Jurnal Sistem Informasi Bisnis 04(2025)

On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/81786

Cross sectoral Collaboration in Decision Support Systems for Critical Information Infrastructure Protection: An Innovative Approach

Prasetyo Adi Wibowo Putro*, Satria Tegar Bimantara

Cryptographic Engineering, Politeknik Siber dan Sandi Negara, Bogor, Indonesia

Submitted: November 1th 2025; Reviced: December 19th 2025;
Accepted: December 22th 2025; Available Online:December 29th 2025
DOI: 10.21456/vol15iss4pp525-534

Abstract

The protection of Critical Information Infrastructure (CII) is increasingly challenged by evolving cyber threats and the growing interdependence of digital services, which require coordination beyond traditional, sector-siloed security approaches. This study proposes a Decision Support System (DSS) for CII protection that operationalizes cross-sector collaboration to generate dynamic security recommendations using a connectivity-first selection and a resource/governance similarity fallback when connected references are unavailable. Following the Knowledge Management Systems Development Life Cycle (KMSDLC), the DSS was designed and implemented based on structured interviews with stakeholders responsible for national digital services. The prototype was evaluated using the System Usability Scale (SUS) and achieved a mean score of 78.75 ("Good"), indicating strong user acceptance. The primary contribution is a reproducible, collaboration-enabled DSS mechanism that addresses limitations of static DSS models by supporting adaptive recommendations from structured cross-sector inputs. The study also provides practical implications for multi-stakeholder CIIP governance by clarifying how interdependence and similarity can be used to support auditable security-control recommendations. Future work will focus on outcome-based effectiveness evaluations (e.g., expert agreement and task completion time) and may optionally explore predictive analytics as a separate module; however, the current system remains rule-based and does not implement AI/ML components.

Keywords: Cross sectoral collaboration; Decision support systems; Critical information infrastructure protection; System usability scale; Cybersecurity.

1. Introduction

Challenges in protecting Critical Information Infrastructure (CII) are intensifying as cyber-attacks become more sophisticated and increasingly capable of bypassing conventional security controls (Adepu *et al.,* 2019). In operational technology environments, attacks that target components such as Supervisory Control and Data Acquisition (SCADA) systems demand detection and response capabilities that extend beyond signature-based approaches. This has driven the development of Intrusion Detection Systems (IDS) that incorporate machine learning to improve threat coverage and generalization to emerging attack patterns (Cimova *et al.,* 2022). The risk landscape is further complicated by disinformation campaigns that can distort consumption behavior, disrupt operational decisions, and amplify systemic vulnerabilities, reinforcing the need for robust monitoring and countermeasures across technical and socio-technical layers (Jamalzadeh *et al.,* 2022). Collectively, these trends indicate that CIIP/CIIS decision-making increasingly requires integrated situational awareness and adaptive security responses.

Addressing these interconnected risks calls for cross-sector collaboration (CSC), particularly where infrastructures are interdependent and failures can propagate across organizational boundaries. Evidence from cross-sector research highlights that integrating data and knowledge across institutional silos can improve the comprehensiveness of policy and operational decision-making (Pinto *et al.,* 2023). However, CSC is not simply a technical data-integration exercise; it also demands coordination across multiple institutions, alignment of objectives, and standardized information governance to ensure legitimate and secure data use (Mirzania *et al.,* 2022). From a systems-of-systems viewpoint, growing infrastructure interdependencies increase the complexity and uncertainty of engineering decisions, requiring governance mechanisms that explicitly manage uncertainty and cross-domain effects (Røsok *et al.,* 2023). Prior CSC literature across domains such as disaster management, supply chains, and cross-sector partnerships—also emphasizes that the effectiveness of collaboration depends on network structures, enabling parameters, and the mitigation of unintended consequences (Hu *et al.,* 2022; Luthra *et*

*) Coresponding Author: prasetyo.adi@poltekssn.ac.id

On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/81786

al., 2022; Maiolini *et al.,* 2023). To support a structured synthesis of this diverse body of work, frameworks such as the Consolidated Framework for Collaboration Research (CFCR) consolidate key constructs into domains that can guide systematic analysis and reporting (Calancie *et al.,* 2021). Complementarily, decision sciences have evolved through operations research and the integration of AI in Decision Support Systems (DSS) to better handle uncertainty and complex decision contexts (Lu & Li, 2020), while practical tools for collaboration (e.g., CASPI) demonstrate actionable approaches for strengthening collaboration across service systems (Gupta *et al.,* 2022).

Despite these advances, many DSS frameworks still struggle to keep pace with rapidly evolving cyber threats and to operationalize the integration of complex, heterogeneous, and high-velocity data streams. Traditional DSS models often rely on static data storage and historical cases, yet contemporary environments increasingly require dynamic updating and continuous re-assessment of decision variables (Mehla & Jain, 2021; Oh *et al.,* 2023). In cybersecurity, learning-based approaches such as reinforcement learning and deep learning have been explored to support adaptive decision-making in dynamic environments (Hussen *et al.,* 2023). Similarly, the need to identify cross-platform threats (including Advanced Persistent Threats, APTs) has motivated multi-stream classification approaches that can learn shared representations across different data streams to improve predictive performance (Li *et al.,* 2024). These strands of work collectively underline a key methodological direction: DSS should move from static, single-source reasoning toward adaptive

reasoning over multi-source inputs—while still respecting governance constraints.

