




Sri Lanka Institute of Information Technology

ISP- (IE 3092)

Individual Assignment

Project Proposal

Submitted by:				
STUDENT NAME	STUDENT ID.	CONTACT NO.	EMAIL	SIGNATURE
Nanayakkara Y.D.T.D.	IT21826368	+94763066541	it21826368@my.sliit.lk	

Module In charge:	Mr. Deemantha.S Mr. Tharaniyawarma.k
Project Topic:	<i>Applying Machine Learning for Real-Time Security Threat Detection in Smart Homes.</i>
Date:	7 th August of 2024

Contents

1	Introduction.....	3
1.1	Overview.....	3
1.2	How to Use?.....	3
1.3	Importance of Security in Smart Homes.....	4
2	Existing Problems	5
3	Objectives	6
3.1	Main Objective:	6
3.2	Sub-Objectives:.....	6
4	Literature Review.....	7
5	Proposed Methodology	9
5.1	Implementation Process	9
5.2	Software Requirements	10
5.3	Hardware Requirements.....	10
5.4	Big Picture	10
6	References	11

1 Introduction

1.1 Overview.

What is a smart home?

Same as the “*regular*” home but connectivity among electronic devices improves the way we live in.
– the verge [1].

From the same idea, the project is to improve the smart home security.

Project focuses on leveraging machine learning algorithms to enhance the security of smart home environments. Developing a machine learning model that detects real-time threats, including unauthorized access and possible emerging risks that can affect smart homes.

For model training, analyzing data from IoT devices, sensors, and cameras involves key steps like extracting relevant features, preprocessing the data, labeling it with normal or suspicious behavior, training machine learning algorithms, and validating the model’s performance. Continuous learning is also applied to adapt to new threats over time.

By achieving this goal, aiming to create a usable, customizable, and security-rich smart home threat detection system.

1.2 How to Use?

For ease of use, the system integrates seamlessly with the existing smart home setup. Only need additionally adding the control hub, making installation and configuration straightforward.

- Users sync their connected devices during data initialization, and the system automatically trains its machine learning model.
- Users can monitor home security via a user-friendly dashboard that provides real-time status and alerts for potential threats like unauthorized access or unusual activity. They can review detailed reports and logs and adjust alert settings and sensitivity levels.
- Adding new devices involves following integration instructions in the dashboard.
- Troubleshooting guides help resolve common issues, and customer support is available within the application for personalized assistance.
- The main hub or controlling interface may be updated, and the system periodically updates its machine learning model to stay current with new threats, ensuring ongoing protection for the smart home.

- Functionality of a smart home
 - Heating
 - Lighting
 - Audio/Visual
 - Digital Assistance
 - Security
- Benefits in a smart home
 - Convenience
 - Easy Control.
 - Smart Scheduling.
 - Energy Efficiency
 - Automation
 - Seamless Operations.
 - Custom Setting to your preferences.
 - Security
 - Safeguard against intruders and cyber threats.
 - Real-Time Alerts.

Based on these functionalities and benefits smart home have its place on future.

1.3 Importance of Security in Smart Homes

- Protection of Personal Data and Information collected by devices.
- Prevention of Unauthorized Access.
- Safeguarding Against Remote Hacking.
- Mitigating Risk of Device compromise or malfunctioning systems.
- Maintaining System Integrity.
- Protecting Against Physical and Financial Loss.

2 Existing Problems

- Security Threats
 - Unauthorized access, Data breaches and privacy concerns.
- System Limitations
 - Ineffective in dynamic environments
 - Delays in detection and response
- False Alarms
 - User desensitization
 - Resource wastage
- Real-Time Monitoring Challenges
 - High data processing demands
 - Integration issues with diverse devices
- Integration and Scalability
 - Compatibility problems with new devices
 - Difficulty adapting to evolving threats
- Growth of using Smart Devices

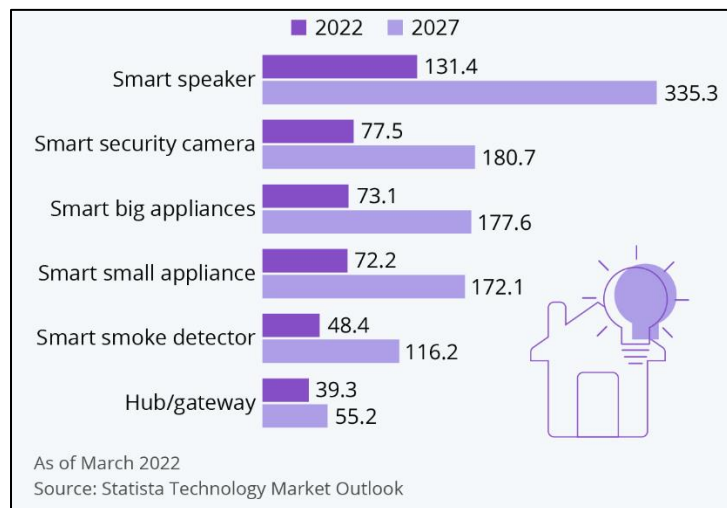


Figure 1 :Estimated number of households worldwide with the above smart devices (In millions) [2]

3 Objectives

3.1 Main Objective:

- To develop a machine learning-based system for real-time threat detection in smart homes as a solution to the existing problems.

3.2 Sub-Objectives:

- To *improve accuracy* by reducing false alarms and enhancing threat detection precision.
- To *enable real-time processing* for immediate threat detection and response.
- To *ensure seamless integration* with various smart home devices.
- To *achieve scalability*, allowing *adaptation* to new devices and evolving threats.

