IT4010 Research Project – 2025 July

Topic Assessment Form

Project ID : **25-26J-029**

1. Topic (12 words max)

An Adaptive Zero Trust Security Framework for SOHO IoT Networks

2. Research group the project belongs to

CI - Computing Infrasrtucture

3. Specialization of the project belongs to

Computer Systems and Network Engineering(CSNE)

4. If a continuation of a previous project:

Project ID	
Year	

5. Brief description of the research problem including references (200 – 500 words max) – references not included in word count.

The recent surge in Internet of Things (IoT) devices has made Small Office/Home Office (SOHO) networks evolve into heterogeneous and intricate networks. Though the devices provide high levels of usability, they also, at the same time, present a high and generally unmanaged attack surface. The greatest issue of this study is the inherent vulnerabilities of these consumer-level devices and their failure by conventional network security measures to properly defend against them [1]. The majority of IoT devices are deployed with extremely tight resource constraints, which makes it infeasible to utilize strong security measures on the device itself. This is also compounded by insecure practices like the utilization of weak or hardcoded default passwords, a prevalent attack vector leveraged by botnets like Mirai. Traditional security models based on perimeter defenses are ineffective against this threat landscape, as they offer little protection once a device on the "trusted" network has been compromised, making it easy lateral movement for the attackers [2].

Software-Defined Networking (SDN) offers a good solution to handle these challenges. SDN, by separating the control and data planes of the network, allows centralized intelligence along with programmable management of the whole network. This enables adaptable application of certain security regulations without requiring alteration of the resource-limited Internet of Things (IoT) devices. The present study suggests an integrated and economical security mechanism that adopts Software-Defined Networking (SDN) for establishing a Zero Trust Architecture (ZTA) and an active defense strategy [2][3].

The ZTA architecture follows the "never trust, always verify"[2] principle that calls for ongoing authentication and authorization of every machine before granting access to network resources. This is complemented by an active defense mechanism that uses network deception (honeypots) to lure and analyze attackers and automatically generate new mitigation rules to harden the network against new threats [4]. While ZTA and SDN-based security are mature research areas, their integration with active defense to create a self-hardening, adaptive security system specifically for the cost-sensitive and non-technical SOHO space is a significant research gap. The goal of this project is to create and evaluate a framework which focuses on automation, resilience, and usability particularly for domestic users [5].

References

[1] H. Ahmadvand, C. Lal, H. Hemmati, M. Sookhak, and M. Conti, "Privacy-Preserving and Security in SDN-Based IoT: A survey," *IEEE Access*, vol. 11, pp. 44772–44786, Jan. 2023, doi: 10.1109/access.2023.3267764.

[2] M. L. Gambo and A. Almulhem, "Zero Trust Architecture: A Systematic Literature Review," *TechRxiv*, Feb. 2025, doi: 10.36227/techrxiv.173933211.18231232/v1

[3] S. R. Mishra, B. Shanmugam, K. C. Yeo, and S. Thennadil, "SDN-Enabled IoT Security Frameworks—A review of Existing challenges," *Technologies*, vol. 13, no. 3, p. 121, Mar. 2025, doi: 10.3390/technologies13030121

[4] J. Li, C. Wang, Z. Li, and Y. Ding, "A Honeypot-enabled SDN-based Selector for Industrial Device Access Control," *2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC)*, pp. 523–528, Oct. 2021, doi: 10.1109/dsc53577.2021.00083.

[5] N. F. Amirah and L. Ngah, "Development of SDN Controller Testbed Using Rasberry Pi 4", *IJSET*, vol. 2, no. 2, pp. 29-38, Dec. 2021 Available: https://tatiuc.edu.my/ijset/index.php/ijset/article/view/102

.

6. Brief description of the nature of the solution including a conceptual diagram (250 words max)

The solution proposed is a multi-layered, dynamic security system for safeguarding vulnerable Internet of Things (IoT) devices in Small Office/Home Office (SOHO) networks. The system takes advantage of the centralized management aspect of Software-Defined Networking (SDN), with an economically feasible Raspberry Pi being utilized as the network controller.

The framework uniquely integrates a Zero Trust Architecture (ZTA) with an Active Defense approach. In the ZTA model, no device is inherently trusted; instead, each device must go through a secure onboarding process to receive a unique identity, whereupon it is assigned least-privilege network access based on its intended function. This initial micro-segmentation automatically reduces threats.

The Active Defense component continuously monitors for anomalous behavior using light-weight heuristics. The SDN controller transparently redirects suspicious traffic to a honeypot container. Deception in this case allows the framework to study attacker tactics in a secure way and automatically gather threat intelligence, (e.g.: malware IP addresses). This intelligence is reported back to the controller, which generates and implements new, persistent blocking rules, which therefore establish a self-enforcing, secure framework that defends the network against evolving threats without necessitating any transformation of the IoT devices themselves.