Building on this context, the present research targets a critical gap in DSS models for Critical Information Infrastructure Protection (CIIP): many remain sector-isolated and depend on static historical data for security recommendations. Although such isolated approaches can reduce implementation complexity and preserve internal data control, they tend to create a silo effect, limiting the ability to anticipate cascading failures across interconnected infrastructures and constraining cross-domain situational awareness. Moreover, over-reliance on historical patterns can encourage a reactive posture and reduce preparedness against novel threats that do not match prior cases. While earlier studies underscore the value of cross-sector collaboration for cybersecurity, its practical integration into DSS remains constrained by multi-party privacy requirements, coordination frictions, and the absence of standardized governance for timely information exchange. Therefore, this study proposes a DSS that produces dynamic security recommendations by incorporating cross-sector inputs into its reasoning process and applying similarity-based analysis to support more proactive security decision-making.

2. Related Theory

2.1. Intersectoral Collaboration in CIIP

Intersectoral collaboration in CIIP refers to concerted efforts between public and private entities to protect critical information infrastructures from cyber threats (Hernandez-Ardieta *et al.,* 2013; Putro *et al.,* 2024). This collaborative approach is essential for overcoming the 'silo effect' in security management, as it facilitates the sharing of actionable intelligence and the synchronization of defensive strategies across different organizational boundaries (Calancie *et al.,* 2021).This collaboration is deemed essential due to the complexity and global scope of cybersecurity operations, which require coordinated efforts and pooled resources to effectively manage threats (Hernandez-Ardieta *et al.,* 2013). Within a collaborative framework, the exchange of information about threats and security breaches is crucial to enhancing the overall security posture. An effective information exchange model can be exemplified through a game-theoretic framework, where organizations are incentivized to share honestly to maximize mutual benefits and minimize security investments (Douha *et al.,* 2023).

Unlike routine system developments that focus solely on reactive measures, this study adopts the Critical Information Infrastructure Protection (CIIP) framework proposed by Putro (2024). This framework, crafted through intensive consultation with regulators, system owners, users, and academics, emphasizes the importance of synergizing role-based decisions with historical experiences to formulate actions that are not only reactive but also proactive against evolving threats. The primary advantage of this approach lies in its proactive synergy, which uses historical data to anticipate risks rather than merely respond to incidents. Furthermore, its multi-stakeholder design ensures that the system's logic is rigorously aligned with both regulatory requirements and user-centric needs, providing a clear technical distinction from standard application development.

2.2. Decision Support Systems (DSS) in CIIP

Role-based Decision Support Systems (RB-DSS) are designed to provide decision-making support tailored to users' specific roles within an organization. This ensures that relevant information and tools are accessible in accordance with users' responsibilities, thereby enabling effective and efficient decision-making in safeguarding critical information infrastructures (van Delden *et al.,* 2011).

Case-based Decision Support Systems (CB-DSS) use historical data and past incidents to inform current decision-making. By analyzing previous scenarios and outcomes, these systems assist organizations in

On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/81786

developing strategies to address recurring challenges and anticipate future threats, thus enhancing the adaptive capacity in managing CIIP (Johnson *et al.,* 2015).

3. Methodology

This study employs the Knowledge Management Systems Development Life Cycle (KMSDLC) model from Garvin, as elaborated by Rahman(2020), to implement the Critical Information Infrastructure Protection (CIIP) framework proposed by Putro (2024). Furthermore, Rahman(2020) states that this methodology ensures a structured development process for a web-based Decision Support System (DSS), facilitating systematic acquisition, interpretation, and application of knowledge essential for enhancing CIIP. The KMSDLC is used as shown in Figure 1.

The methodology begins with the Acquiring Knowledge phase, in which essential data are collected through structured interviews. Respondents were selected using purposive sampling to ensure the inclusion of key stakeholders with specific expertise and decision-making authority across five distinct critical infrastructure institutions (including the government, telecommunications, and financial sectors). This criterion applies to individuals with at least 5 years of experience in cybersecurity operations or policymaking. The structured interviews were guided by a validated instrument comprising four primary thematic areas: (1) current bottlenecks in intersectoral information sharing, (2) functional requirements for automated recommendation generation from structured inputs (human-in-the-loop), (3) data privacy and trust constraints, and (4) specific performance metrics for evaluating DSS effectiveness. This phase is crucial as it ensures the system's design specifications are grounded in the actual operational challenges and regulatory requirements of CIIP.

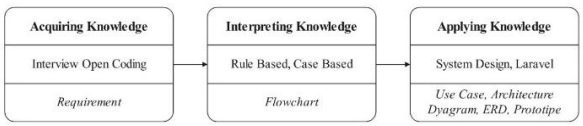

Figure 1. Research Flow

Following data collection, the Interpreting Knowledge phase involves analyzing and organizing the information into a comprehensive flowchart. This flowchart represents the knowledge architecture of the DSS, outlining how different pieces of information interact and integrate within the system. This structured representation is vital for ensuring that the system's design is logical, coherent, and aligned with the users' operational workflows.

The Applying Knowledge phase focuses on translating the designed flowchart into a functional prototype of the web-based DSS. The development of the prototype is guided by insights from earlier phases, ensuring the system is tailored to meet the real-world demands of CIIP. The prototype is built to test the feasibility and effectiveness of the proposed solution in a controlled environment.

