Online Journal of Applied Knowledge Management

A Publication of the International Institute for Applied Knowledge Management

Volume 12, Issue2, 2024

Prototype design of securing the internet of things in smart homes

Stephen Mujeye, Illinois State University, USA, smujey1@ilstu.edu

Abstract

The Internet of Things (IoT) technology has revolutionized how businesses operate and changed our daily lives. IoT devices are used in different areas, including smart cities, smart agriculture, smart healthcare, and smart homes. The number of IoT devices connected worldwide continues to rise, and 75 billion devices are expected to be connected by 2025. Even though IoT devices are rapidly spreading, they come with security and privacy challenges. Traditional methods for securing against cyber-attacks are inefficient and inadequate for securing IoT devices. This study aimed to design and implement a secure hub ecosystem prototype with an Intrusion Detection System (IDS), including Machine Learning (ML), to defend IoT devices in a smart home. After the literature about the security of IoT devices in smart homes was analyzed to identify current challenges and limitations, a secure IoT hub ecosystem prototype was implemented. Benign data and malicious data were generated in the IoT testbed. Data was collected from the IoT smart home testbed and implemented using a supervised IDS with ML. The results demonstrate the effectiveness of network segmentation using a hub in mitigating device detection, Denial-of-Service (DoS), and Man-In-The-Middle (MITM) attacks, which were successful in unsegmented networks. Additionally, supervised machine learning classifiers, such as Random Forest and J48, exhibited exceptional performance with precision, recall, and F-measure scores exceeding 97%, highlighting their potential for detecting malicious activities and classifying IoT devices accurately. These findings underscore the importance of combining network segmentation, advanced machine learning algorithms, and user education to strengthen IoT security in smart homes. The results contribute valuable insights to the development of resilient IoT security frameworks.

Keywords: Internet of Things (IoT), smart home, Machine Learning (ML), Intrusion Detection Systems (IDS), cyber-attacks.

Introduction

Shafiq et al. (2022) defined the Internet of Things (IoT) as a network of devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity, enabling the objects to connect and exchange data. On the other hand, Hussain (2021) referred to IoT as a collection of smart devices or objects connected to the Internet to provide different services. IoT devices have created a revolutionary impact on human life, and they have been used in smart healthcare, smart industry, smart city, smart grid, and smart homes. IoT devices produce and manage vast volumes of sensitive data.

DOI: https://doi.org/10.36965/OJAKM.2024.12(2)40-58

Accepting Editor: Meir Russ

The number of connected IoT devices worldwide has been increasing since 2015, and it is projected that over 75 billion devices will be connected in 2025, as shown in Figure 1 (Adapted from Vailshery, 2023). Meneghello et al. (2019) also pointed out that the number and variety of IoT devices connected to the Internet will continue to rise. The increase in IoT devices will impact on network performance, security, and other factors. Proper planning for the increase and its effects in areas such as smart homes is imperative.

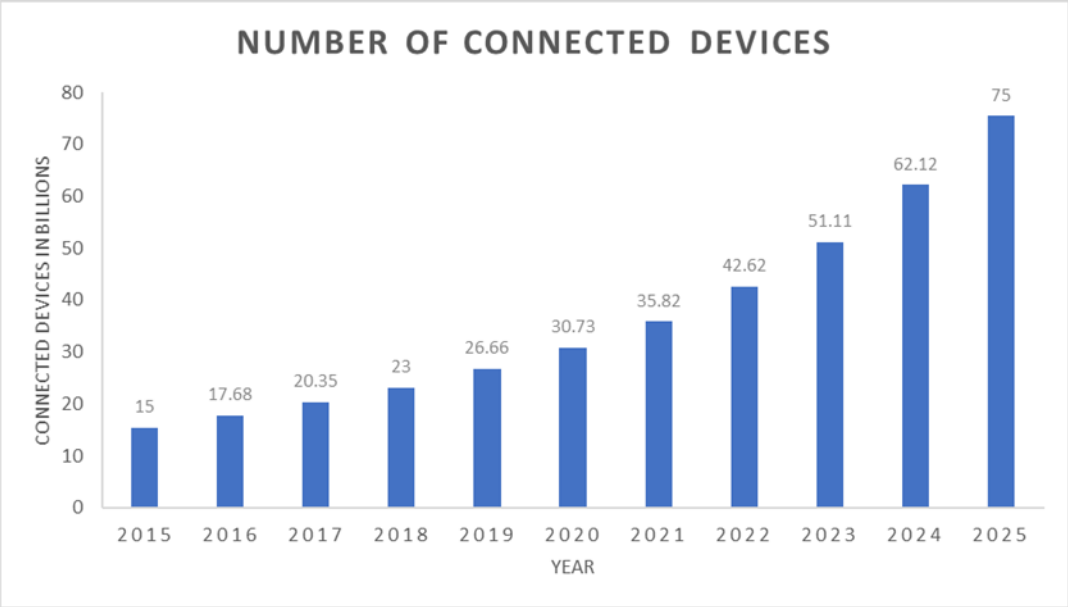

Figure 1. Connected IoT Devices (Adapted from Statista IoT).

The revenue generated by IoT devices worldwide has also increased since 2020, as shown in Figure 2 (Adapted from Vailshery, 2023).

