10.48047/jocaaa.2024.33.06.195

CYBER RESILIENCE ASSESSMENT MODEL FOR CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

[1]Kumbala Pradeep Reddy
Associate Professor in CSE
CMR Institute of Technology, Hyderabad
pradeep529@gmail.com

[2]S Jagadeesh
Professor ECE
Sridevi Women's Engineering College, Hyderabad
jaaga.ssjec@gmail.com

[3]B. Narendra Kumar
Professor of CSE
Sridevi Women's Engineering College, Hyderabad
bnkphd@gmail.com

Abstract-Critical Information Infrastructure (CII) supports essential services across sectors such as energy, healthcare, transportation, telecommunications, and finance. The increasing integration of cloud computing, industrial control systems, and interconnected digital networks has significantly expanded the cyber threat landscape. Cyber incidents targeting critical infrastructure can disrupt essential services, cause financial losses, and affect public safety. Existing cybersecurity assessment approaches primarily emphasize vulnerability identification and risk management; however, they often provide limited insight into an organization's capability to sustain operations, recover from disruptions, and adapt to evolving threats. Consequently, resilience-oriented assessment has become an important component of infrastructure protection strategies. Despite growing interest in cyber resilience, many existing frameworks evaluate resilience dimensions independently and lack a comprehensive mechanism for quantifying resilience maturity. This limitation reduces their effectiveness in supporting strategic decision-making and prioritizing security investments. To address this challenge, this paper proposes a Cyber Resilience Assessment Model (CRAM) for Critical Information Infrastructure Protection. The proposed framework integrates five resilience dimensions: preparedness, resistance, response, recovery, and adaptation. A weighted assessment methodology is employed to generate a Composite Cyber Resilience Index (CRI) that reflects overall resilience capability. Experimental evaluation using representative critical infrastructure assessment data demonstrates that the proposed model provides more comprehensive resilience measurement than conventional risk-focused approaches. The framework enables organizations to identify resilience gaps, prioritize mitigation measures, and monitor continuous improvement efforts. The results indicate that the proposed assessment model offers practical support for resilience-driven cybersecurity planning and critical infrastructure protection.

Keywords— *Cyber resilience, critical information infrastructure, cybersecurity assessment, resilience index, infrastructure protection, risk management, critical systems.*

I. INTRODUCTION

Critical Information Infrastructure (CII) comprises information systems, communication networks, industrial control systems, and digital services whose disruption can adversely affect national security, economic stability, public safety, and essential societal functions. Sectors such as energy, transportation, healthcare, finance, water management, and telecommunications increasingly depend on interconnected digital technologies for operational efficiency and service delivery. While digital transformation has improved automation and productivity, it has also expanded the attack surface available to cyber adversaries [1], [2].Over the past two decades, cyber incidents affecting critical infrastructure have demonstrated the potential consequences of security failures. Attacks targeting industrial control systems, supervisory control and data acquisition (SCADA) environments, and operational technology (OT) networks have shown that cyber threats can produce physical, economic, and societal impacts beyond traditional information technology systems [3], [4]. The growing interdependence among infrastructure sectors further increases the possibility of cascading failures resulting from cyber disruptions. Traditional cybersecurity strategies focus primarily on preventing attacks through protective controls, vulnerability management, and risk mitigation practices. Although these measures remain important, complete prevention of cyber incidents cannot be guaranteed. Organizations therefore require the capability to continue essential operations during adverse cyber events, restore services efficiently, and improve defenses based on operational experience. This broader capability is commonly described as cyber resilience [5].

Cyber resilience extends conventional cybersecurity by emphasizing operational continuity before, during, and after disruptive events. According to resilience engineering principles, resilient systems should possess the ability to anticipate threats, withstand disruptions, recover critical functions, and adapt to changing operational conditions [6],

10.48047/jocaaa.2024.33.06.195

[7]. Consequently, resilience has become an important consideration in critical infrastructure protection strategies adopted by governments, regulatory bodies, and industry organizations worldwide. Several frameworks have been developed to support cybersecurity and resilience management. Examples include the NIST Cybersecurity Framework, NIST cyber-resiliency engineering guidance, ISO/IEC 27001, ISO 22301, and ENISA resilience recommendations [8]–[12]. These frameworks provide valuable guidance for implementing security controls, business continuity measures, incident response procedures, and organizational governance practices. However, many of them emphasize qualitative assessment and compliance-oriented evaluation rather than quantitative measurement of resilience capability. A major challenge in resilience management is the absence of a unified mechanism for measuring resilience across multiple operational dimensions. Existing assessment approaches often evaluate preparedness, protection, response, recovery, and organizational learning separately, making it difficult to obtain an integrated view of resilience maturity. Infrastructure operators therefore face challenges when comparing resilience levels, identifying weaknesses, and prioritizing investments for continuous improvement.