Finally, the prototype is subjected to rigorous testing through a pilot study involving six representatives selected from the five initial interviewee institutions. This testing is designed to evaluate the usability and functionality of the DSS using the System Usability Scale (SUS) (Hamid *et al.,* 2020; Marcilly *et al.,* 2023; Reeder *et al.,* 2019). The SUS is a standardized, ten-item Likert scale instrument that provides a reliable, global view of subjective usability assessments. It covers various dimensions, including system complexity, ease of use, and the consistency of the interface. Each respondent's raw score is normalized to produce a single value ranging from 0 to 100 through a specific calculation: odd-numbered items have 1 subtracted from the user score, while even-numbered items have their score subtracted from 5, and the sum is then multiplied by 2.5. A score above 68 is benchmarked as the threshold for 'above average' usability. Feedback from this testing phase is crucial for refining the DSS, ensuring it not only meets functional requirements but is also user-friendly and effective for intersectoral CIIP operations

The current DSS implements a rule-based recommendation mechanism driven by (i) interdependence/connectivity-based selection, (ii) risk-impact refinement when needed, and (iii) a similarity-based fallback using structured indicators (resources and governance). The system does not implement AI/ML models, nor does it use OCR or NLP for automated text extraction or language processing. In this paper, the term automation refers to *automated recommendation generation from structured inputs* within a human-in-the-loop workflow, where authorized stakeholders maintain and validate CIIP data before recommendations are produced.

4. Result

4.1. Acquiring Knowledge

The initial phase of the research involved identifying knowledge, carried out by the researchers and developers of the Decision Support System (DSS) in collaboration with managers of general SPBE (Public Service Governance) applications, such as SP4N LAPOR, Srikandi, and SPSE. Based on interviews conducted at the beginning of the study, several agencies involved in managing these general SPBE applications were identified, including the Presidential Staff Office (KSP), the National Archives of Indonesia (ANRI), and the National Public Procurement Agency (LKPP). The interviewee for the

On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/81786

system needs analysis were the application managers, profiled as shown in Table 1.

Table 1 Interviewees for DSS Analysis

No	Initials	Education	Experience (years)	Position
1	AK	Master's	14	Civil Servant at KSP
2	PU	Master's	19	Civil Servant at ANRI
3	S	Master's	14	Senior Policy Analyst of Digital Procurement Systems LKPP
4	SS	Master's	25	Head of Security for Energy and Natural Resources Directorate, BSSN
5	M	Master's	15	CISO at one of the state-owned banks in Indonesia

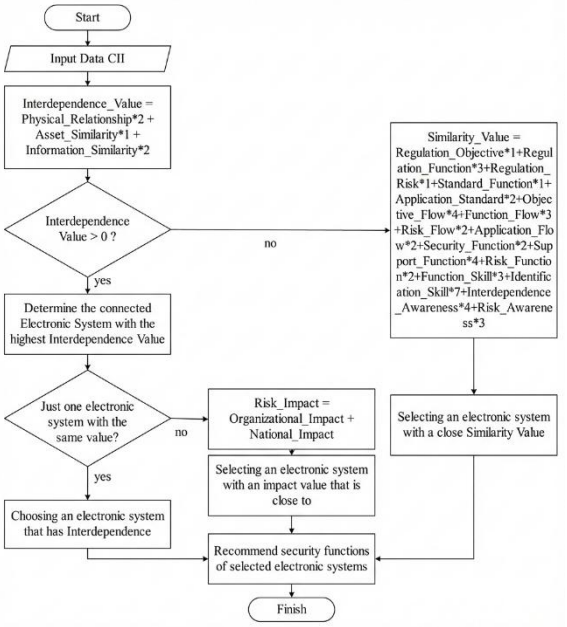

Figure 2. Decision Flow Diagram

The DSS for CIIP is essential to provide exemplary implementations of security measures. As articulated by AK as KSP representative, "*The best practices that we acquire and learn, we endeavor to implement as requirements. These requirements are what we ask developers to fulfill*." This sentiment is echoed by S as representative from LKPP, "*One of the considerations in the security process is exactly this, Sir.*" Technical data from the DSS can also offer system developers insights on how to realize a security standard. This is highlighted by a KSP interviewee, "*For SPBE applications, the key insights in Indonesia come from findings by BSSN. These findings serve as a baseline for developers to align with. It's about aiding developers in creating more secure applications*."

4.2. Interpreting Knowledge

The Decision Support System (DSS) flow revolves around connectivity, as the security of interconnected electronic systems should be equivalent. This concept was highlighted by an interviewee from ANRI, who explained, "*Why is this important? Because the archives in Srikandi that respond to features sending and receiving in whatever form, for example, from BSSN to ANRI, from ANRI to the Ministry of Finance, and from there onwards...*" However, some connected electronic systems may not yet be included in the DSS database, necessitating a case-similarity approach. Case similarity is assessed based on resources and governance considerations. Each indicator is weighed, with proportions derived from the loading factors obtained through PLS SEM testing.

Based on the interview findings, the primary function of the DSS is to request security control recommendations. As depicted in the decision flow diagram in Figure 2, the DSS output is a recommendation for security control for an electronic system that meets the criteria. The initial criterion is connectivity. The DSS searches for the electronic system with the highest connectivity value; however, if multiple systems have equal connectivity values, the system whose risk level is closest to our system will be selected. Similarly, if no connected systems are found, an electronic system with similar resources and governance will be chosen.

The DSS Use Case Diagram is presented in Figure 3. In this DSS, all electronic systems are referred to as CII, but they are ranked by connectivity. Recommendations are selected from the database's electronic system data. Therefore, functions for inputting and editing CII data are essential. To ensure that CII data can only be modified by its owner, proper access rights and user identification or login mechanisms are required.

