**IoT Based Smart Automation Using WPA2 Security & Radius Server in Cisco Packet Tracer**

# ****Introduction****

The Internet of Things (IoT) is a significant advancement in digital transformation, redefining modern living and business. It connects virtual and physical layers, giving people more control and opportunities to stay connected. The smart home is an example of how IoT technologies work together and independently. This paper explores the implementation of an IoT smart home network using a Cisco Packet Tracer simulation, envisioning a future where smart homes are connected with corporate data communications, becoming a home-like and economically reasonable habitat. The technical complexities of such a multifunctional network are explored, suggesting a potential future where smart networked home systems could be essential for corporate change and consumer dialogue.

# ****Current Netwok Topology****

The success and operational feasibility of the IoT ecosystem in smart homes are influenced by the network topology. The IoT and RADIUS server connect peripheral devices, providing continuous interaction. A WRT300N wireless router connects end household devices to the server, enabling communication and portal functionality. IoT devices like windows, doors, and ceiling fans act as end nodes, allowing for control and monitoring through a web-based portal. The project is simulated using Cisco Packet Tracer's real-time network topology and device Proximus visualization tool. RADIUS server authentication protocols and WPA2 encryption ensure data integrity and entry-proofness, while the server authenticates users and device activities.

# Theoretical Expansion

## Overview

The IoT-based smart home network is expanding into business data communications, offering strategic implications for operational administration, data processing, and decision-making inefficiencies. This expansion will harness the full potential of IoT technology, enhancing innovation and simplifying access to company management and business intelligence from home, thereby enhancing overall business operations.

## Business Oriented IoT Devices

The integration of IoT devices in corporate environments offers new opportunities for control and optimization. Smart thermostats and energy management systems save operating expenses through energy consumption analytics and advanced climate control. Intelligent security cameras and access control systems improve security and data recording, meeting regulatory compliance and confidentiality demands (Jerald, 32-37). These devices can address efficiency and security needs while also generating valuable data for innovation and expansion.

## Network Segmentation

Network segmentation is a crucial tool for enhancing security and performance in company processes. It helps businesses design a network that segregates critical data from user access, optimizes network traffic, and provides appropriate bandwidth and resources for key business sectors. This division of network infrastructure can allow for a tailored network management strategy for different business spheres, whether internal or customer-oriented.

## Advanced User Interface

The human-IoT environment is evolving with an advanced control panel that offers a unique perspective on device performance and energy consumption. It's an intelligent platform that forecasts user needs, makes efficiency suggestions, and uses predictive algorithms for repetitive processes (Brambilla, 14). Its real-time data visualizations and customized dashboards will enable informed decisions.  
Integration of Voice Control and Machine Learning

The integration of voice control and machine learning in IoT smart home systems is transforming the way users interact with their devices. Voice assistants allow users to issue commands without using their hands, while machine learning allows systems to learn from users' experiences and adjust to new use scenarios (Chattopadhyay, 223-244). This new feature will enable more autonomous systems, allowing them to respond to explicit commands and execute actions as a cohesive unit, paving the way for more personalized and customizable environments.

## Business Applications Dashboard

A business application dashboard is a command center for managing IoT devices in a business setting, providing a centralized view of functions, performance indicators, and alerts. It will enable easy control and management across locations, enabling immediate decision-making based on real-time data. The dashboard will also enable remote device configuration and troubleshooting, ensuring uniformity and security in multi-site businesses. Future advancements could include predictive analytics for estimating malfunctions and potential outages.

## Advanced Security

The integration of IoT networks into home and commercial infrastructures necessitates enhanced data communication security to prevent cyber-attack threats. Active security strategies include updating encryption systems, implementing advanced measures like WPA3, stringent authentication procedures, end-to-end encryption, zero-trust design, frequent security audits, and security upgrades to limit access to unauthorized individuals and securely share sensitive data (Xu, 2840-2853).

# Conclusion

This paper highlights the importance of IoT-based smart home systems in enhancing efficiency and security in residential and commercial environments. It emphasizes the need to balance security with innovation, ensuring user confidentiality and data privacy. The challenge lies in promoting innovation while reinforcing security infrastructure, ensuring IoT systems remain reliable tools for individuals and companies.

**Works Cited**

Brambilla, Marco, Eric Umuhoza, and Roberto Acerbis. "Model-driven development of user interfaces for IoT systems via domain-specific components and patterns." Journal of Internet Services and Applications 8.1 (2017): 14.

Chattopadhyay, Ananya, Sushruta Mishra, and Alfonso González-Briones. "Integration of machine learning and IoT in healthcare domain." Hybrid artificial intelligence and IoT in healthcare (2021): 223-244.

Osman, Amr, et al. "Transparent Microsegmentation in Smart Home {IoT} Networks." 3rd USENIX Workshop on Hot Topics in Edge Computing (HotEdge 20). 2020.

Song, Minzheong. "A Study on Business Types of IoT-based Smarthome: based on the theory of Platform Typology." *The Journal of the Institute of Internet, Broadcasting and Communication* 16.2 (2016): 27-40.

Vimal Jerald, A., S. A. Rabara, and T. D. P. Bai. "Internet of things (IoT) based smart environment integrating various business applications." International Journal of Computer Applications 128.8 (2015): 32-37.

Xu, Qian, et al. "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations." IEEE Access 4 (2016): 2840-2853.