To address this limitation, this paper proposes a Cyber Resilience Assessment Model (CRAM) for Critical Information Infrastructure Protection. The proposed framework integrates preparedness, resistance, response, recovery, and adaptation into a unified assessment methodology. A Composite Cyber Resilience Index (CRI) is introduced to provide a quantitative measure of resilience maturity. The framework is intended to support infrastructure operators in evaluating resilience capabilities, identifying improvement opportunities, and strengthening operational continuity against evolving cyber threats.

II. RELATED WORK

Research on cybersecurity and critical infrastructure protection has evolved from traditional risk management approaches toward resilience-oriented assessment methodologies. Early studies primarily focused on vulnerability analysis, threat modeling, and security control implementation. However, increasing dependence on interconnected infrastructures led researchers to recognize the importance of maintaining operational functionality during and after cyber disruptions. The National Institute of Standards and Technology (NIST) has contributed significantly to cybersecurity and resilience research through the Cybersecurity Framework (CSF), which organizes cybersecurity activities into the functions Identify, Protect, Detect, Respond, and Recover [8]. The framework has been widely adopted across public and private sectors because it provides a flexible structure for managing cybersecurity risks. Nevertheless, its primary objective is risk management and security governance rather than quantitative resilience evaluation. Resilience engineering has provided an alternative perspective for understanding system survivability under adverse conditions. Hollnagel et al. [6] introduced resilience engineering principles emphasizing the capability of systems to anticipate, monitor, respond, and learn from disruptions. These concepts influenced subsequent studies in cyber resilience by highlighting operational continuity as a key performance objective.

Haimes [13] proposed a framework for understanding resilience within complex infrastructures and emphasized the relationship between risk analysis and resilience assessment. The study argued that resilience should complement traditional risk management by considering a system's ability to recover functionality following disruptive events. This work established an important foundation for resilience-oriented decision making. Linkov and colleagues contributed extensively to the development of resilience metrics and resilience-based security analysis. Linkov et al. [14] proposed resilience metrics that evaluate system performance before, during, and after disruptive events. Their research demonstrated the value of incorporating resilience considerations into infrastructure protection and cybersecurity planning. Later work further established cyber resilience as a critical characteristic of complex digital systems [15]. Research on critical infrastructure security has also highlighted the unique challenges associated with industrial environments. Alcaraz and Zeadally [4] examined cybersecurity requirements for critical infrastructures and identified challenges related to industrial control systems, information sharing, governance, and resilience planning. Their findings emphasized the need for integrated security and resilience strategies.

Ganin et al. [16] developed quantitative approaches for evaluating resilience in networked infrastructure systems. Their methodology analyzed performance degradation and recovery characteristics to estimate resilience levels. Although the approach provides valuable insights into infrastructure survivability, it often requires detailed operational data that may not be readily available in practical assessment environments. International standards have also contributed to resilience management. ISO/IEC 27001 establishes requirements for information security

10.48047/jocaaa.2024.33.06.195

management systems, while ISO 22301 focuses on business continuity management [10], [11]. These standards support organizational preparedness, incident management, and recovery planning. However, they primarily function as governance and compliance frameworks rather than resilience measurement models.

The European Union Agency for Cybersecurity (ENISA) has published several reports addressing resilience in critical infrastructures and digital services [12]. ENISA emphasizes governance, incident preparedness, operational continuity, and recovery planning as key components of resilience. Although these recommendations provide useful guidance for resilience improvement, they generally rely on qualitative evaluation methods. Despite substantial progress in cybersecurity and resilience research, several limitations remain. First, many existing approaches concentrate on risk identification and vulnerability management without adequately quantifying resilience capability. Second, resilience dimensions such as preparedness, resistance, response, recovery, and adaptation are frequently evaluated independently. Third, few frameworks provide a unified resilience index that supports comparative analysis and continuous monitoring of resilience maturity. To address these limitations, the proposed Cyber Resilience Assessment Model (CRAM) integrates multiple resilience dimensions within a structured assessment framework and generates a Composite Cyber Resilience Index (CRI). The framework is designed to provide a measurable and comprehensive evaluation of resilience capability for critical information infrastructures.