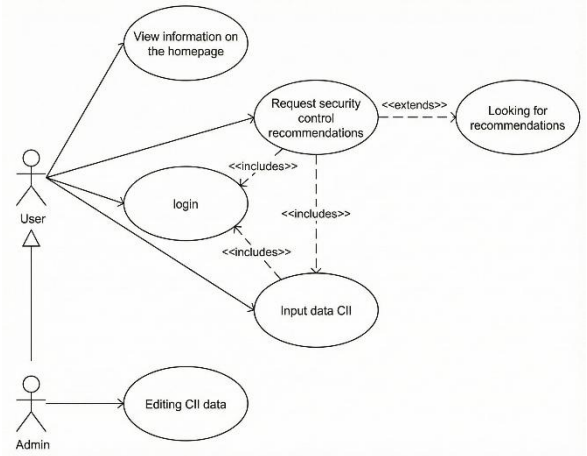

Figure 3. Use Case Diagram

On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/81786

The system encompasses six essential use cases designed to streamline user interactions. First, Use Case Login enables registered users to authenticate using their credentials, granting access to the dashboard. Once logged in, users can request Use Case Security Control Recommendations tailored to their electronic system by providing information on relationships, risks, and governance. The Use Case Input Data IIV use case ensures accurate data collection by prompting users to supply essential details about their systems. These inputs drive the Use Case Search Recommendations functionality, where the system generates tailored security guidance using a rules-based approach or default standards if criteria are unmet. Additionally, users can update their system details via the Use Case Edit Data IIV use case to maintain information accuracy. Lastly, unauthenticated visitors can access the Use Case Homepage to view general system information, facilitating engagement and understanding of the platform. Together, these use cases create a cohesive framework for user-centric operations.

4.3. Applying Knowledge

The Decision Support System (DSS) was implemented using the Laravel framework. In alignment with the Laravel architecture pattern, the DSS architecture adheres to the Model-View-Controller (MVC) design, with layered diagram details as illustrated in Figure 4. A relational database is used to store CII data, organized according to the Entity-Relationship Diagram (ERD) shown in Figure 5. Rules and case calculations for determining recommendations are implemented within the business layer using algorithms depicted in the flow diagram. Furthermore, authentication and access control mechanisms are established to regulate which functions and views users can access. The topmost layer, the presentation layer, is also implemented following the MVC model.

The Decision Support System (DSS) employs a Model-View-Controller (MVC) framework to ensure both scalability and maintainability. Within this architecture, the controller handles data validation and core computations, while session variables manage intermediate results and user-specific interactions. This workflow is exemplified in the 'Looking for Recommendation' use case (Figure 6), where the system processes input and calculates scores using algorithms embedded in the business logic layer. Finally, results are dynamically retrieved from the relational database and rendered through the view layer, delivering a seamless interactive experience.

For testing purposes, the dataset used in the prototype was not synthetically generated. Master data were obtained from institutional system owners, specifically from ANRI, the administrator of Srikandi; LKPP, the administrator of SPSE; and BSSN, the national cybersecurity authority. The master data for these electronic systems was input by designated respondents from each respective institution, guided by the researchers to ensure alignment with the structured CIIP indicators implemented in the DSS.

This guided data entry process was conducted to preserve consistency between institutional master data and the predefined governance, resource, workflow, and interdependency indicators. The objective of the study was not to evaluate data-entry convenience, but to assess the accuracy and relevance of security control recommendations generated for newly analyzed electronic systems. Therefore, preprocessing focused on ensuring completeness and structural conformity of institutional indicators rather than on automated data cleansing or transformation procedures.

The implementation confirms that interdependence is not merely conceptual but operationalized within the recommendation logic. The connectivity-first mechanism ensures structural alignment among interconnected electronic systems, while risk-impact refinement maintains proportional decision-making. When direct interdependence references are unavailable, the similarity-based fallback preserves consistency across governance and resource contexts. This layered selection logic demonstrates how cross-sector collaboration is embedded computationally within the DSS architecture.