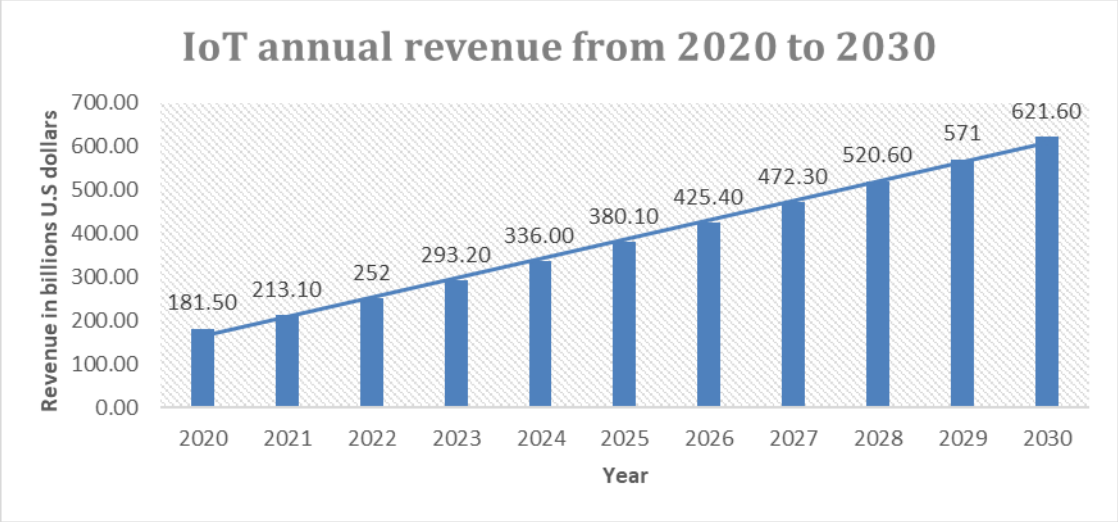

Figure 2. Annual revenue generated by IoT devices (Adapted from Statista IoT).

DOI: https://doi.org/10.36965/OJAKM.2024.12(2)40-58

Accepting Editor: Meir Russ

Girish et al. (2023) submitted that IoT devices are becoming increasingly pervasive in homes because of the advantages and services they provide to users. The number of users using IoT devices in smart homes worldwide has increased since 2019, as shown in Figure 3 (Adapted from Vailshery, 2023). Korneeva et al. (2021) performed a study in different countries and concluded that there is an increase in consumers preferring to have smart homes. Their data shows that more people are converting their homes to smart homes with IoT devices, increasing the need to develop security measures.

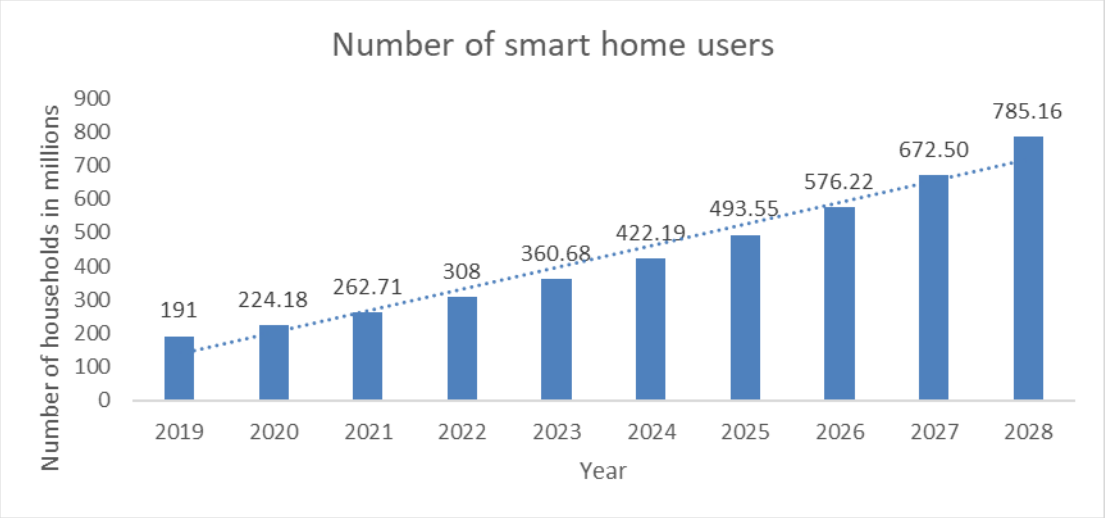

Figure 3. Number of smart home users (Adapted from Statista IoT).

Even though IoT devices have been widely used in different industries such as manufacturing, agriculture, transportation, education, and healthcare, the security of the devices continues to be a challenge. IoT devices have resource constraints due to limited memory, computational capacity, and power. Such constraints make it hard for traditional security mechanisms to adequately detect and protect IoT devices against attacks and compromises (Rathore & Park, 2018). Since IoT devices have Internet connectivity, they are constantly targeted by cyber attackers. IoT devices come with vulnerabilities that make them susceptible to security attacks, including spoofing attacks, Denial of Service (DoS) attacks, and replay attacks (Stergiou et al., 2018). The Open Web Application Security Project (OWASP) 2018 listed the following as the top 10 vulnerabilities of IoT devices:

1. Weak Guessable or Hardcoded Passwords
2. Insecure Network Services
3. Insecure Ecosystem Interfaces
4. Lack of Secure Update Mechanism
5. Use of Insecure or Outdated Components
6. Insufficient Privacy Protection
7. Insecure Data Transfer and Storage

DOI: https://doi.org/10.36965/OJAKM.2024.12(2)40-58

Accepting Editor: Meir Russ

8. Lack of Device Management
9. Insecure Default Settings
10. Lack of Physical Hardening

Recent advancements in IoT technologies have revolutionized smart home environments and delivered remarkable convenience and automation while simultaneously introducing critical security vulnerabilities (Chen et al., 2014; Poyner & Sherratt, 2018). Prior research underscores the increasing risks posed by network anomalies and intrusion attacks, coming from areas such as insecure communication protocols, heterogeneous device ecosystems, and data privacy concerns (Garg et al., 2020; Sarwar et al., 2023). Machine Learning (ML)-based anomaly detection frameworks have emerged as promising tools for mitigating these risks by identifying malicious activities in IoT networks (Chaabouni et al., 2019; Diro & Chilamkurti, 2018). Sarwar et al. (2023) highlighted the effectiveness of supervised learning models, including AdaBoost and Random Forest, in accurately detecting threats including keylogging, service scanning, and data exfiltration. Despite their potential, these approaches face critical limitations, including issues with data imbalance, high computational requirements, and challenges in generalizing emerging threats (Albulayhi et al., 2022; Hasan et al., 2019). This body of research highlights an urgent need for scalable, optimized, and interpretable solutions to bolster the security of IoT-enabled smart home systems.