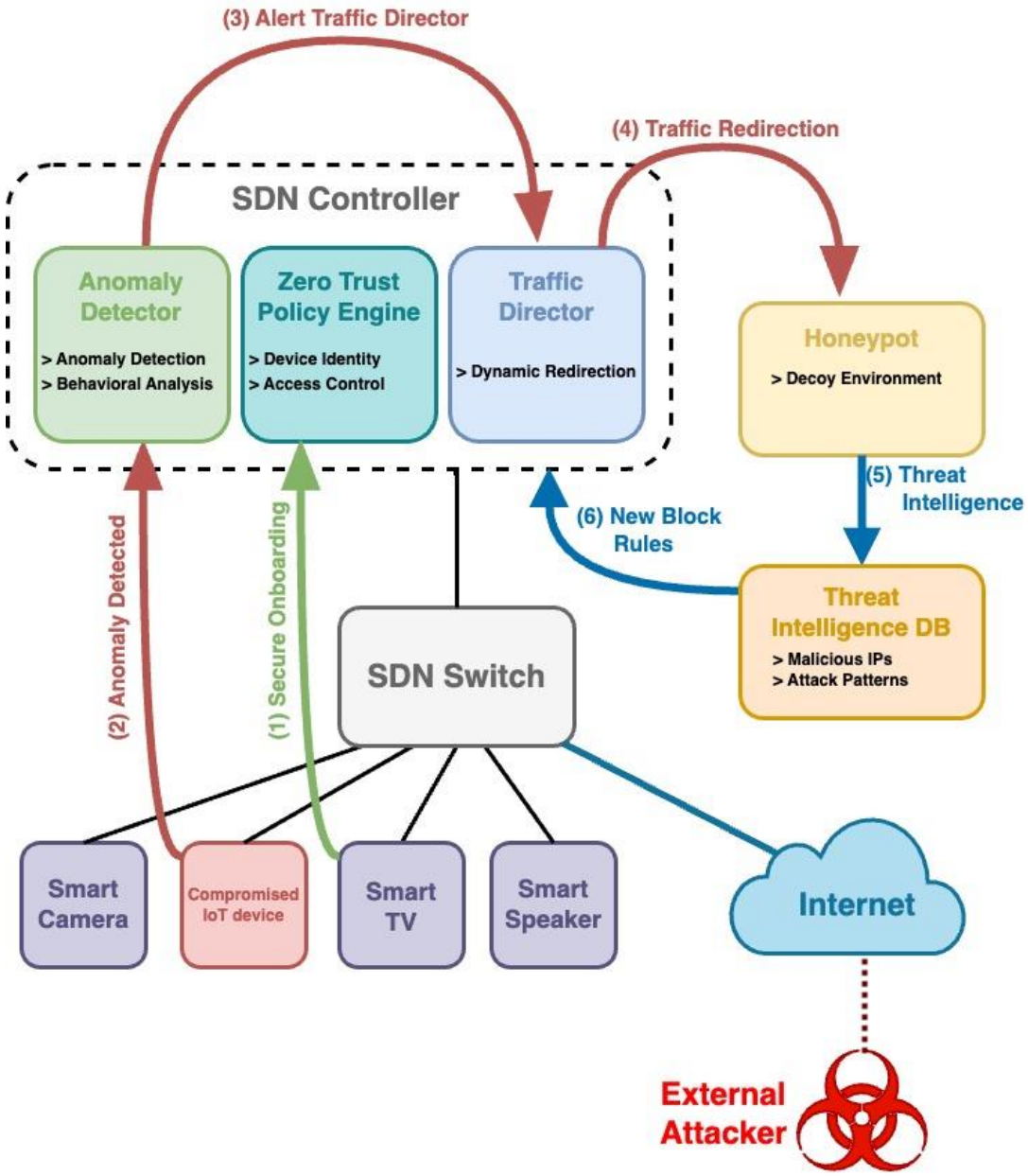


Figure: Conceptual diagram

7. Brief description of specialized domain expertise, knowledge, and data requirements (300 words max)

This project requires a multidisciplinary fusion of technical skills in network security, more precisely in Software-Defined Networking (SDN), Zero Trust Architecture (ZTA), and Internet of Things (IoT) security protocols.

Domain Expertise and Knowledge:

A fundamental understanding of network architecture, especially the separation of the control and data planes in SDN, is necessary. The members of the team must have practical experience with the implementation of security policies and traffic redirection by an SDN controller like Ryu and the OpenFlow protocol. Python knowledge is also necessary for programming the security modules of the controller.