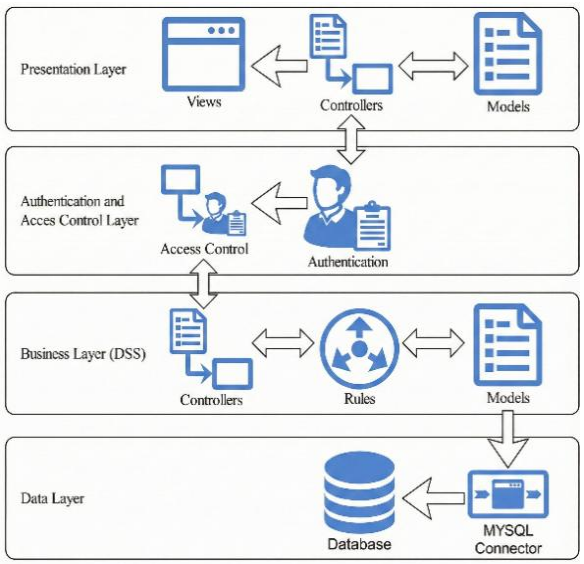

Figure 4. Application Architecture Diagram

On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/81786

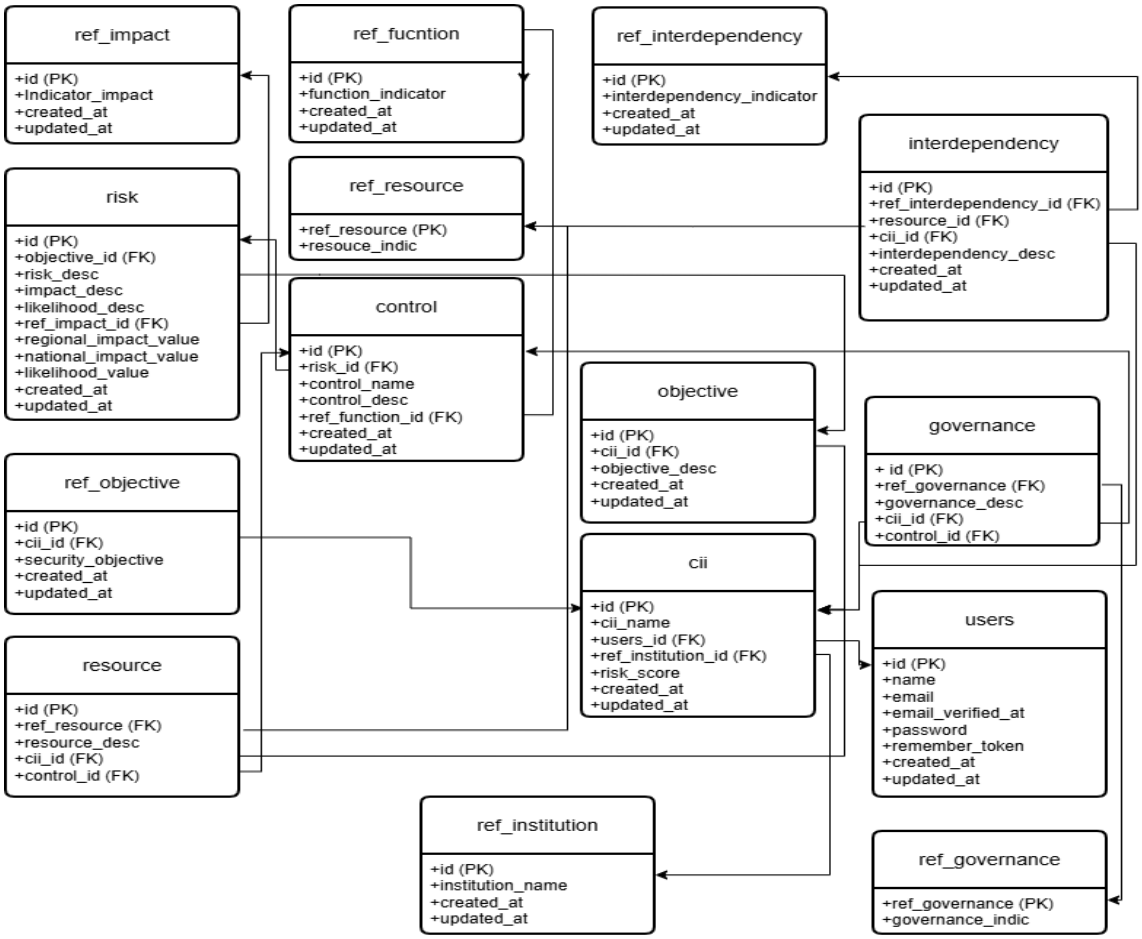

Figure 5. Entity Relationship Diagram

```
// Merge and retrieve similarity values
$similarityValues = $similarityValues1->concat($similarityValues2);

// Check which entry is closest to the total_value
$closestEntry = $similarityValues->sortBy(function ($item) use ($data) {
return abs($item->similarity_score - $data['total_value']);
})->first();

// Retrieve the name of the closest entry
$selectedSystem = collect([$closestEntry->name])->toArray();

$data = [
...session('diagnosis_data'),
'form4' => $data,
'selected_system' => $selectedSystem, ];

// Save data to session and redirect to the results page
session()->put('diagnosis_data', $data);
return to_route('diagnosis.form.result');
```