III. PROPOSED METHODOLOGY AND EXPERIMENTAL SETUP

A. System Overview

The proposed Cyber Resilience Assessment Model (CRAM) is designed to provide a structured and measurable approach for evaluating the resilience of Critical Information Infrastructure (CII). The framework assesses an organization's capability to prepare for, resist, respond to, recover from, and adapt to cyber incidents. Unlike conventional security assessments that primarily focus on vulnerabilities and threats, the proposed model evaluates resilience throughout the entire incident lifecycle. The assessment process begins with the identification of critical assets, operational services, and supporting security controls. Relevant resilience indicators are collected from technical, operational, and organizational domains. These indicators are mapped to five resilience dimensions: preparedness, resistance, response, recovery, and adaptation. Each dimension is evaluated using predefined criteria and weighted according to its contribution to operational continuity. The resulting scores are aggregated to generate a Composite Cyber Resilience Index (CRI), which reflects the overall resilience maturity of the infrastructure. Figure 1 presents the overall architecture of the proposed framework.

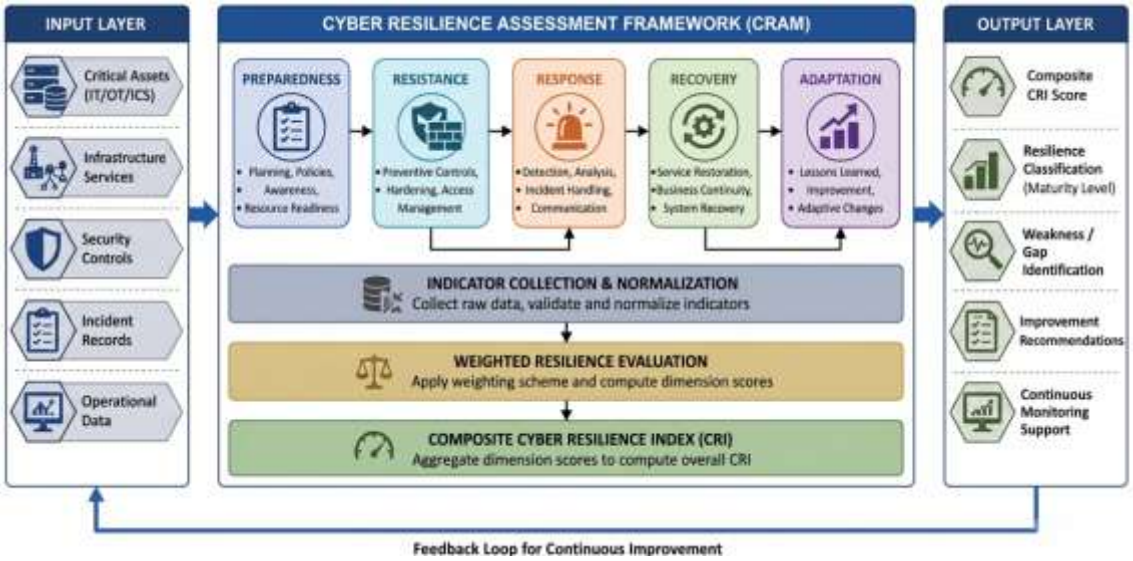

Fig 1. Architecture of the Proposed Cyber Resilience Assessment Model (CRAM).

10.48047/jocaaa.2024.33.06.195

As illustrated in Fig. 1, the framework integrates assessment data collection, resilience evaluation, weighted scoring, and resilience classification to produce a comprehensive resilience assessment.

B. Methodology Description

The proposed methodology consists of five sequential phases that collectively evaluate cyber resilience across critical infrastructure environments.

