical Energy Infrastructure presented as a detailed plan to design and conceptually prove an effective Digital Forensic Readiness Framework. Based on a systematic review of modern literature that validates a real acute threat environment and a lack of OT-specific forensic models, the study is developed on the basis of a strict Design Science Research approach that has the benefit of developing a theoretically sound framework. This study will create a blueprint to be used by future researchers in advancing the academic discourse as well as offer the industry a standards-based, organized strategy to improve investigative preparedness, minimize recovery time and eventually improve the resilience of the most vital energy services to society.

## References

- [1] Dragos Inc., "Dragos Industrial Ransomware Analysis: Q1 2025," Dragos, Hanover, MD, USA, Rep., 2025. [Online]. Available: <https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q1-2025>
- [2] KELA, "Escalating Ransomware Threats to National Security: 2025 Global Analysis," KELA Cyber Intelligence, Tel Aviv, Israel, Rep., 2025.
- [3] Trustwave SpiderLabs, "Ransomware Attacks Against the Energy and Utilities Sector," Trustwave, Chicago, IL, USA, Blog Post, 2025. [Online]. Available: <https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/trustwave-spiderlabs-ransomw-are-attacks-against-the-energy-and-utilities-sector/>
- [4] Resecurity, "Ransomware Attacks against the Energy Sector on the Rise: Nuclear and Oil & Gas are Major Targets," Resecurity, Los Angeles, CA, USA, Rep., 2025.
- [5] Z. Baig, "Digital Forensics and Jurisdictional Challenges for the IIoT," *IEEE Security & Privacy*, vol. 23, no. 2, pp. 45–52, Mar. 2025.
- [6] Microminder CS, "ICS/SCADA Security: A Complete Guide," Microminder Cyber Security, London, UK, Guide, 2025. [Online]. Available: <https://www.micromindercs.com/blog/ics-scada-security>
- [7] Acronis Cyber Protection, "Snake/EKANS Ransomware Attacks Industrial Control Systems," Acronis, Schaffhausen, Switzerland, Blog Post, 2020. [Online]. Available: <https://www.acronis.com/en/blog/posts/snakeekans-ransomware-attacks-industrial-control-systems-acronis-stops-it/>
- [8] Red Canary, "Windows Registry Malware Attacks: Knowledge is the Best Defense," Red Canary, Denver, CO, USA, Blog Post, 2024. [Online]. Available: <https://redcanary.com/blog/threat-detection/windows-registry-attacks-threat-detection/>
- [9] Mechanical Journals, "Tracking Physical-Cyber Failures in Iranian Power Plant Operations," *Int. J. Mech. Tech. Mater. Eng.*, vol. 51, no. 6, pp. 624–630, 2025.
- [10] L. Daubner, "Forensic Experts' View of Forensic-Ready Software Systems," *J. Softw. Maint. Evol., Res. Pract.*, vol. 36, no. 3, pp. 1–15, 2024.
- [11] M. Zubair, U. Tariq, and A. Alghamdi, "Forensic Readiness of Industrial Control Systems Under Availability Constraints," *Forensic Sci. Int. Digit. Investig.*, vol. 42, p. 301402, Sep. 2022.

- [12] F. Yahya, "Memory Forensics: Core of Cyber Investigations Unveiled," Faisal Yahya Cybersecurity, Blog Post, 2025. [Online]. Available: <https://faisalyahya.com/cybersecurity-response/memory-forensics-core-of-cyber-investigations-unveiled/>
- [13] R. N. Rais, S. A. Chaudhry, and M. S. Khan, "Memory Forensic Analysis of a Programmable Logic Controller," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 8, pp. 5678–5690, 2022.
- [14] V. R. Kebande, R. A. Ikuesan, N. M. Karie, and H. S. Venter, "Digital Forensics: Confronting Modern Cyber Crimes," *IEEE Access*, vol. 8, pp. 1–15, 2020.
- [15] A. Albugmi, "Digital Forensics Readiness Framework (DFRF) to Secure Database Systems," *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 2, pp. 13450–13456, Apr. 2024.
- [16] S. Friedl, "IoT Forensics Readiness - Influencing Factors," *Forensic Sci. Int. Rep.*, vol. 9, p. 100345, 2024.
- [17] J. Cortado, "Memory Forensics: Importance of Analyzing Volatile Data," Forensics Weekly Executive Summaries, Univ. of Hawaii West Oahu, 2025. [Online]. Available: <https://westoahu.hawaii.edu/cyber/forensics-weekly-executive-summmaries/memory-forensics-importance-of-analyzing-volatile-data/>
- [18] Z. Baig, "Digital Forensics and Jurisdictional Challenges for the IIoT," *IEEE Security & Privacy*, vol. 23, no. 2, pp. 45–52, Mar. 2025.