ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED

Technical Research Center

Paper Title Here

Research Paper: ISAU-RP-9XX-202X-XYZ (issued by ISAU)

Author Full Name or Task Group #
Author Date Here

An ISAUnited.org Published Research Paper
Institute of Security Architecture United (ISAUnited.org)

Author or Task Group Number:
Author Full Name or ISAU-TGXX-202X

Publishing Reviewer(s):
ISAUnited Master Fellow Committee
Affiliation: ISAUnited.org

Authored Date:
[Add here]

Publication Date:
[Add here]

Document Reference Number:
ISAU-RP-9XX-202X-XYZ
Assigned by the Institute Document Management Register

Abstract

- *Provide a high-level overview of the research paper.*
- *Summarize the key problems, objectives, and conclusions.*
- *Highlight critical takeaways for executives and decision-makers.*

Key words: Add here…

Contents

Paper Title Here

ISAUnited Technical Research Template

NOTE: Citation & References Requirement (Policy ISAU-POL-45)

All submissions to the ISAUnited Research Center Reports library must include embedded in-text citations and a complete References section in either APA (7th ed.) or IEEE format, used consistently throughout the manuscript. Cite every non-original claim, standard, figure, and table at the point of use (APA author–date or IEEE numeric brackets), and provide full reference metadata (author/organization, year, title, version/identifier, and DOI or stable URL). Submissions lacking embedded citations, a matching References list, or using mixed/placeholder styles will be returned to authors for correction before review.

NOTE: Whitepaper vs Research Paper (ISAU TRC Submission Guidance)

In the technical and academic writing community, a whitepaper and a research paper serve different purposes and therefore carry different expectations.

- A whitepaper is a practitioner-focused document that explains a problem, analyzes technical options, proposes a defensible solution, or provides architectural guidance, supported by evidence, diagrams, and engineering reasoning. It emphasizes clarity, applicability, and actionable insight rather than original scientific discovery.
- By contrast, a research paper adheres to formal academic research conventions and contributes new knowledge, including original hypotheses, structured methodologies, data collection, analysis, comparative evaluation, and peer-verifiable findings. Research papers follow established scholarly standards (problem statement, literature review, methodology, results, and discussion), while whitepapers follow technical-industry standards (problem framing, architecture analysis, solution design, and engineering validation).
- ISAU accepts both forms; however, submitters must accurately classify their work. If a submission does not include original research methodology or new empirical findings, it is considered a white paper, not a research paper. This distinction ensures integrity, precision, and consistency across all ISAU publications.

1. Introduction

- *Introduce the topic and its relevance to cybersecurity, security architecture, or security engineering.*
- *Define key concepts and objectives of the whitepaper.*
- *Mention any research methodology used (if applicable).*

2. Problem Statement

- *Clearly define the cybersecurity challenge, risk, or gap being addressed.*
- *Provide supporting data, statistics, or real-world examples.*
- *Explain why this issue is critical for organizations.*

3. Technical Analysis and Risk Evaluation

3.1 Technical Engineering and Design Analysis

This section outlines technical design principles, security controls, and engineering considerations for the topic under discussion. It should include architecture diagrams, risk assessments, and implementation best practices.

3.2 Technical Adversarial and Defensible Analysis (TADA)

- *Conduct structured adversarial analysis and defensible architecture validation.*
- *Identify potential attack vectors and evaluate mitigation strategies.*
- *Apply real-world adversarial models to test security resilience.*
- *Assess the risks, vulnerabilities, and attack vectors related to the topic.*
- *Use technical diagrams, threat models, or attack trees where necessary.*
- *Ensure defensive mechanisms align with ISAUnited Defensible Standards.*

4. Technical Mathematical Computation

- *Use mathematical modeling and quantitative analysis to assess security threats.*
- *Provide algorithmic approaches for risk measurement and mitigation.*
- *Apply numerical computations to validate security controls and architectural robustness.*

5. Proposed Solutions, Recommendations, and Methodologies

- *Present clear, actionable solutions to address the problem.*
- *Provide implementation guidance for security architects and engineers.*
- *Discuss potential challenges in adopting the proposed solutions.*

5.1 Case Studies

Documented examples of cybersecurity principles, methodologies, or frameworks applied in real-world situations. They often involve:

- *A detailed analysis of a single company or project.*
- *A deep dive into what worked, what did not, and key takeaways.*
- *Quantifiable results and lessons learned from implementation.*

5.2 Industry Scenarios

Broaden the perspective, exploring trends, challenges, and strategies across multiple industries. This section helps:

- *Identify sector-specific security challenges (e.g., finance vs. healthcare vs. cloud security).*
- *Discuss common adversarial tactics and defense strategies observed across industries.*
- *Provide emerging trends that influence cybersecurity engineering and architecture.*

6. Conclusion and Future Considerations

- *Summarize key findings.*
- *Highlight future developments, research needs, or improvements.*
- *Encourage further discussion within the industry.*

References

- *Refer to the embedded citations in the text above, numbered and identified in IEEE format such as [1], [2], [3], etc. or APA format.*

Appendix

Appendices & Supporting Documents

- *Include additional technical data, extended research, or supplementary materials.*

End of Document

IO