The implementation of Zero Trust components calls for experience in identity and access management (IAM) principles, including the utilization of Public Key Infrastructure (PKI) and tools such as OpenSSL for certificate provisioning and management on devices. For the Active Defense section, technical expertise in deception technology is a requirement, particularly in the deployment and management of containerized honeypots (e.g., Docker and Cowrie) for enticing and examining potential attackers. An understanding of network emulation with Mininet is also required for establishing the virtual lab.

Data Requirements:

The project has significant data requirements for testing and validation. In particular, it requires access to publicly available, labeled network traffic datasets to simulate real-world attacks and establish behavioral baselines. The **BoT-IoT** and **IoT-23** datasets are especially well-suited for this purpose, as they consist of a mix of benign traffic with labeled malicious traffic from IoT botnets, including DoS and network scanning attacks. Additionally, the system needs access to real-time or regularly updated threat intelligence feeds, e.g: IP and domain blocklists provided by sources such as **Spamhaus** or **abuse.ch**, to facilitate proactive threat blocking. The system will ultimately also produce output in the form of honeypot interaction logs that need to be processed to distill usable intelligence for the sake of automated network hardening.

8. Objectives and Novelty

Main Objective

To create, deploy, and test an affordable, multi-layered security system for SOHO IoT networks using a Raspberry Pi as an SDN controller. The project integrates a Zero Trust Architecture (ZTA) and an Active Defense strategy. The system will enforce the "never trust, always verify" paradigm on all devices through secure onboarding and ongoing monitoring. It will also actively defend the network by using honeypots to entice, analyze, and automatically build mitigation rules against new and unknown threats, creating a strong, self-hardening security system that is accessible to users who lack technical expertise.

Member Name with Registration No	**Sub Objective**	**Tasks**	**Novelty**
GONAGALA G.A.S.T IT22314956	**Implement the SDN Controller for Dynamic Policy and Traffic Control**	• Set up and configure the SDN controller on the Raspberry Pi. • Develop the central application logic that acts as the policy enforcement point for the entire framework. • Receive high-level policy definitions from the Identity module and translate them into granular OpenFlow rules to enforce least-privilege access.	**Dynamic and Multifaceted Traffic Orchestration:** The central innovation involves developing a single, intelligent orchestration engine that dynamically patrols the network data plane by enforcing various security policies (allow, deny, redirect, quarantine) based on a variety of real-time variables, including device identity, trust scores, and current threat intelligence.

		• Listen for threat alerts from the Analyst module. • Dynamically install OpenFlow rules to transparently redirect suspicious traffic to the honeypot. • Enforce mitigation actions based on confirmed threat intelligence from the Analyst module.	
RANAWAKA R.A.S.M. IT22320728	**Secure Onboarding and Identity Management**	• Design and implement a secure onboarding process for new IoT devices. • Create and manage a lightweight device identity database using SQLite on the Raspberry Pi. • Observe the initial traffic patterns of newly onboarded devices to establish a behavioral baseline. • Automatically generate an initial "least privilege" access policy based on the learned behavior and provide it to the Policy Engine.	**Simplified Cryptographic Onboarding for Consumer IoT:** Includes creating a secure and easy onboarding process that demystifies the complexities of Public Key Infrastructure (PKI) for users with no technical know-how. It enables automatic linking of a device's physical identity with a strong, provable network credential, which is a foundational backbone component required to deploy a Zero Trust architecture.

ERIYAGAMA V.K. IT22136510	**Heuristic Analyst and Honeypot Management**	• Develop a heuristic-based anomaly detection system by periodically polling flow statistics from network switches using Ryu. • Compare real-time traffic metrics against the normal baseline profiles to detect anomalies like DoS attacks or network scans. • Send alerts to the Policy Engine to trigger traffic redirection. • Use Docker to deploy and manage lightweight, containerized honeypots to emulate vulnerable IoT services. • Develop scripts to parse honeypot logs to extract actionable threat intelligence (e.g: attacker's IP address, commands used). • Pass confirmed threat intelligence to the Policy Engine for permanent mitigation.	**Integrated Heuristic-Deception Feedback Loop:** The innovation is the tight integration of lightweight anomaly detection with an active deception environment. The heuristic analysis acts as a tripwire that triggers the honeypot to capture high-fidelity threat intelligence. This intelligence is then used to create confirmed, high-confidence mitigation rules, creating a more adaptive defense system than either component could achieve alone.