The primary goal of this study is to identify and address the key security challenges associated with IoT devices in smart home environments. By analyzing existing literature and conducting experimental evaluations, the study aims to assess the effectiveness of network segmentation and ML-based intrusion detection systems in mitigating security risks such as privacy breaches, Denial-of-Service (DoS) attacks, and Man-In-The-Middle (MITM) attacks. This research seeks to provide actionable insights for enhancing IoT security frameworks and fostering a safer adoption of smart home technologies.

Theoretical Background

With the increased usage of IoT devices and the high number of security attacks targeting them, it is crucial to find solutions to secure the devices (Aldhaheri, 2024). Additionally, current security measures, including systemic security architectures and cryptographic security mechanisms, seem inadequate to address challenges with IoT devices. Choi et al. (2018) mentioned that IoT devices are threatened by a lack of authentication, console access, and internal access using vulnerable services such as Telnet. IoT devices have been the weakest link attackers can exploit to gain access to a network. Researchers and practitioners have deemed the security of IoT devices a top priority. Two approaches to securing IoT devices have been suggested: on-device security and network-based security (Husnain et al., 2022). On-device security includes username, password, hash keys, and any other security shields the manufacturer may have included. Network-based security provides security mechanisms that protect IoT devices from inbound attacks while controlling inbound and outbound communications with the device. As Husnain et al. (2022) pointed out, it is worth noting that traditional network defenses such as firewalls and intrusion detection systems have proved inadequate when securing IoT devices.

DOI: https://doi.org/10.36965/OJAKM.2024.12(2)40-58

Accepting Editor: Meir Russ

The security challenges of IoT devices in smart homes have been a focal point in recent studies, with researchers examining vulnerabilities across physical, network, software, and encryption categories. Davis et al. (2020) provided a detailed analysis of these vulnerabilities, highlighting critical issues such as hardware tampering, traffic analysis, outdated firmware, and weak encryption mechanisms. Prior research corroborates these findings, demonstrating the susceptibility of IoT devices to threats like man-in-the-middle attacks and DoS attacks (Andrea et al., 2015). Furthermore, studies have shown that well-known vendors often maintain stronger security postures due to greater regulatory scrutiny, while lesser-known manufacturers lack robust security practices and updates (Costa et al., 2019). Davis et al. contribute to this body of work by emphasizing the gaps in vulnerability coverage for lesser-known vendors in public databases like Common Vulnerabilities and Exposures (CVEs) and the National Vulnerability Database (NVD). Their findings underscore the need for standardized security protocols and more extensive research on IoT security to ensure safer smart home environments.

Girish et al. (2023) mentioned that even though security and privacy threats exist in home networks, the traffic analysis within the home network has been ignored in previous studies and literature. In their research, they collected data in a smart home. They analyzed it, revealing vulnerabilities in IoT devices, the use of insecure network protocols, and the exposure of sensitive data on IoT devices. This can result in the ease of exfiltration of information on smart homes to remote third parties. Their results of the information exfiltration can include financial loss. Moazzami et al. (2016) mentioned that smart home IoT ecosystems often consist of heterogeneous devices that utilize diverse protocols and standards, presenting challenges in ensuring unified security measures. According to Moazzami et al. (2016), heterogeneity in IoT devices complicates interoperability and security enforcement within smart home environments. Figure 4 shows a smart home's wireless and heterogeneity 15 IoT devices.

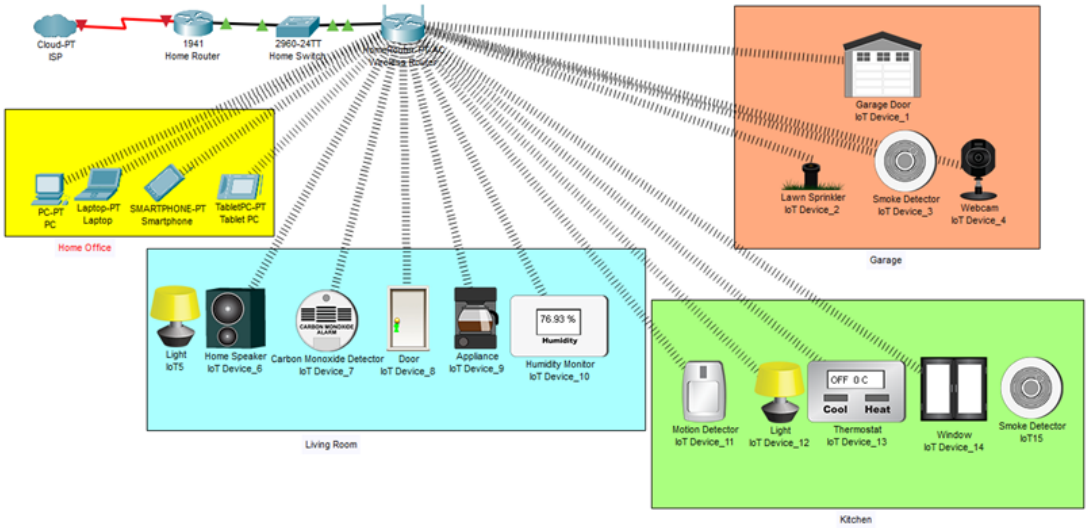

Figure 4. Smart home.

IDS have been used in network security because they can detect and monitor malicious actors (Aldhaheri, 2024). Liao et al. (2013) mentioned that an IDS is a software or hardware appliance

that monitors network traffic and then alerts the network administrator about the suspicious activities found. The IDS can be deployed as host-based when the software runs on the host and as network-based when the appliance runs on the network. IDSs use different detection methods which are (Anthi, 2022):

1. Signature-based, which observes network traffic to detect patterns and signatures of known attacks and abnormalities.
2. Anomaly-based, which raises an alert when the network behavior deviates from a known natural behavior.
3. Hybrid-based is a combination of signature-based and anomaly-based methods.

