Securing Smart Homes: Threat & Vulnerability Analysis with AI Defense

Md. Juwel Mallick  
*Computer Science & Engineering*   
*Bangabandhu Sheikh Mujibur Rahman Science and Technology University  
Gopalganj, Bangladesh*  
juwel.bsc.bsmrstu@gmail.com

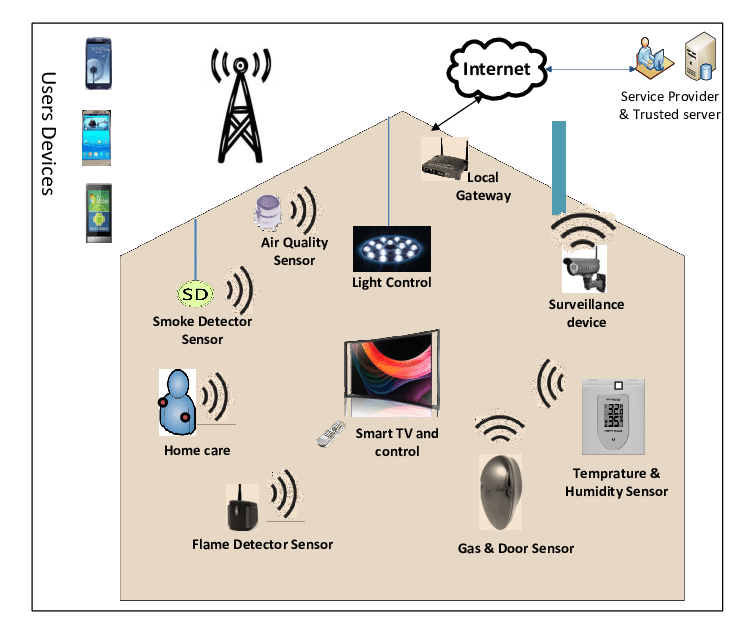
*Abstract*— Smart homes are increasingly ubiquitous, offering enhanced convenience, comfort, and efficiency through automated control of various household systems. These integrated technologies provide users with remote access and real-time monitoring capabilities, revolutionizing daily living experiences and paving the way for a more interconnected and digitally-enabled lifestyle. At the same time, various types of threats and security risks are being created due to the weakness of the system. This thesis focuses on the comprehensive risk analysis of smart home automation systems, emphasizing identifying and analyzing potential threats. The research aims to catalog vulnerabilities, quantify security risks, and develop AI models for attack detection. The anticipated outcomes include actionable recommendations to enhance smart home security and contribute valuable insights for homeowners, manufacturers, and policymakers. Ethical considerations guide the research, ensuring a responsible approach to security testing. The thesis addresses unique cybersecurity challenges in smart homes, offering practical solutions for a more secure and resilient ecosystem.

Keywords—component, formatting, style, styling, insert (key words)

# Introduction

## Background and motivation

In the modern world, many ecosystems are present such as smart homes, industrial automation, smart cities, eHealth, and cloud computing these are becoming increasingly prevalent due to their ability to integrate Internet of Things (IoT) devices, offering convenience, security, and energy efficiency.[1]

Smart homes are one of the major of them that are equipped with interconnected devices and automated systems. Integrating Internet of Things (IoT) devices into home environments offers unexampled levels of monitoring and control. However, this rise in smart homes has also brought about a significant number of security challenges, threats, and vulnerabilities. These technologies become more deeply embedded in our daily lives, and understanding and preventing risks has become compulsory. This thesis's goal is to determine security concerns in smart home automation by identifying and analyzing threats, conducting a comprehensive risk analysis, and designing Artificial intelligence models for attack detection. Expected outcomes include providing actionable recommendations for enhancing smart home security and valuable insights for manufacturers, homeowners, and policymakers. The thesis offers practical solutions for a more resilient and secure system and addresses unique cybersecurity challenges in smart homes.

## Major contributions

This thesis makes a significant contribution to improving smart home automation systems' security. Among its key contributions are:

* Vulnerability Identification
* Threat Analysis
* Machine Learning Model Development for IDS
* Actionable Insights for Homeowners, Manufacturers, and Policymakers
* Security Awareness Increase

These contributions are crucial to solving the cybersecurity issues in smart home environments and promoting a more secure and resilient ecosystem.

# Related Literature Review

# The data is intentionally hidden for security purposes..

# environment of smart home system

The

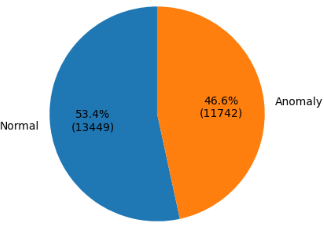
in daily living.

# Methodology(thread analysis)

Thi, and continuous evaluation and improvement.

# ML model designed for IDS

## Dataset Description

The auditable dataset[2] consists of comprises several intrusions simulated in a military network environment, mimicking a typical US Air Force LAN. It contains TCP/IP dump data that shows connections that have been classified as normal or as attacks with particular attack types. A connection record has about approximately 100 bytes in it. From normal and attack data, 41 quantitative and qualitative features (38 quantitative features and 3 qualitative) are derived for each TCP/IP connection.

2 categories in the class variable:

* Normal
* Anomalous

Fig. 2**.** Distribution of Normal and Anomaly Data

Database file (2.88 MB) with 25192 rows and 42 columns.

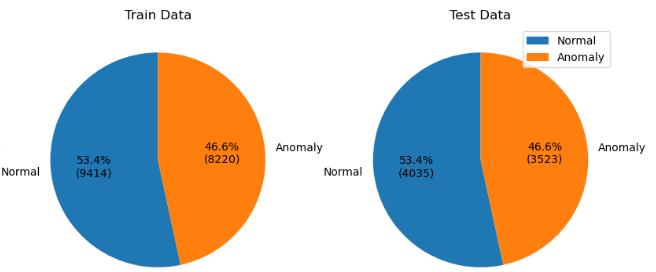
## Data Preprocessing

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | ***protocol\_type*** | ***service*** | ***flag*** | ***class*** |
| count | 25192 | 25192 | 25192 | 25192 |
| unique | 3 | 66 | 11 | 2 |
| top | tcp | http | SF | normal |
| freq | 20526 | 8003 | 14973 | 13449 |

### data description)

Fig. 4. All object(string) type features

### .

Fig. 3. Train data 70% and test 30%

### Tree,

### 

## Integration with Network Infrastructure

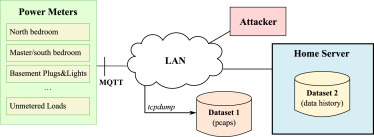
.

Fig. 6. Intrusion & detection in smart homes[4]

ThResults and Analysis

## IDS output

### # The data is intentionally hidden for security purposes..

* for further investigation and resolution.

## Thread & Vulnerability analysis

In the modern world, many ecosystems are present such as smart homes.

# Recommendations

# The data is intentionally hidden for security purposes.Conclusion

This research project aims to conduct a comprehensive risk analysis of smart home automation systems, focusing on the identification and classification of potential attacks and threats using AI and machine learning to learn security vulnerabilities. The expected results include actionable recommendations for improving smart home security, with significant implications for homeowners, manufacturers, and policymakers.

##### Acknowledgment *(Heading 5)*

# The data is intentionally hidden for security purposes..

##### References

1. G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*
2. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
3. I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.
4. K. Elissa, “Title of paper if known,” unpublished.
5. R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.
6. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
7. M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

# The data is intentionally hidden for security purposes.