ISSN(O): 2320-5407 | ISSN(P): 3107-4928

International Journal of Advanced Research

Publisher's Name: Jana Publication and Research LLP

www.journalijar.com

REVIEWER'S REPORT

Manuscript No.: **IJAR-58683**

Title: Toward SDN-Native Cybersecurity: Unified Threat Modeling, Formal Assurance, Behavioral Detection, and Multi-Controller Resilience.

Recommendation:
Accept as it is .....
Accept after minor revision.....
Accept after major revision ...✓.....
Do not accept (*Reasons below*) .....

Rating	Excel.	Good	Fair	Poor
Originality		✓		
Techn. Quality		✓		
Clarity			✓	
Significance			✓	

Reviewer's ID: JPR- **098**

Detailed Reviewer's Report

Decision: Accept after Major Revision

Major Comments

1. **Strengthen empirical validation.**
   The manuscript relies primarily on analytical evaluation, attack-path walkthroughs, requirement coverage, and failure-mode analysis. The authors should provide at least a small reproducible prototype or cyber-range evaluation to demonstrate that the proposed integrated framework can operate in practice. The paper itself identifies detection delay, CPU overhead, verifier latency, bypass resistance, and controller-failover behavior as empirical measurements still requiring validation.
2. **Clarify and substantiate the novelty.**
   The manuscript integrates several established areas—formal verification, ML-based detection, multi-controller resilience, ATT&CK, and policy assurance. The authors should more clearly distinguish what is genuinely novel from what is an integration or synthesis of existing techniques. A detailed comparison with existing integrated SDN security architectures would strengthen the novelty claim.
3. **Provide a more rigorous comparative evaluation.**
   The paper should compare the proposed integrated architecture with

ISSN(O): 2320-5407 | ISSN(P): 3107-4928
International Journal of Advanced Research
Publisher's Name: Jana Publication and Research LLP
www.journalijar.com

existing approaches or conventional isolated security mechanisms using clearly defined criteria such as detection coverage, response safety, controller overhead, resilience, latency, and failure handling. At present, the analytical comparison is primarily conceptual.

4. **Quantify the proposed security–performance trade-off.**
   The framework introduces verification, telemetry collection, correlation, multi-controller coordination, and response validation. These mechanisms may introduce substantial computational and communication overhead. The manuscript should quantify or experimentally evaluate their impact on controller CPU utilization, latency, throughput, memory, and control-plane scalability.
5. **Strengthen the multi-controller resilience analysis.**
   The framework considers compromised, stale, or inconsistent controller replicas, but the proposed resilience mechanisms should be evaluated under realistic failure scenarios. In particular, experiments or simulations involving controller compromise, state divergence, Byzantine behavior, network partition, and recovery should be provided. The manuscript itself identifies quorum assumptions as critical.
6. **Provide greater detail on the ML/behavioral detection component.**
   The framework permits expert rules, statistical detectors, supervised models, and unsupervised/semi-supervised models, but does not prescribe a concrete detection model or evaluation methodology. The authors should specify how models are trained, calibrated, monitored for drift, and evaluated, especially under changing SDN traffic conditions.
7. **Validate the proposed closed-loop learning mechanism.**
   The manuscript proposes that tactical, operational, and strategic learning update indicators, thresholds, playbooks, telemetry, threat models, and invariants. This is a strong conceptual idea, but the paper should demonstrate how updates are safely promoted and how feedback contamination or model poisoning is prevented in practice.
8. **Make the threat-to-control traceability measurable.**
   ATT&CK-informed traceability is one of the stated contributions. The authors should provide a measurable coverage metric showing how many threats/techniques can be mapped to observables, invariants, analytics, response actions, and recovery evidence rather than relying mainly on illustrative mappings.

ISSN(O): 2320-5407 | ISSN(P): 3107-4928
International Journal of Advanced Research
Publisher's Name: Jana Publication and Research LLP
www.journalijar.com

REVIEWER'S REPORT

Minor Revisions

1. **Improve the distinction between conceptual claims and validated claims.**
   Since the manuscript deliberately avoids presenting hypothetical measurements as experimental results, this distinction should remain explicit throughout the abstract, results, discussion, and conclusion.
2. **Define the terminology more precisely**, particularly *SDN-native cybersecurity*, *assurance*, *invariant*, *evidence contract*, *governed detection*, and *cyber resilience*.
3. **Improve the presentation of the analytical scenarios.**
   For each scenario, clearly identify assumptions, attacker capabilities, expected evidence, decision criteria, response authority, and success/failure conditions.
4. **Add quantitative criteria to the requirement-coverage matrix.**
   The current analytical outcomes such as "covered," "partially covered," and "uncovered" would be more useful if accompanied by measurable criteria.
5. **Clarify the interoperability mechanism.**
   The discussion of adapters and centralized, hierarchical, and federated profiles is useful, but concrete examples of the required interfaces and exchanged security evidence would improve reproducibility.
6. **Strengthen the discussion of false positives and operational impact**, particularly for packet-in flooding and other attacks where legitimate traffic may resemble malicious behavior.
7. **Improve the figures and architectural diagrams** so that data flow, trust boundaries, evidence flow, controller interactions, and feedback paths are clearly distinguishable.
8. **Review the references and citation formatting**, particularly online references and standards, for consistent bibliographic style.
9. **Improve language and formatting consistency**, including section headings, table captions, terminology, abbreviations, and typographical errors.