Rule-based IDSs have been successful in traditional networks; however, they have proven ineffective in detecting and blocking malicious activities in networks with IoT devices. Traditional IDS is insufficient in providing security to IoT systems because of IoT devices' characteristics of limited energy, ubiquitous, heterogeneity, and limited bandwidth capability (Ashraf et al., 2020). The complexities of IoT devices have made the intrusion detection system inefficient. ElKashlan (2023) performed a study that compared ML algorithms to evaluate the effectiveness of IDS in detecting cyberattacks in IoT devices used in electric vehicles. Additionally, Balaji et al. (2022) also conducted a study in which they used ML on a data set collected from IoT devices to examine the effectiveness of an IDS to detect anomalies. Incorporating machine learning (ML) and deep learning (DL) techniques into IDSs can improve their capability to detect network attacks in IoT-based networks. In this project, a secure hub ecosystem prototype with IDS, including ML, will be designed and implemented to defend IoT devices in a smart home.

Methodology

The goal of this proposed project was to design and implement a secure hub ecosystem prototype with an IDS, including ML, to defend IoT devices in a smart home. The following are the specific objectives:

1. Analyze the literature about the security of IoT in smart homes to identify the current challenges and limitations.
2. Evaluate and implement a prototype of a secure hub ecosystem to defend against heterogeneous IoT devices in smart home attacks.
3. Implement an IoT smart home testbed.
4. Evaluate and implement a supervised IDS with deep learning designed for IoT-based networks.

The above objectives correspond to the following Research Questions (RQ):

RQ1. What are the current challenges and limitations of the security of IoT devices in smart homes in literature?

RQ2. What security features can be incorporated in a smart home IoT hub with heterogeneous devices?

RQ3. What are the differences in the attack results without the IoT hub and when the hub was deployed?

RQ4. Can supervised ML IDS algorithms (classifiers) classify and identify attacks in IoT devices?

DOI: https://doi.org/10.36965/OJAKM.2024.12(2)40-58

Accepting Editor: Meir Russ

The hub ecosystem prototype, including the IoT smart home testbed, was set up and used in this study.

Data Collection

The following section explains specific data collection strategies:

RQ1. What are the current challenges and limitations of the security of IoT devices in smart homes in literature?

This study employs a Systematic Literature Review (SLR) to investigate the challenges and limitations of securing IoT devices within smart home environments. The methodology follows the framework proposed by Tranfield et al. (2003), consisting of three stages: planning the review, conducting the review, and synthesizing the findings. Initially, a comprehensive search strategy was devised to retrieve relevant studies from academic databases, including Computers & Applied Sciences Complete, ACM Digital Library, Scopus, and IEEE Xplore.

Article Selection Process

The search protocol focused on peer-reviewed articles published in the last five years to ensure the inclusion of up-to-date findings on IoT security in smart homes. Search terms included combinations of keywords such as "IoT security," "smart home," "cybersecurity," "intrusion detection systems," "machine learning," and "challenges." A total of 31 articles were identified during the initial search phase. To ensure relevance and quality, articles were screened based on their titles, abstracts, and full texts. This process resulted in the exclusion of studies that did not specifically address IoT security challenges or focused solely on other contexts outside smart homes. A set of 20 articles met the inclusion criteria and were selected for the final analysis. These articles were analyzed to extract insights into current challenges and limitations in IoT device security within smart homes.

Analysis and Synthesis

The selected studies were coded and categorized to identify recurring themes, challenges, and limitations in the literature. Key focus areas included issues such as resource constraints, device interoperability, privacy risks, susceptibility to cyberattacks, and evolving threat landscape. A qualitative synthesis was conducted to integrate findings and provide a comprehensive understanding of the identified challenges. These insights are intended to inform future research and practical applications in enhancing IoT security in smart home environments.

RQ2. What security features can be incorporated in a smart home IoT hub with heterogeneous devices?

In their study, Yu et al. (2015) addressed the escalating security challenges posed by the widespread deployment of IoT devices. They argued that traditional security measures, such as perimeter defenses, antivirus software, and vendor patching, are fundamentally inadequate for IoT ecosystems due to the scale, heterogeneity, and resource constraints of devices. They highlight vulnerabilities such as default credentials, unpatched firmware, and cross-device dependencies that create complex attack surfaces, particularly in smart home environments.

In their study, Davis et al. (2021) explored various network segmentation designs tailored to improve the security of IoT devices in smart home environments. The researchers analyze multiple segmentation frameworks, including micro-segmentation, segregated architectures, and smart segmentation frameworks, to address vulnerabilities stemming from heterogeneous IoT ecosystems. An IoT hub architecture with segmented IoT devices was used because of its capability to support authentication, confidentiality, access control, device cloaking, heterogeneity awareness, and monitoring attacker behaviors.

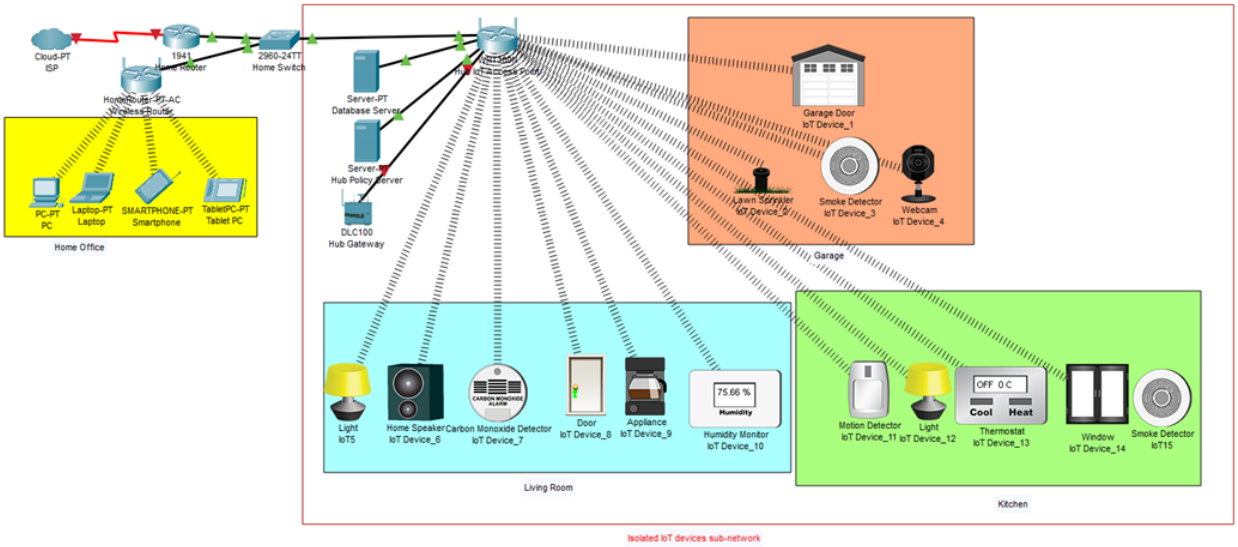

Figure 5. Proposed hub prototype.