Figure 6. Source Code Implementation for Use Case Looking for Recommendation

On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/81786

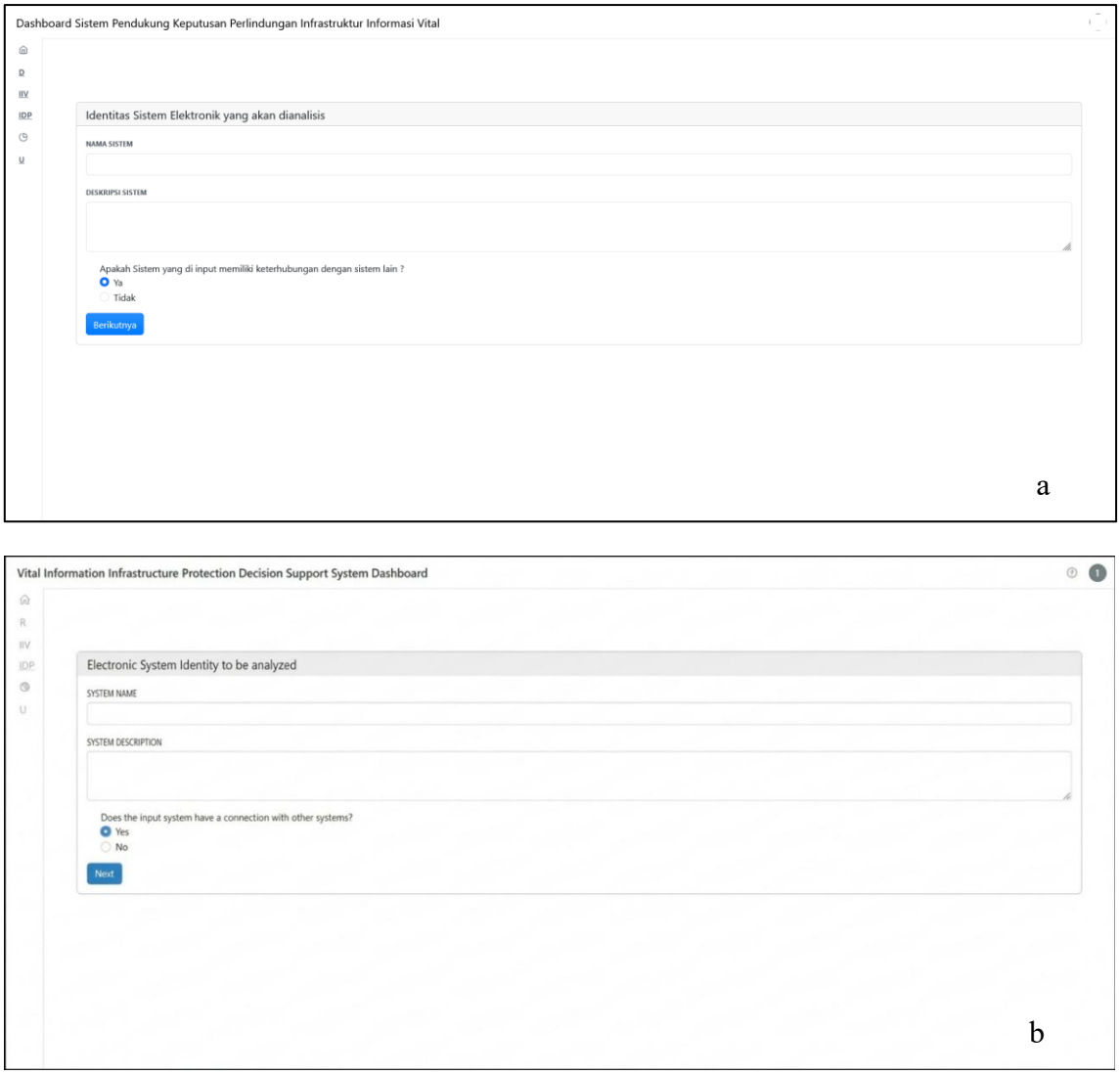

Figure 7. Implementation of bilingual interface in the Vital Information Infrastructure Protection Decision Support System: (a) Indonesian version, (b) English version.

5. Discussion

The testing phase aimed to evaluate the utility of the developed Decision Support System (DSS) and to assess prospective user acceptance using the System Usability Scale (SUS). For the test dataset, additional information from SP4N LAPOR, SPSE, and Srikandi was incorporated, subject to security constraints that restrict data use to what administrators permit. Beyond these three electronic systems, other interconnected systems were included to reflect operational relevance and interdependence within the CIIP context.

Testing involved six respondents (Table 2). Although one respondent had only two years of tenure in their current position, they possessed twelve years of prior experience in information technology. Participants represented multiple government levels (national ministries and city and county agencies). All respondents were prospective DSS users and first-time operators of the prototype. The test was conducted using a deployed instance of the DSS (hosted at http://padiwp.cloud), after which each respondent completed the SUS questionnaire (Brooke, 2020).

SUS scores varied substantially across respondents, ranging from 52.5 to 97.5, with a mean score of 78.75 (Table 3), indicating overall acceptability and a “Good” usability rating. The variability suggests differences in participants’ technical familiarity and highlights challenges in designing an interface that accommodates diverse user backgrounds. Respondent R3 (lowest score) reported difficulties related to navigation and comprehension of technical terms, indicating a need for clearer terminology, improved information architecture, and more structured onboarding. In contrast, Respondent R2 (highest score) emphasized the system’s practical utility and alignment with their technical expertise, implying that the DSS effectively supports domain-

On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/81786

specific needs when users have strong cybersecurity or IT backgrounds. These findings suggest that while the DSS is usable for technical stakeholders, usability and accessibility can be strengthened for non-technical or cross-functional users through role-sensitive guidance, improved help content, and more consistent interface cues.

Respondents also provided actionable feedback for improving core functionality. Suggestions included adding a feature to save evaluation data, making recommendation outputs more technically specific, and expanding the quantity and coverage of system data. These inputs align with the system's original design intent but also reflect practical constraints in CIIP settings, where sharing detailed technical specifications securely across institutions can be difficult. Additionally, one respondent noted the importance of refining interface error handling to prevent users from being exposed to framework-specific developer error messages.

The DSS received a favorable acceptance rating, supporting its feasibility as a coordination and recommendation tool. Consistent with the use case model (Figure 3), the system involves two primary actor roles: admin and user. In the CIIP context, the admin role can be assigned to a central cybersecurity authority, while user roles correspond to organizations that manage CII assets. Rather than introducing new institutional roles, the DSS strengthens existing responsibilities by providing structured mechanisms for coordination, identifying relevant reference systems, and generating security control recommendations.

