Novelty of My Snort Documentation

The research paper I took inspiration from primarily focused on the theoretical aspects of Snort and its role in intrusion detection.

here is direct link to research paper :

https://www.researchgate.net/profile/Shabnam-Sharma-2/publication/329716671_Intrusion_Detection_Prevention_System_using_SNORT/links/5ef984e8299bf18816eff4ae/Intrusion-Detection-Prevention-System-using-SNORT.pdf

However, it lacked a practical hands-on implementation. To bridge this gap, I introduced the following unique aspects in my project:

🔹 Practical Hands-On Learning: Instead of just explaining Snort’s functionality, my project provides a step-by-step guide on installing, configuring, and using Snort 3 to detect ICMP packets in real time.

🔹 Rule Creation & Customization: The existing research lacked details on how to create and implement Snort rules. I addressed this by designing and demonstrating custom rules, laying the foundation for future security implementations.

🔹 Bridging Theory with Practical Application: This project transforms theory into actionable knowledge by allowing users to simulate real-world network attacks and detect them using Snort.

🔹 Foundation for Advanced Security Measures: The methodology used in this project can be extended to detect more complex threats, making it a strong starting point for further research in intrusion detection and prevention.