The hub prototype was on an isolated network consisting of a separate access point to create a network segment with IoT devices, a hub gateway to handle authentication of IoT devices, and a hub policy server to ensure the requests comply with defined policies. The hub gateway handled authentication, and it was the only visible device to users outside of the network segment. To address the significant security challenges posed by resource-limited IoT devices, Canavese et al. (2024) introduced the IoT Proxy, a modular gateway designed to enhance IoT security by externalizing security functions from the devices to a centralized and secure network hub. Access Control Lists (ACL) were configured on the router to prevent devices on the hub from communicating with devices that were outside. The policy server was used to grant or reject requests. The hub prototype collected all data to and from the IoT devices only. Furthermore, the hub prototype was separated from the main home's access point. As shown in Figure 5, the proposed hub prototype with solutions to IoT device security challenges was configured and deployed.

RQ3. What are the differences in the attack results without the IoT hub and when the hub was deployed?

Baligodugula et al. (2024) emphasized the critical role of network segmentation in enhancing security within Industrial Internet of Things (IIoT) environments. They highlighted how segmentation mitigates risks posed by the heterogeneity of interconnected devices, which often

vary in security requirements and computational capabilities. As such, attacks from the IoT smart home testbed were performed first without the hub and when the hub was deployed. The hub provides micro-segmentation and Davis et al. (2021) mentioned that micro-segregation is a promising solution to reduce lateral attacks, isolating devices into functional groups that restrict unnecessary communication and minimize attack surfaces. A penetration test to the testbed was performed during the two scenarios mentioned above, and the data was collected and saved on the database server. Table 1 lists the IoT Devices that were used in the smart home testbed and the protocols used by each of the devices.

Table 1. IoT devices in the smart home testbed

IoT Device	Protocol(s)
Amazon Echo Dot (5th Gen)	Wi-Fi
Smart light	Wi-Fi
Smart switches	Wi-Fi
TP Link Camera	Wi-Fi
Smart TV	Wi-Fi
Samsung SmartThings Hub	Wi-Fi, Z-Wave Plus, Zigbee
Hive Smart plug	Wi-Fi
Echo Glow smart lamp	Bluetooth, Wi-Fi

RQ4. Can supervised ML IDS algorithms (classifiers) classify and identify attacks in IoT devices?

Anthi (2022) mentioned that supervised ML algorithms can effectively classify and identify attacks in IoT devices, making them a viable component of IDS solutions for securing smart homes and IoT networks. Supervised ML classifiers have shown promise as being effective in intrusion detection in IoT systems. Othman et al. (2018) proposed a machine learning-based intrusion detection model to classify and identify attacks in IoT environments involving the use of supervised learning algorithms, specifically Support Vector Machine (SVM), as the primary classifier. On the other hand, Shukla (2017) developed an IDS leveraging supervised and unsupervised machine learning techniques to detect wormhole attacks in IoT networks using a Decision Tree algorithm as the primary supervised classifier.

In this study, a supervised ML IDS using 10 classifiers was implemented to collect data from regular activities and a broad spectrum of attacks. IoT devices on the testbed were used to generate benign data. The activities included cameras detecting movement, the lights being turned on and off, and the home appliances being turned on. Two weeks of benign data were collected and saved on the server. Two weeks of malicious data were also collected. The attacks were systematically launched to generate and collect malicious data from the testbed. The IDS collected data in the categories of reconnaissance, DoS, and MITM. The IDS also collected logs with information such

as data, time, type, and variation of the attack detected. Additionally, the IDS collected data and classified it as benign or malicious.

Analysis

The data collected from the selected articles was extracted. A summary of the challenges and limitations of security in IoT devices in the last five years from the selected articles was compiled. The data collected from the hub was analyzed for the IoT device from which it originated. Packets were classified and recorded based on the IoT device from which they were detected. The data collected was analyzed to determine which IoT device generated the most packets. The data collected was analyzed based on which type of attack was most successful. The data collected from the IDS was analyzed based on the different matrixes. The confusion matrix for binary classification with the four counts of true positives, true negatives, false positives, and false negatives was used to determine if the data collected was accurate. Table 2 was used:

Table 2. Confusion matrix for binary classification

		Predicted	
		Benign	**Malicious**
Actual	**Benign**	True positive	False negative
	Malicious	False positive	True negative

The Waikato Environment for Knowledge Analysis (Weka) open-source tool kit widely used for analyzing machine learning algorithms was used (Patil & Burkpalli, 2021). The Weka ML algorithm performs classification experiments using the default hyper-parameters. The three measures that were used to analyze and evaluate the performance of a classifier or IDS algorithm are precision (P), recall (R), and F-measure (F). P measures if the proportion of malicious packet identification was correct, R measures what proportion of malicious packets were identified correctly, and F measures, which provides a single weighted metric to evaluate the overall classification performance.

Results

Current Challenges and Limitations in Literature

The 20 peer-reviewed articles were selected from different databases including ACM Digital, Computer & Applied Science, and IGI Global. Table 3 lists the most common challenges and limitations of the security of IoT devices in smart homes identified in the reviewed literature.