Table 2. Respondent List for the Questionnaire

Respondent	Institution	Job Role	Tenure (years)	Experience in IT Field (years)
R1	Ministry of Communication and Informatics of the Republic of Indonesia	Technology Utilization Analyst	2	12
R2	City Communication and Informatics Office	Junior Computer Technician	13	17
R3	District Communication and Informatics Office	Junior Expert Computer Technician	18	18
R4	City Communication and Informatics Office	Section Head	12	12
R5	Meteorology, Climatology, and Geophysics Agency	Junior Meteorology and Geophysics Observer	15	10
R6	National Cyber and Crypto Agency	Junior Staff at the Center for Data and Information Communication Technology	17	15

Table 3. SUS Evaluation Data

Respondent	**P 1**	**P 2**	**P 3**	**P 4**	**P 5**	**P 6**	**P 7**	**P 8**	**P 9**	**P 10**	**∑**	**Score**
R1	4	4	3	3	4	4	3	3	4	3	35	87.5
R2	4	4	4	4	4	4	3	4	4	4	39	97.5
R3	2	2	3	1	3	2	3	2	2	1	21	52,5
R4	4	3	3	3	3	4	3	3	3	3	32	80
R5	2	3	3	3	3	3	3	4	3	4	31	77.5
R6	3	3	3	3	3	4	3	3	3	3	31	77.5
Average												78.75

Beyond usability, the findings indicate that the DSS is feasible as a coordination and recommendation tool for CIIP stakeholders. The main practical implications are the need for (i) stronger governance-controlled data maintenance, (ii) clearer technical terminology and onboarding support for non-technical users, and (iii) richer evaluation beyond usability. Future work should therefore validate the usefulness of recommendations through expert assessment and scenario-based testing, and improve the recommendation output format to be more actionable and technically specific. This evaluation does not measure predictive accuracy or computational efficiency, as the DSS operates through a

deterministic rule-based mechanism. Instead, the assessment focuses on operational feasibility, the relevance of recommendations, and user acceptance in realistic CIIP collaboration settings.

Overall, this study contributes by demonstrating how cross-sector collaboration can be operationalized within a DSS framework to generate dynamic CIIP recommendations using interdependence- and risk-guided selection with a similarity-based fallback. The proposed mechanism differs from traditional DSS approaches that rely primarily on static historical data. Practical implications include providing CIIP managers with structured, auditable recommendations supported by multi-source inputs. Future research should prioritize larger-scale evaluations and outcome-based metrics (e.g., expert agreement and task completion time). Predictive analytics may be explored as an optional extension; however, the current DSS remains rule-based and does not implement AI/ML components.

The human-in-the-loop design introduces a trade-off: it increases data maintenance effort but improves accountability and data quality. Efficiency gains are expected mainly in recommendation/coordination once data are available, while scalability depends on standardized templates, access control/audit trails, and periodic data refresh.

6. Conclusion

This study demonstrates how cross-sector collaboration in Critical Information Infrastructure Protection (CIIP) can be translated into a structured and reproducible Decision Support System (DSS) architecture. By operationalizing a connectivity-first selection mechanism refined through risk-impact proximity and supported by a governance–resource similarity fallback, the research embeds interdependence reasoning directly into executable recommendation logic. The SUS evaluation confirms that this rule-based mechanism is operationally feasible and acceptable for multi-institutional use.

Beyond prototype implementation, the contribution of this study lies in formalizing collaboration-oriented CIIP constructs into an auditable and deterministic decision-support procedure. The findings indicate that structured interdependence modeling can support consistent and transparent risk-informed decision-making across institutional boundaries without relying on predictive AI-based automation. By reducing silo-driven blind spots while preserving governance control, the proposed approach strengthens methodological clarity in DSS design for CIIP environments.

Future research should focus on outcome-based evaluation of effectiveness, including expert agreement on recommendations, coverage across heterogeneous system types, and task-completion efficiency under scenario-based testing. Predictive analytics may be explored as an optional extension module; however, such capabilities should be clearly distinguished from the current rule-based architecture and evaluated independently.

References

Adepu, S., Kang, E., & Mathur, A. P., 2019. Challenges in secure engineering of critical infrastructure systems. *Proceedings - 2019 34th IEEE/ACM International Conference on Automated Software Engineering Workshops, ASEW 2019*, *1*, 61–64. https://doi.org/10.1109/ASEW.2019.00030

Brooke, J., 2020. SUS: A “Quick and Dirty” Usability Scale. *Usability Evaluation In Industry*, *November 1995*, 207–212. https://doi.org/10.1201/9781498710411-35

Calancie, L., Frerichs, L., Davis, M. M., Sullivan, E., White, A. M., Cilenti, D., Corbie-Smith, G., & Hassmiller Lich, K., 2021. Consolidated Framework for Collaboration Research derived from a systematic review of theories, models, frameworks and principles for cross-sector collaboration. *PLOS ONE*, *16*(1), e0244501. https://doi.org/10.1371/journal.pone.0244501

Cimova, K., Henderson, D., Allik, M., Brown, D., Meier, P., Mayor, C., Watson, N., Craig, P., & Tweed, E., 2022. Barriers and facilitators of cross-sectoral data linkage to inform healthy public policy and practice: lessons from three case study projects in Scotland. *International Journal of Population Data Science Journal Website*, *7*, 286. https://doi.org/10.23889/ijpds.v7i3.2062

Douha, N. Y. R., Sasabe, M., Taenaka, Y., & Kadobayashi, Y., 2023. An Evolutionary Game Theoretic Analysis of Cybersecurity Investment Strategies for Smart-Home Users against Cyberattacks. *Applied Sciences (Switzerland)*, *13*(7). https://doi.org/10.3390/app13074645

Gupta, S., Modgil, S., Bhattacharyya, S., & Bose, I., 2022. Artificial intelligence for decision support systems in the field of operations research: review and future scope of research. *Annals of Operations Research*, *308*(1–2), 215–274. https://doi.org/10.1007/s10479-020-03856-6

Hamid, S., Bawany, N. Z., & Zahoor, K., 2020. Assessing ecommerce websites: Usability and accessibility study. *2020 International Conference on Advanced Computer Science and Information Systems, ICACSIS 2020*, 199–204. https://doi.org/10.1109/ICACSIS51025.2020.9263162

Hernandez-Ardieta, J. L., Tapiador, J. E., & Suarez-Tangil, G., 2013. Information sharing models for cooperative cyber defence. *International Conference on Cyber Conflict, CYCON*, 1–28.

