Chapter 9
Advancing Ransomware Resilience in Critical Infrastructure

Soumya Roy
https://orcid.org/0009-0000-6594-6049
Brainware University, India

Kaushik Chanda
https://orcid.org/0000-0003-0053-5577
Brainware University, India

Subhadip Nandi
https://orcid.org/0009-0009-8087-3306
Brainware University, India

Anudeepa Gon
Brainware University, India

ABSTRACT

This chapter examines the evolution of ransomware attacks on critical infrastructure by synthesizing research findings from 2018 to 2025. The study systematically reviewed literature and industry reports from databases including Google Scholar, Scopus, IEEE Xplore, and Web of Science using keywords such as "ransomware," "critical infrastructure," "cybersecurity," and "machine learning." Comparative analysis was conducted through tables that illustrate rising incident frequencies, extended downtime, and significant economic impacts—up to a 500% increase in some sectors. Advanced technologies, including AI and ML, are shown to reduce detection and response times by up to 50%. The chapter also identifies emerging tactics such as double extortion and backup encryption, proposes an enhanced risk

DOI: 10.4018/979-8-3373-2282-7.ch009

assessment model integrating dynamic threat intelligence, and outlines recommendations for policy and future research to bridge gaps in legacy system security and adaptive defense measures.

1. INTRODUCTION

The rapid evolution of digital technologies has transformed every aspect of our society, yet it has also led to an unprecedented rise in cyber threats—most notably ransomware attacks targeting critical infrastructure. In the early stages of cybersecurity research, the primary focus was on identifying vulnerabilities in legacy control systems and assessing the disruptive potential of ransomware. Early studies provided a foundational understanding by employing basic risk assessment models, such as:

$Risk = Likelihood \times Impact$

These initial models served as useful tools for quantifying risk; however, they were primarily developed in an era when cyberattacks were less sophisticated and the digital ecosystem was less interconnected.

Over the past several years, significant advancements have been made in mitigating cyber risks. Researchers and practitioners have introduced robust frameworks—such as the NIST Cybersecurity Framework—to provide structured approaches to risk management. Additionally, the adoption of multi-factor authentication (MFA), network segmentation, and continuous monitoring has contributed to the fortification of systems against ransomware. The integration of artificial intelligence (AI) and machine learning (ML) has further revolutionized the field, enabling rapid detection and automated response to cyber incidents, with some studies reporting reductions in response times by as much as 50%. These advancements have collectively improved the resilience of critical infrastructure sectors, including water, power, and emergency response systems.

Despite these strides, recent developments have introduced new challenges that expose critical gaps in the existing body of work. Modern ransomware attacks now incorporate sophisticated tactics such as double extortion—where attackers not only encrypt data but also threaten to leak it—and the targeted encryption of backup systems. Furthermore, the widespread deployment of Internet of Things (IoT) devices and the advent of smart grid technologies have dramatically increased the attack surface, rendering traditional security measures less effective. These emerging threats have not been fully addressed by previous research, which largely focused on traditional IT environments. As a result, there remains a pressing need to re-evaluate existing defence mechanisms in light of these new challenges and to develop advanced strategies that incorporate state-of-the-art technologies.

Security and Privacy Challenges of Deep Learning: A Comprehensive Survey

J. Andrew Onesimu, Karthikeyan J., D. Samuel Joshua Viswasand Robin D. Sebastian (2021). *Research Anthology on Privatizing and Securing Data (pp. 1258-1280).*

www.irma-international.org/chapter/security-and-privacy-challenges-of-deep-learning/280228