DOI: https://doi.org/10.36965/OJAKM.2024.12(2)40-58

Accepting Editor: Meir Russ

Table 3. Challenges and limitations

Challenges and limitations	No	References
Privacy Risks	10	(Alasmary & Tanveer, 2023; Aldhaheri et al, 2024; Asharf et al., 2020; Davis et al., 2020; Girish et al., 2023; Hu et al., 2023; Mahlous and Sultan, 2023; Nemec Zlatolas et al., 2022; Vojković et al., 2020)
Security Vulnerabilities and Risks	10	(Alasmary & Tanveer, 2023; Allifah & Zualkernan, 2022; Alsalman, 2024; Choi et al. 2018; Davis et al., 2020; Girish et al., 2023; Korneeva et al., 2021; Mahlous & Sultan, 2023; Meneghello et al., 2019; Vojković et al., 2020)
Complex and Evolving Threat Landscape	9	(Aldhaheri et al., 2024; Allifah & Zualkernan, 2022; Anthi et al., 2022; Asharf et al., 2020; Bhardwaj et al., 2023; Hu et al., 2023; Husnain et al., 2022; Rahim et al., 2023; Mahlous & Sultan, 2023)
Resource Constraints	7	(Aldhaheri et al., 2024; Alsalman, 2024; Alasmary & Tanveer, 2023; Anthi et al., 2022; Asharf et al., 2020; Husnain et al., 2022; Meneghello et al., 2019)
Inadequate or Absence of Security Standards	6	(Bhardwaj et al., 2023; Choi et al., 2018; Davis et al., 2020; Husnain et al., 2022; Mahlous & Sultan, 2023; Meneghello et al., 2019)
Heterogenous Networks	4	(Alasmary & Tanveer, 2023; Allifah & Zualkernan, 2022; Bhardwaj et al., 2023; Sarwar et al., 2023)
Challenges in Device Management and Update	3	(Davis et al., 2020; Hu et al., 2023; Meneghello et al., 2019)
Lack of Awareness and Education	3	(Nemec Zlatolas et al., 2022; Vojković et al., 2020; Mahlous & Sultan, 2023)
Insufficient Regulatory Framework	2	(Choi et al., 2018; Vojković et al., 2020)

The top two challenges and limitations in the reviewed articles were privacy risks and security vulnerabilities and risks. Privacy concerns are frequently mentioned with IoT devices collecting vast amounts of personal data (Alasmary & Tanveer, 2023; Aldhaheri et al., 2024; Asharf et al., 2020; Davis et al., 2020; Girish et al., 2023; Hu et al., 2023; Mahlous & Sultan, 2023; Nemec Zlatolas et al., 2022; Vojković et al., 2020). Managing and securing this data from unauthorized access or misuse is a major challenge. Numerous studies highlight technological vulnerabilities,

including weak encryption, outdated technology, and insecure communication protocols, which expose IoT devices to cyberattacks (Alasmary & Tanveer, 2023; Allifah & Zualkernan, 2022; Alsalman, 2024; Choi et al. 2018; Davis et al., 2020; Girish et al., 2023; Korneeva et al., 2021; Mahlous & Sultan, 2023; Meneghello et al., 2019; Vojković et al., 2020).

Nine articles emphasize the rapidly changing nature and complexity of cyber threats, which makes it difficult for IoT systems to adapt quickly and maintain effective security (Aldhaheri et al, 2024; Allifah & Zualkernan, 2022; Anthi et al., 2022; Asharf et al., 2020; Bhardwaj et al., 2023; Hu et al., 2023; Husnain et al., 2022; Rahim et al., 2023; Mahlous & Sultan, 2023). Resource constraints appear in multiple sources (Alasmary & Tanveer, 2023; Aldhaheri et al., 2024; Alsalman, 2024; Anthi et al., 2022; Asharf et al., 2020; Husnain et al., 2022; Meneghello et al., 2019). IoT devices often face limitations in processing power, memory, and energy resources, which make it difficult to implement robust security features and handle complex security tasks. Other challenges and limitations were inadequate or absence of security standards; heterogeneous networks; challenges in device management and update; lack of awareness and education; and insufficient regulatory framework. The absence of standardized security practices is mentioned, leading to inconsistent security measures across IoT devices and manufacturers, increasing the risk of vulnerabilities (Bhardwaj et al., 2023; Choi et al. 2018; Davis et al., 2020; Husnain et al., 2022; Mahlous & Sultan, 2023; Meneghello et al., 2019).

Attack Results

Table 4 provides a summary of the penetration test results before the hub was deployed and after the hub was deployed. Nmap was used to gather information about the network before it was segmented and as well as after the IoT devices were segmented into a hub. All the IoT devices were successfully detected before the hub was deployed, however, they were not detected after the deployment of the hub.

Table 4. Attack results

Attack	Method Used	Unsegmented IoT	IoT in a Hub
Device Detection	Nmap	Successful	Unsuccessful
DoS	Deauth, Mirai Botnet	Successful	Unsuccessful
MITM	Aircrack-ng, tcpdump	Successful	Unsuccessful

Deauth and Mirai Botnet were used to deploy DoS attacks. *Aircrack-ng* and *tcpdump* were used to intercept and analyze traffic within the network. Both DoS and MITM attacks to the IoT devices were successful when unsegmented and they were not successful when the IoT devices were behind the hub. The Internet Protocol (IP) and Media Access Control (MAC) addresses of the devices in the Home Network as shown in Figure 5 were visible in each of the attacks. On the other hand, the IP and MAC addresses of the IOT devices were only visible when the hub was not deployed.

DOI: https://doi.org/10.36965/OJAKM.2024.12(2)40-58
Accepting Editor: Meir Russ

Supervised ML IDS Algorithms

A desktop computer was connected to the network shown in Figure 5. Kali Linux was configured on the desktop computer. All the IoT devices in Table 1 were connected. Additionally, another desktop computer was used as a Syslog Server for the storage of log files. Two weeks of benign data and two weeks of malicious data from the IoT testbed were collected and saved on the Syslog Server. The data included using the SmartThings Hub, smart lights, camera, smart TV, and the Amazon Echo Dot

Table 5. Weighted average results

	Device Classification			Malicious Or Benign			Attack Type		
Classifier	**P**	**R**	**F**	**P**	**R**	**F**	**P**	**R**	**F**
Naïve Bayes	82.2	80.4	79.2	95.2	94.2	94.2	91.2	88.2	87.1
Bayesian Network	97.1	96.8	97.6	95.2	95.4	95.2	97.8	98.7	98.8
J48	97.4	97.2	96.8	99.7	99.8	99.9	98.4	98.8	98.7
Zero R	0.0	12.8	0.0	0.0	48.8	0.0	0.0	27.0	0.0
One R	91.2	82.2	83.4	93.4	92.2	92.4	98.8	96.8	97.5
Simple Logistic	94.2	93.7	93.4	97.5	96.8	97.1	98.6	99.4	98.4
SVM	93.5	94.2	93.4	96.2	96.4	97.5	99.3	99.5	99.1
Random Forest	97.2	97.2	97.1	99.8	99.7	99.7	98.7	97.9	98.3