Hu, Z., Wu, G., Wu, H., & Zhang, L., 2022. Urban Climate Cross-sectoral preparedness and

mitigation for networked typhoon disasters with cascading effects. *Urban Climate*, *42*(February), 101140. https://doi.org/10.1016/j.uclim.2022.101140

Hussen, N., Elghamrawy, S. M., Salem, M., & El-Desouky, A. I., 2023. A Fully Streaming Big Data Framework for Cyber Security Based on Optimized Deep Learning Algorithm. *IEEE Access*, *11*(June), 65675–65688. https://doi.org/10.1109/ACCESS.2023.3281893

Jamalzadeh, S., Barker, K., González, A. D., & Radhakrishnan, S., 2022. Protecting infrastructure performance from disinformation attacks. *Scientific Reports*, *12*(1), 12707. https://doi.org/10.1038/s41598-022-16832-w

Johnson, G., Whittington, R., Scholes, K., Angwin, D., & Regnér, P., 2015. *Fundamentals of Strategy third edition*.

Li, Y.-F., Gao, Y., Ayoade, G., Khan, L., Singhal, A., & Thuraisingham, B., 2024. Heterogeneous Domain Adaptation for Multistream Classification on Cyber Threat Data. *IEEE Transactions on Dependable and Secure Computing*, *21*(1), 1–11. https://doi.org/10.1109/TDSC.2022.3181682

Lu, Y., & Li, Y., 2020. Cross-sector collaboration in times of crisis: findings from a study of the Funing tornado in China. *Local Government Studies*, *46*(3), 459–482. https://doi.org/10.1080/03003930.2019.1677626

Luthra, S., Sharma, M., Kumar, A., Joshi, S., Collins, E., & Mangla, S., 2022. Overcoming barriers to cross-sector collaboration in circular supply chain management: a multi-method approach. *Transportation Research Part E: Logistics and Transportation Review*, *157*, May 2021, 102582. https://doi.org/10.1016/j.tre.2021.102582

Maiolini, R., Versari, P., Rullani, F., & Seitanidi, M. M., 2023. The Role of Community Participation in Cross-Sector Social Partnerships. *Nonprofit and Voluntary Sector Quarterly*, *52*(5), 1386–1412. https://doi.org/10.1177/08997640221130696

Marcilly, R., Zheng, W. Y., Quindroit, P., Pelayo, S., Berdot, S., Charpiat, B., Corny, J., Drouot, S., Frery, P., Leguelinel-Blache, G., Mondet, L., Potier, A., Robert, L., Ferret, L., & Baysari, M., 2023. Comparison of the validity, perceived usefulness, and usability of I-MeDeSA and TEMAS, two tools to evaluate alert system usability. *International Journal of Medical Informatics*, *175*(May 2023), 105091. https://doi.org/10.1016/j.ijmedinf.2023.105091

Mehla, S., & Jain, S., 2021. Development and evaluation of knowledge treasure for emergency situation awareness. *International Journal of Computers and Applications*, *43*(5), 483–493. https://doi.org/10.1080/1206212X.2019.1574950

Mirzania, M., Shakibazadeh, E., & Ashoorkhani, M., 2022. Challenges for implementation of inter-sectoral efforts to improve outbreak response using consolidated framework for implementation research; Iran's COVID-19 experience. *BMC Health Services Research*, *22*(1), 1–10. https://doi.org/10.1186/s12913-022-08510-4

Oh, S. H., Jeong, M. K., Kim, H. C., & Park, J., 2023. Applying Reinforcement Learning for Enhanced Cybersecurity against Adversarial Simulation. *Sensors*, *23*(6). https://doi.org/10.3390/s23063000

Pinto, A., Herrera, L. C., Donoso, Y., & Gutierrez, J. A., 2023. Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure. *Sensors*, *23*(5), 1–18. https://doi.org/10.3390/s23052415

Putro, P. A. W., Sensuse, D. I., & Wibowo, W. S. S., 2024. Framework for critical information infrastructure protection in smart government: a case study in Indonesia. *Information & Computer Security*, *32*(1), 112–129. https://doi.org/10.1108/ICS-03-2023-0031

Rahman, A. A., & Selwyn, J., 2020. A novel approach to design quality model for knowledge management systems. *International Journal of Scientific and Technology Research*, *9*(2), 872–877.

Reeder, B., Drake, C., Ozkaynak, M., & Wald, H. L., 2019. Usability testing of a mobile clinical decision support app for urinary tract infection diagnosis in nursing homes. *Journal of Gerontological Nursing*, *47*(7), 11–17. https://doi.org/10.3928/00989134-20190408-01

Røsok, O. P., de Bruijne, M. L. C., & Veeneman, W. W., 2023. Dealing with Cross-Sectoral Uncertainty: A Case Study on Governing Uncertainty for Infrastructures in Transition. *Sustainability (Switzerland)*, *15*(4). https://doi.org/10.3390/su15043750

van Delden, H., van Vliet, J., Rutledge, D. T., & Kirkby, M. J., 2011. Comparison of scale and scaling issues in integrated land-use models for policy support. *Agriculture, Ecosystems and Environment*, *142*(1–2), 18–28. https://doi.org/10.1016/j.agee.2011.03.005