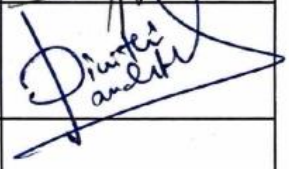
DEWARATHNE P.S. IT22004536	**Continuous Trust Evaluation**	• Develop a system to manage a dynamic "trust score" for each device in the identity database. • Implement a lightweight continuous device attestation mechanism to periodically verify the integrity of connected devices. • Lower a device's trust score upon receiving alerts from the Analyst module or upon a failed attestation check. • Communicate trust score changes to the Policy Engine so it can adjust access policies (e.g: quarantine a low-trust device).	**Dynamic Trust Scoring for Adaptive Zero Trust:** The novelty is the creation of a dynamic trust score for SOHO devices based on multiple factors, including both behavioral heuristics (from the Analyst) and device integrity checks (attestation). This score provides a quantifiable measure of trust that allows the Policy Engine to make adaptive, fine-grained access control decisions, which is a core tenet of a true Zero Trust model.

9. Individual component description of how it is complied with the specialization.

Member Name with Registration No	**Description**
GONAGALA G.A.S.T IT22314956	Effectively utilizing knowledge in **SDN** and the **OpenFlow protocol**. The fundamental Ryu controller application acquires overarching directives from all supplementary modules and converts these into detailed OpenFlow regulations. This is a process of configuring the network to utilize least-privilege protocols for newly onboarded devices, redirecting questionable traffic to the honeypot dynamically, and establishing long-term block policies to prevent confirmed threats. To accomplish this task successfully demands advanced skills in **network programming**, in addition to profound knowledge of how to modulate traffic streams at the data plane.
RANAWAKA R.A.S.M. IT22320728	Lays the groundwork for the Zero Trust Architecture through the identity management of all devices, which involves an understanding of **Identity and Access Management (IAM)** principles and **Public Key Infrastructure (PKI)**. The system employs specific onboarding process to provision the target IoT device with a unique cryptographic identity, e.g.: an X.509 certificate generated with OpenSSL. During onboarding, profiles the device's normal network behavior to create a baseline, then uses this to automatically generate its initial, tight access control policy.
ERIYAGAMA V.K. IT22136510	Integrating **network traffic analysis** with **deception technology**, this component acts as the framework's active threat detection system. It employs heuristic analysis by monitoring OpenFlow statistics to detect behavioral anomalies, which serve as an initial tripwire. Upon detection, it leverages its deception capabilities by alerting the controller to redirect suspicious traffic to a managed, containerized honeypot. The final task is to parse honeypot interaction logs to extract high-fidelity, actionable threat intelligence, which is then fed back to the Policy Engine for an automated, intelligence-driven response.
DEWARATHNE P.S. IT22004536	Operationalizing the core Zero Trust principle of **continuous verification**, this component's specialization lies in maintaining a dynamic trust score for every device on the network. This score is a quantifiable measure of trustworthiness that is continuously re-evaluated based on multiple data points, including real-time behavioral alerts from the Heuristic Analyst and the results of its own periodic device integrity checks (attestation). Its primary function is to communicate any degradation in a device's trust score to the Policy Engine, enabling the framework to make adaptive, risk-based access control decisions,

	such as revoking privileges or quarantining a device that is no longer trustworthy.

10. Supervisor details

	Title	First Name	Last Name	Signature
Supervisor	Ms.	Shashika	Lokuliyana	
Co-Supervisor	Ms.	Dinithi	Pandithage	
External Supervisor				
Summary of external supervisor's (if any) experience and expertise				

SLIIT UNI
THE KNOWLEDGE UNIVERSITY

IT4010 Research Project – 2025 July

Topic Assessment Form

<u>This part is to be filled by the Topic Screening Staff members.</u>

a) Does the chosen research topic possess a comprehensive scope suitable for a final-year project?

Yes	✓	No	

b) Does the proposed topic exhibit novelty?

Yes	✓	No	

c) Do you believe they have the capability to successfully execute the proposed project?

Yes	✓	No	

d) Do the proposed sub-objectives reflect the students' areas of specialization?

Yes	✓	No	

e) Supervisor's Evaluation and Recommendation for the Research topic:

Recommended for project proposal.

IT4010 Research Project – 2025 July

Topic Assessment Form

Acceptable: Mark/Select as necessary

Topic Assessment Accepted	
Topic Assessment Accepted with minor changes*	✓
Topic Assessment to be Resubmitted with major changes*	
Topic Assessment Rejected. Topic must be changed	

* Detailed comments given below

Comments

1) Reword the objectives and tasks, novelty componnest accordingly.

Staff Member's Name	Signature
Shashika Lokuliyana	
Dinithi Panditharathne	

*__Important__:

1. According to the comments given by the evaluator, make the necessary modifications and get the approval by the **Evaluator**.
2. If the project topic is rejected, identify a new topic, and request the RP Team for a new topic assessment.