Table 5 shows the weighted average results after cross-validation. Table 5 was used to report and select the best performance results from 8 IDS algorithms or classifiers listed. The performance comparison of various classifiers reveals that Random Forest and J48 are the most effective, consistently achieving precision, recall, and F1-scores above 97% across all categories, including device classification, benign activity detection, and attack type identification. Bayesian Network and Support Vector Machine (SVM) also demonstrate strong performance, particularly in attack detection, with metrics exceeding 95%. Simple Logistic and One R perform reliably, with metrics

DOI: https://doi.org/10.36965/OJAKM.2024.12(2)40-58
Accepting Editor: Meir Russ

in the range of 82-99%, showing slightly lower precision for device classification compared to other tasks. In contrast, Naïve Bayes delivers moderate performance, with scores around 80-90%, while Zero R is the weakest classifier, failing to detect patterns effectively and yield near-zero results. Overall, advanced classifiers like Random Forest and J48 are well-suited for robust IoT security due to their superior accuracy and consistency across all evaluation metrics.

Table 6 shows the packet results when classifying with devices that were used. The confusion matrix illustrates the performance of a classification model in identifying seven IoT device types. The model performs exceptionally well overall, with high true positive rates for most devices. Echo Dot, SmartThings Hub, Smart lamp, and TP Link Camera exhibit near-perfect classification, with over 99% accuracy and minimal misclassifications. Smart TV is also accurately classified, though 176 instances are mistakenly identified as Smart light. Smart light shows the highest misclassification, with 1,380 instances incorrectly predicted as Smart TV, suggesting a potential overlap in their features. Smart plug has strong performance but shows minor misclassifications as Smart lamp (88) and other devices. Despite some confusion between Smart light and Smart TV, the model demonstrates robust accuracy and effective discrimination across device categories.

Table 6. Confusion matrices classifying IoT devices

			Predicted						
			a	**b**	**c**	**d**	**e**	**f**	**g**
Actual	**Echo Dot**	**a**	9900	2	8	2	0	0	0
	Smart TV	**b**	2	9658	176	7	1	1	4
	Smart light	**c**	7	1380	8646	5	1	1	10
	SmartThings Hub	**d**	0	0	0	9840	0	2	16
	Smart lamp	**e**	2	0	0	2	9960	0	15
	Smart plug	**f**	2	4	0	4	0	9880	88
	TP Link Camera	**g**	1	2	0	0	0	0	9990

Table 7 shows the confusion matrix when classifying network traffic as either malicious or benign. The confusion matrix illustrates the performance of a classifier in distinguishing between malicious and benign network traffic. The model demonstrates exceptional accuracy, correctly classifying 38,868 malicious samples and 38,850 benign samples, with only 12 false negatives (malicious traffic misclassified as benign) and 18 false positives (benign traffic misclassified as malicious). This results in near-perfect precision and recall for both categories, indicating the classifier is highly effective in identifying malicious traffic while minimizing false alarms. The minimal misclassification rates highlight the model's robustness and reliability for network security applications.

DOI: https://doi.org/10.36965/OJAKM.2024.12(2)40-58

Accepting Editor: Meir Russ

Table 7. Confusion matrices classifying network traffic

			Predicted	
			a	b
Actual	Malicious	a	38,868	12
	Benign	b	18	38,850

Conclusions

This study's findings emphasize the role of knowledge management in improving IoT security frameworks through advanced technologies such as network segmentation and machine learning. Penetration testing results revealed the critical importance of employing a secure IoT hub for effective network segmentation. By isolating IoT devices and securing traffic, the hub mitigated attacks such as device detection, DoS, and MITM attacks, highlighting the vulnerabilities of unsegmented IoT networks. Supervised machine learning algorithms were integral to the study's knowledge-driven approach to IoT security. Models such as Random Forest and J48 classifiers demonstrated outstanding performance metrics, with precision, recall, and F1-scores consistently exceeding 97%. These algorithms effectively classified IoT devices, detected malicious activities, and identified benign traffic. Conversely, simpler models like Naïve Bayes and Zero R struggled to handle the complexity of IoT data, reinforcing the need for sophisticated algorithms to manage knowledge and data patterns in dynamic IoT environments. Confusion matrix analyses validated these models' efficacy, achieving near-perfect classification accuracy for both device types and network traffic. Such precise identification underscores the potential for machine learning to integrate into comprehensive IoT security frameworks, ensuring robust defenses against emerging threats.

Recommendations and Future Work

From a knowledge management perspective, the study suggests prioritizing user education to enhance awareness of IoT security. The integration of network segmentation and advanced machine learning solutions requires a strong foundation of user understanding to maximize their effectiveness. Moreover, fostering a culture of proactive knowledge sharing among stakeholders, including developers, users, and policymakers, can drive innovation and adaptability in IoT security practices. Future research should explore the scalability of these solutions in larger IoT ecosystems and investigate the integration of real-time threat detection mechanisms with knowledge repositories. Furthermore, addressing the cost implications of deploying such advanced systems will be crucial for widespread adoption. In conclusion, this research highlights the synergistic role of knowledge management, network segmentation, and machine learning in addressing IoT security challenges. By leveraging these approaches, organizations can significantly enhance their resilience against cyber threats and contribute to the evolving landscape of smart home security.

DOI: https://doi.org/10.36965/OJAKM.2024.12(2)40-58

Accepting Editor: Meir Russ

Acknowledgment

The author would like to thank the anonymous referees for their careful review and valuable suggestions.