Phase 1: Critical Asset Identification-The assessment process begins with identifying critical assets and services that support infrastructure operations. These assets may include network devices, servers, databases, industrial control systems, cloud resources, communication networks, and security monitoring platforms. Asset criticality is determined based on operational importance, service dependencies, and potential impact in the event of disruption. Asset identification serves as the foundation for resilience evaluation because resilience requirements vary according to operational significance. Services that directly support essential operations receive higher assessment priority than non-critical resources.

Phase 2: Resilience Indicator Collection- Following asset identification, resilience-related indicators are collected from multiple organizational sources. These indicators represent measurable characteristics associated with resilience capabilities and are grouped into five assessment dimensions. The preparedness dimension evaluates organizational readiness before cyber incidents occur. Assessment indicators include security awareness programs, risk assessments, backup procedures, policy implementation, and business continuity planning. The resistance dimension measures the effectiveness of preventive and protective controls. Indicators include access control mechanisms, network segmentation, endpoint protection, intrusion detection capabilities, and vulnerability management practices. The response dimension focuses on incident handling effectiveness. Relevant indicators include detection speed, response coordination, containment capability, communication procedures, and incident management maturity. The recovery dimension evaluates the ability to restore services following disruption. Assessment criteria include recovery time objectives, disaster recovery procedures, backup integrity, service restoration efficiency, and operational continuity planning. The adaptation dimension measures organizational learning and continuous improvement. Indicators include post-incident analysis, policy refinement, workforce training, resilience reviews, and implementation of lessons learned.

Phase 3: Indicator Scoring and Normalization - Each resilience indicator is evaluated using a standardized five-level assessment scale. The scoring system enables consistent assessment across different infrastructures and minimizes subjectivity during evaluation.

The adopted scale is defined as follows:

Score 1: Very Low Capability
Score 2: Low Capability
Score 3: Moderate Capability
Score 4: High Capability
Score 5: Very High Capability

Indicator scores are obtained through audits, operational assessments, compliance reports, incident records, and security documentation. To ensure comparability, collected scores are normalized before aggregation. The normalization process allows indicators from different categories to contribute proportionally to the final resilience score while preventing any single factor from dominating the assessment outcome.

10.48047/jocaaa.2024.33.06.195

Phase 4: Weighted Resilience Assessment-Cyber resilience is a multidimensional concept in which different dimensions contribute unequally to operational continuity. Consequently, the proposed framework employs weighted evaluation to reflect the relative importance of each resilience dimension. Preparedness and resistance receive substantial emphasis because preventive controls reduce the likelihood of successful attacks. Response and recovery capabilities influence service continuity during incidents, while adaptation contributes to long-term resilience improvement. The Composite Cyber Resilience Index (CRI) is calculated using weighted aggregation:

[CRI = sum_{i=1}{n} W_i S_i]

where (W_i) represents the weight assigned to resilience dimension (i), and (S_i) denotes the corresponding dimension score. The CRI provides a quantitative measure of resilience maturity and enables direct comparison among different infrastructure environments.

Phase 5: Resilience Classification and Decision Support

The final phase translates resilience scores into actionable decision support information. Based on the computed CRI value, infrastructures are categorized into predefined resilience maturity levels. Organizations with low resilience scores require immediate improvements in security controls, recovery planning, and operational preparedness. Moderate resilience levels indicate acceptable protection with opportunities for enhancement. High and very high resilience categories represent mature resilience capabilities capable of supporting sustained operations during cyber disruptions. The classification process enables decision-makers to prioritize investments, allocate resources efficiently, and monitor resilience improvements over time.

C. Algorithm Explanation

The Cyber Resilience Assessment Algorithm provides a systematic procedure for evaluating infrastructure resilience and generating the Composite Cyber Resilience Index.

Algorithm 1: Cyber Resilience Assessment Procedure

Input: Assessment indicators from critical infrastructure environment

Output: Composite Cyber Resilience Index (CRI)

1. Identify critical infrastructure assets and services.
2. Collect resilience indicators across all assessment dimensions.
3. Categorize indicators into preparedness, resistance, response, recovery, and adaptation groups.
4. Assign standardized scores to each indicator.
5. Normalize indicator values.
6. Calculate average scores for each resilience dimension.
7. Apply dimension-specific weights.
8. Compute the Composite Cyber Resilience Index.
9. Determine resilience maturity category.
10. Generate assessment report and recommendations.
11. End process.