4 Literature Review

[3]

Technique Used		Approach	Author and Publications	Published Year
Machine Learning and Real-time Intrusion Detection with Data-Driven Approaches	Anomaly detection	Pattern recognition	Machine Learning, revised and updated edition (The MIT Press Essential Knowledge series) - Ethem Alpaydin	August 2021
	Behavioral analysis	User profiling	A User Identification Algorithm Based on User Behavior Analysis in Social Networks - IEEE Access - Ling Xing	March 2019
	Network traffic analysis	Network Monitoring	A Survey on Encrypted Network Traffic Analysis Applications, Techniques, and Countermeasures- Eva Papadogiannaki, Sotiris Ioannidis	July 2021
	Date fusion techniques combining data from multiple sensors for enhanced detection.	Multi-sensor data integration	Automated Multi-Sensor Data Fusion Using the Unified Data Library - Kristen R. Haynes, J. Hollon	June 2021
Emerging Technologies	Edge computing for processing data closer to the source for faster response.	Edge computing	Edge Computational Intelligence for AI-Enabled IoT Systems - Shrikaant Kulkarni, Jaiprakash Narain Dwivedi	February 2024
			At the Confluence of Artificial Intelligence and Edge Computing – sensors - Amira Bourechak	February 2023
	Advanced algorithms for threat detection and response.	AI Algorithm	Edge Computing with Artificial Intelligence: A Machine Learning Perspective - Shuiguang Deng	September 2019

Evaluation and Optimization	False positive/negative rates in balancing detection with false alarms.	Statistical Analysis	Balancing true and false detection of intermittent sensory targets by adjusting the inputs to the evidence accumulation process - Anna C Geuzebroek	August 2023
	Performance metrics (accuracy, precision, recall).	Statistical Analysis	Algorithms for Optimization - Mykel J. Kochenderfer, Tim A. Wheeler	March 2019
	Model optimization	Optimization techniques		
Privacy	Data minimization	Data Minimization	PAX: Using Pseudonymization and Anonymization to Protect Patients' Identities and Data in the Healthcare System - Mishall Al-Zubaidie	April 2019
	Anonymization and pseudonymization	Anonymization techniques		
	Privacy-preserving machine learning: techniques to protect sensitive information	Privacy preserving ML	Privacy-Preserving Machine Learning Threats and Solutions -Mohammad Al-Rubaie	April 2019

5 Proposed Methodology

5.1 Implementation Process

To implement the proposed system for the smart homes, the project will be divided into several key phases. These phases will ensure systematic development, integration, and evaluation of the system.

Phase	Details
I. Requirement Analysis.	<ul style="list-style-type: none"> ▪ Determine the specific security needs and constraints for the smart home environment. ▪ Identify Devices and User Requirements.
II. Data Collection and Preparation.	<ul style="list-style-type: none"> ▪ Gather data from open-access datasets or various smart home sensors such as motion detectors, cameras, and other IoT devices. ▪ Clean, normalize, and label the collected data to ensure it is suitable for analysis and model training.
III. Feature Extraction and Selection.	<ul style="list-style-type: none"> ▪ Determine the key features from the data that indicate normal and abnormal behaviors. ▪ Implement methods to extract these features from the preprocessed data, ensuring they are relevant for training the machine learning models.
IV. Model Development.	<ul style="list-style-type: none"> ▪ Algorithm Selection. ▪ Train Models.
V. System Design and Integration.	<ul style="list-style-type: none"> ▪ Design Architecture. ▪ Develop Interface.
VI. Real-Time Processing Implementation.	<ul style="list-style-type: none"> ▪ Establish a real-time data processing pipeline to continuously monitor and analyze incoming data. ▪ Implement Anomaly Detection.

VII. Testing and Evaluation.	<ul style="list-style-type: none"> ▪ Functional Testing. ▪ Performance Evaluation.
VIII. Deployment	<ul style="list-style-type: none"> ▪ Develop a detailed strategy for deploying the system in live smart home environments. ▪ Install System.
IX. Monitoring and Maintenance.	<ul style="list-style-type: none"> ▪ Monitor Performance and regular updates.

5.2 Software Requirements

Category	Components	Purpose
Machine Learning Frameworks	TensorFlow	Model development and training
Image Processing	OpenCV	Image processing (from cameras)
Data Preprocessing & Visualization	Pandas	Data Preprocessing & Visualization
Real-Time Data Processing	Kafka	Real-Time Data Processing
Low-Latency Inference	TensorFlow Serving	Low-Latency Inference

5.3 Hardware Requirements

Category	Components	Purpose
Edge Devices	Raspberry Pi, Arduino	Data collection, basic processing, model inference
Power Supply	Efficient Power Sources	Continuous operation of devices and sensors
Network Infrastructure	Reliable Internet Connection	Connectivity for cloud services and remote monitoring

5.4 Big Picture

Smart homes, while offering convenience, have become increasingly susceptible to security threats. This project aims to develop a robust system prioritizing resident safety. By leveraging advanced machine learning techniques, the system will continuously monitor smart home devices for anomalous behavior indicative of potential security breaches. Through real-time analysis, it will detect and respond to threats promptly, safeguarding homes and providing peace of mind.

6 References

- [1] "TheVerge.com," [Online]. Available: <https://www.theverge.com/23749376/smart-home-explained-voice-assistant-tv-gadgets>.
- [2] "Weforum.org," [Online]. Available: <https://www.weforum.org/agenda/2022/04/homes-smart-tech-market/>.
- [3] H. Snyder, "Literature review as a research methodology_ An overview and guidelines".