# STRENGTHENING HOME NETWORKS: EVALUATING ROUTERS AGAINST NIST STANDARDS

OLUWAPEMIISIN G. AKINGBOLA, DR. TOLUWALOGO ODUMOSU

## Introduction

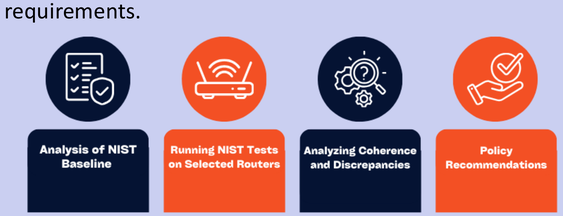
Routers today are designed to simplify the setup and management of a secure home network. Connecting IoT devices is made simpler by the fact that many routers are made to function with smart home ecosystems. People with little experience with technology can now operate a router thanks to its user-friendly designs. As a result, this has led to an increase in router adoption and accessibility in numerous American households [1]. According to SYMANTEC, Routers are one of the most attractive points of attack because they sit at the front gate of nearly every network and are the gateway to all internet-connected devices in the home [3]. Because a router serves as a firewall and a middleman for practically all networking traffic, it may be attacked in two ways: it can let in new attacks and serve as a launchpad for more sophisticated ones [4].

## Research Question

Are the present policy measures being proposed and implemented effectively securing home routers and IoT-integrated networks against evolving cybersecurity threats and mitigate risks arising from inadequate regulations and standards ensuring user data and privacy protection?

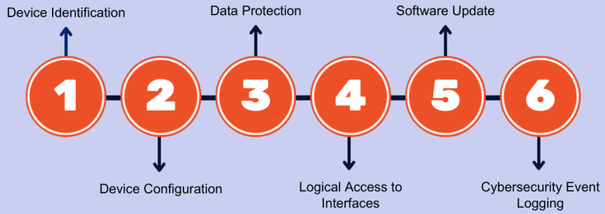
## Methodology

This study employs a systematic approach to evaluate the security of consumer-grade routers against evolving cybersecurity challenges. By leveraging established NIST cybersecurity baselines, technical frameworks, and compliance standards, the research aims to evaluate router performance while considering usability and regulatory requirements.

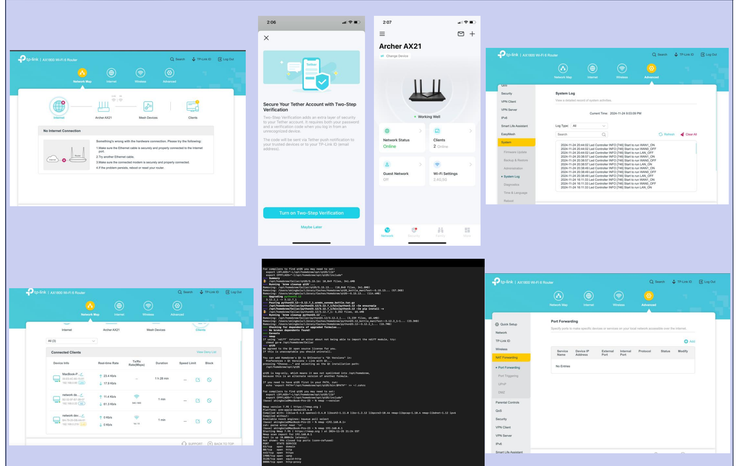



## NIST BASELINES FOR ROUTERS

- The **NIST Cybersecurity Baselines**, particularly those outlined in **NIST IR 8425** and **NIST IR 8425A**, provide detailed cybersecurity requirements and guidelines for consumer Internet of Things (IoT) devices, including routers.
- It encompass **6 core outcomes** applicable to IoT and routers, with additional **router-specific enhancements** like segmentation and remote access security [2].




## TP-LINK Archer AX21 TEST



*Test of both the the Web and Mobile GUI of the TP-Link Router*

## EERO 6 ROUTER TEST

*Amazon's Eero 6 Router Analysis*

## FUTURE WORK

Not all tests performed to date have fully conformed with the NIST cybersecurity baselines. Beyond meeting minimum security criteria, the objective of this study is to advocate for policies that take into consideration both personal security demands in the house and bare-metal security measures. This will be achieved by an examination of the policy implications for developing an all-encompassing framework.

## References


- Gangadharaiah, S., & Bhajantri, L. B. (2024). Secure data dissemination and routing in Internet of Things. International Journal of Information Technology, 1-18.
- Recommended Cybersecurity Requirements for Consumer Grade Router Products 6 Initial Preliminary Draft
- Symantec Internet Security Threat Report Attack Trends for Q3 and Q4 2002
- Scully, C., & Wang, P. (2018). Router security penetration testing in a virtual environment. In Information Technology-New Generations: 14th International Conference on Information Technology (pp. 119-124). Springer International Publishing.