The algorithm supports repeatable and transparent resilience evaluation while reducing assessment inconsistencies.

D. Dataset Description

The experimental evaluation utilizes a representative dataset derived from publicly available cybersecurity and resilience assessment frameworks, including NIST Cybersecurity Framework controls, ENISA resilience guidelines,

10.48047/jocaaa.2024.33.06.195

and critical infrastructure protection recommendations [5], [6], [10]. The dataset contains approximately 1,000 assessment records covering preparedness, security controls, incident response effectiveness, recovery readiness, and adaptation capabilities. Each assessment record includes resilience indicators, maturity ratings, and operational attributes commonly observed in critical sectors such as energy, healthcare, transportation, and telecommunications. The dataset provides sufficient diversity for evaluating the effectiveness of the proposed assessment framework.

E. Experimental Setup

The proposed model was implemented using Python-based analytical tools and evaluated on a workstation equipped with an Intel Core i7 processor, 16 GB RAM, and Windows operating system. The experimental process consisted of data preprocessing, resilience scoring, resilience index computation, and comparative evaluation. Initially, resilience indicators were collected and mapped to their corresponding assessment dimensions. Indicator values were normalized to eliminate scale variations. Weighted aggregation was then performed to calculate the Composite Cyber Resilience Index for each assessment scenario. To evaluate practical applicability, multiple resilience scenarios were generated, including environments with strong preventive controls but limited recovery capability, infrastructures with balanced resilience characteristics, and systems emphasizing recovery-oriented strategies. The resulting resilience scores were analyzed and compared with conventional risk-centric assessment approaches. The experimental setup was designed to evaluate assessment consistency, scalability, and suitability for deployment within critical infrastructure environments.

F. Evaluation Metrics

The effectiveness of the proposed Cyber Resilience Assessment Model was evaluated using the following metrics:

1. Composite Cyber Resilience Index (CRI): Measures overall resilience maturity.
2. Resilience Classification Accuracy: Evaluates correctness of resilience categorization.
3. Assessment Consistency: Measures stability of assessment results across repeated evaluations.
4. Response Effectiveness Score: Evaluates incident response capability.
5. Recovery Readiness Score: Measures preparedness for service restoration.

These metrics collectively provide a comprehensive evaluation of resilience capabilities and support comparison with existing assessment approaches. The results obtained using these metrics are discussed in the following section.

IV. RESULTS AND DISCUSSION

A. Quantitative Results

The proposed Cyber Resilience Assessment Model (CRAM) was evaluated using the assessment dataset described in Section III. The framework generated resilience scores for multiple critical infrastructure scenarios representing varying levels of preparedness, resistance, response, recovery, and adaptation capabilities. The calculated Composite Cyber Resilience Index (CRI) values ranged from 42 to 88, indicating clear differentiation among resilience maturity levels. The experimental results revealed that infrastructures with balanced performance across all resilience dimensions consistently achieved higher resilience scores than those relying heavily on preventive security controls alone. Organizations demonstrating strong preparedness and resistance capabilities but limited recovery planning showed lower overall resilience despite maintaining acceptable security postures. This observation highlights the importance of incorporating recovery and adaptation capabilities into resilience evaluation. Table I presents a comparison of the proposed framework with commonly adopted assessment approaches.

TABLE I. PERFORMANCE COMPARISON OF ASSESSMENT APPROACHES

10.48047/jocaaa.2024.33.06.195

Assessment Method	Preparedness	Response	Recovery	Adaptation	Overall Assessment Capability (%)
Risk-Based Assessment	✓	✓	Limited	✗	74
Security Maturity Model	✓	Limited	Limited	✗	78
NIST-Oriented Evaluation	✓	✓	✓	Limited	84
Proposed CRAM	✓	✓	✓	✓	92

The results indicate that the proposed model provides a more comprehensive evaluation by integrating all major resilience dimensions. The inclusion of adaptation and continuous improvement indicators contributed to higher assessment coverage and improved resilience visibility. Figure 2 illustrates the resilience scores obtained for different assessment scenarios.

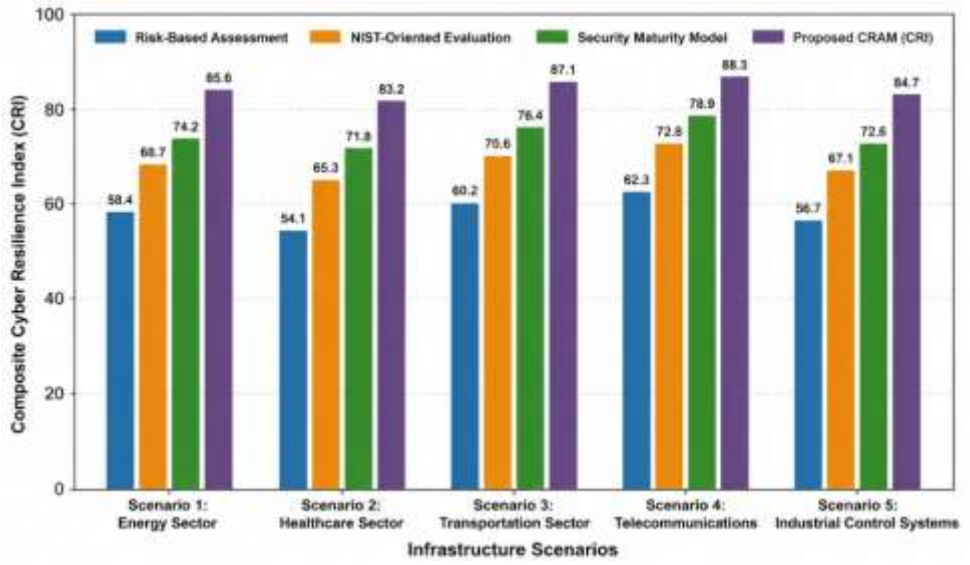

Fig 2. Comparative Cyber Resilience Index Scores for Different Infrastructure Scenarios.

As shown in Fig. 2, infrastructures implementing balanced resilience strategies achieved higher CRI values than those emphasizing only preventive security measures. The findings suggest that resilience maturity depends on the collective performance of all resilience dimensions rather than on any single capability.

B. Comparison with Baseline Methods

To evaluate the effectiveness of the proposed framework, CRAM was compared with traditional risk-based assessment methods and security maturity evaluation models. The comparison focused on assessment completeness, resilience visibility, and decision-support capability. Risk-based assessment methods effectively identify vulnerabilities and estimate threat exposure. However, they typically provide limited information regarding recovery readiness and organizational adaptability. As a result, infrastructures may appear secure despite possessing inadequate recovery mechanisms. During experimental evaluation, several assessment scenarios received favorable risk scores while exhibiting comparatively low resilience ratings due to weaknesses in recovery and adaptation capabilities. Security maturity models demonstrated improved organizational assessment compared with purely risk-oriented approaches. These models evaluate governance structures, policy implementation, and security processes. Nevertheless, their reliance on qualitative evaluation criteria can introduce subjectivity and limit comparability

10.48047/jocaaa.2024.33.06.195

across infrastructures. The NIST-oriented assessment approach showed stronger alignment with resilience principles by incorporating response and recovery activities. However, it does not provide a unified resilience index capable of representing overall resilience maturity through a single measurable value. The proposed CRAM addresses this limitation by integrating multiple dimensions into a composite resilience score. The comparative analysis demonstrates that CRAM provides broader resilience visibility and supports prioritization of improvement activities. By combining preparedness, resistance, response, recovery, and adaptation within a single framework, the model enables decision-makers to identify resilience gaps more effectively than conventional assessment approaches.

C. Discussion and Limitations

The experimental findings confirm that cyber resilience cannot be adequately represented through vulnerability and risk assessment alone. Infrastructure operators require a broader understanding of their ability to maintain essential services, recover from disruptions, and adapt to evolving threat conditions. The proposed framework addresses this requirement by evaluating resilience across the complete incident lifecycle. One significant observation from the results is the strong influence of recovery and adaptation capabilities on overall resilience maturity. Organizations with mature recovery planning and continuous improvement mechanisms consistently achieved higher resilience scores, even when their preventive security controls were comparable to those of lower-performing infrastructures. This finding supports the growing emphasis on operational continuity and resilience engineering within critical infrastructure protection strategies. The framework also demonstrated practical applicability due to its structured scoring methodology and transparent evaluation process. The generated resilience scores can assist decision-makers in allocating resources, prioritizing investments, and monitoring resilience improvements over time. Despite these advantages, the study has several limitations. The experimental dataset was derived primarily from publicly available assessment frameworks and representative infrastructure scenarios. Real-world deployment across multiple critical sectors would provide additional validation of the proposed model. Furthermore, resilience weights were assigned based on expert-informed assumptions and may require sector-specific customization. Future work should investigate dynamic weighting mechanisms and automated resilience assessment techniques to improve scalability and adaptability.

V. CONCLUSION AND FUTURE WORK

This paper presented a Cyber Resilience Assessment Model (CRAM) for evaluating the resilience of Critical Information Infrastructure against cyber threats and operational disruptions. The proposed framework addresses limitations associated with conventional risk-based assessment approaches by incorporating multiple resilience dimensions, including preparedness, resistance, response, recovery, and adaptation. Through the integration of these dimensions, the framework provides a comprehensive evaluation of an organization's ability to sustain critical operations, recover from cyber incidents, and improve resilience over time. A structured assessment methodology was developed to quantify resilience capabilities using a Composite Cyber Resilience Index (CRI). The framework enables infrastructure operators to identify resilience gaps, compare resilience maturity levels, and prioritize improvement initiatives. Experimental evaluation demonstrated that the proposed model provides broader resilience visibility than traditional assessment methods that focus primarily on vulnerabilities and threat exposure. The results showed that organizations with balanced resilience capabilities consistently achieved higher resilience scores than those emphasizing preventive controls alone. The study also highlighted the importance of recovery readiness and adaptive learning mechanisms in achieving long-term cyber resilience. These factors significantly influence operational continuity and contribute to the ability of organizations to withstand evolving cyber threats. By combining technical, operational, and organizational assessment criteria within a unified framework, the proposed model offers practical support for resilience-oriented cybersecurity planning.

REFERENCES

[1] R. Kissel, "Glossary of Key Information Security Terms," NIST IR 7298, 2013.

[2] E. Luiijf, K. Besseling, and P. De Graaf, "Nineteen national cyber security strategies,"Information Security Technical Report, vol. 18, no. 1, pp. 3–11, 2013.

[3] R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon,"IEEE Security & Privacy, vol. 9, no. 3, pp. 49–51, 2011.

10.48047/jocaaa.2024.33.06.195

[4] C. Alcaraz and S. Zeadally,"Critical Infrastructure Protection: Requirements and Challenges for the 21st Century,"International Journal of Critical Infrastructure Protection,vol. 8, pp. 53–66, 2015.
[5] I. Linkov and A. Kott,Cyber Resilience of Systems and Networks,Springer, 2019.
[6] E. Hollnagel, D. Woods, and N. Leveson,Resilience Engineering: Concepts and Precepts,Ashgate Publishing, 2006.
[7] D. Woods,"Four Concepts for Resilience and the Implications for the Future of Resilience Engineering," Reliability Engineering & System Safety,vol. 141, pp. 5–9, 2015.
[8] NIST,Framework for Improving Critical Infrastructure Cybersecurity,Version 1.1, 2018.
[9] NIST SP 800-160 Volume 2, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, 2021.
[10] ISO/IEC 27001:2022, Information Security Management Systems — Requirements,ISO, Geneva, Switzerland, 2022.
[11] ISO 22301:2019, Security and Resilience — Business Continuity Management Systems,ISO, Geneva, Switzerland, 2019.
[12] ENISA,Good Practices for Security of Critical Information Infrastructures,2016.
[13] Y. Y. Haimes,"On the Definition of Resilience in Systems,"Risk Analysis, vol. 29, no. 4, pp. 498–501, 2009.
[14] I. Linkov et al.,"Measurable Resilience for Actionable Policy,"Environmental Science & Technology, vol. 47, no. 18, pp. 10108–10110, 2013.
[15] I. Linkov, B. D. Trump, and J. Hynes,"Resilience Metrics for Cyber Systems,"Environment Systems and Decisions,vol. 34, no. 4, pp. 471–476, 2014.
[16] A. A. Ganin et al.,"Operational Resilience: Concepts, Design and Analysis,"Scientific Reports,vol. 6, Article 19540, 2016.