References

Albulayhi, K., Abu Al-Haija, Q., Alsuhibany, S. A., Jillepalli, A. A., Ashrafuzzaman, M., & Sheldon, F. T. (2022). IoT intrusion detection using machine learning with a novel high-performing feature selection method. *Applied Sciences, 12*(10), 5015. https://doi.org/10.3390/app12105015

Aldhaheri, A., Alwahedi, F., Ferrag, M. A., & Battah, A. (2024). Deep learning for cyber threat detection in IoT networks: A review. *Internet of Things and Cyber-Physical Systems, 4,* 110–128. https://doi.org/10.1016/j.iotcps.2023.09.003

Allifah, N. M., & Zualkernan, I. A. (2022). Ranking security of IoT-based smart home consumer devices. *IEEE Access*, *10*, 18352–18369. https://doi.org/10.1109/ACCESS.2022.3148140

Alsalman, D. (2024). A comparative study of anomaly detection techniques for IoT security using adaptive machine learning for IoT threats. *IEEE Access, 12*, 12345–12356. https://doi.org/10.1109/ACCESS.2024.1234567

Alasmary, H., & Tanveer, M. (2023). ESCI-AKA: Enabling secure communication in an IoT-enabled smart home environment using authenticated key agreement framework. *Mathematics (Basel), 11*(16), 3450-. https://doi.org/10.3390/math11163450

Andrea, I., Chrysostomou, C., & Hadjichristofi, G. C. (2015). Internet of Things: Security vulnerabilities and challenges. *Proceedings of the IEEE Symposium on Computers and Communication (ISCC)* (pp. 180–187). https://doi.org/10.1109/ISCC.2015.7405513

Anthi, E. (2022). *Detecting and defending against cyber attacks in a smart home internet of things ecosystem (dissertation).* Cardiff University, Wales, United Kingdom.

Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., & Wahab, A. (2020). A review of intrusion detection systems using machine and deep learning in Internet of Things: Challenges, solutions, and future directions. *Electronics, 9*(7), Article 1177. https://doi.org/10.3390/electronics9071177

Balaji, R., Deepajothi, S., Prabaharan, G., Daniya, T., Karthikeyan, P., & Velliangiri, S. (2022). Survey on intrusions detection system using Deep Learning in IOT Environment. *Proceedings of the 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*. https://doi.org/10.1109/icscds53736.2022.9760993

Baligodugula, V. V., Ghimire, A., & Amsaad, F. (2024). An overview of secure network segmentation in connected IIoT environments. *Computing & AI Connect, 1*, Article 2024.004. https://doi.org/10.69709/CAIC.2024.193182

Bhardwaj, A., Kaushik, K., Alshehri, M., Mohamed, A. A.-B., & Keshta, I. (2023). ISF: Security analysis and assessment of smart home IoT-based firmware. *ACM Transactions on Sensor Networks*. https://doi.org/10.1145/3578363

Canavese, D., Mannella, L., Regano, L., & Basile, C. (2024). Security at the edge for resource-limited IoT devices. *Sensors, 24*(2), Article 590. https://doi.org/10.3390/s24020590

Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network intrusion detection for IoT security based on learning techniques. *IEEE Communications Surveys & Tutorials, 21*(3), 2671–2701. https://doi.org/10.1109/COMST.2019.2896380

Chen, S., Xu, H., Liu, D., Hu, B., & Wang, H. (2014). A vision of IoT: Applications, challenges, and opportunities with China perspective. *IEEE Internet of Things Journal, 1*(4), 349–359. https://doi.org/10.1109/JIOT.2014.2337336

Choi, S.-K., Yang, C.-H., & Kwak, J. (2018). System hardening and security monitoring for IoT devices to mitigate IoT security vulnerabilities and threats. *KSII Transactions on Internet and Information Systems, 12*(2), 906–918.

Costa, L., Barros, J., & Tavares, M. (2019). Vulnerabilities in IoT devices for smart home environment. *Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP).*

Davis, B. D., Mason, J. C., & Anwar, M. (2020). Vulnerability studies and security postures of IoT devices: A smart home case study. *IEEE Internet of Things Journal, 7*(10), 10102–10110. https://doi.org/10.1109/JIOT.2020.2983983

Davis, T., Wang, M., Zavarella, T., & Zhang, M. (2021). Analysis and extension of home IoT network segmentation architectures. *MIT Technical Report*. https://courses.csail.mit.edu

Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems, 82*, 761–768. https://doi.org/10.1016/j.future.2017.08.043

ElKashlan, M., Elsayed, M. S., Jurcut, A. D., & Azer, M. (2023). A machine learning-based intrusion detection system for IoT electric vehicle charging stations (EVCSs). *Electronics (Basel)*, *12*(4), 1044-. https://doi.org/10.3390/electronics12041044

Garg, S., Kaur, K., Kaddoum, G., & Choo, K. R. (2020). Toward secure and provable authentication for Internet of Things: Realizing Industry 4.0. *IEEE Internet of Things Journal, 7*(5), 4598–4606. https://doi.org/10.1109/JIOT.2020.2976702

Girish, A., Hu, T., Prakash, V., Dubois, D. J., Matic, S., Huang, D. Y., Egelman, S. et al. (2023). In the room where it happens: Characterizing local communication and threats in Smart Homes. *Proceedings of the 2023 ACM on Internet Measurement Conference*. https://doi.org/10.1145/3618257.3624830

Hu, T., Dubois, D. J., & Choffnes, D. (2023). BehavIoT: Measuring smart home IoT behavior using network-inferred behavior models. *Proceedings of the 2023 ACM Internet Measurement Conference (IMC '23)*, Montreal, QC, Canada. https://doi.org/10.1145/3618257.3624829

Husnain, M., Hayat, K., Cambiaso, E., Fayyaz, U. U., Mongelli, M., Akram, H., Ghazanfar Abbas, S., & Shah, G. A. (2022). Preventing MQTT vulnerabilities using IoT-enabled intrusion detection system. *Sensors (Basel, Switzerland), 22*(2), 567-. https://doi.org/10.3390/s22020567

Hussain, F., Abbas, S. G., Shah, G. A., Pires, I. M., Fayyaz, U. U., Shahzad, F., Garcia, N. M., & Zdravevski, E. (2021). A framework for malicious traffic detection in IoT healthcare environment. *Sensors (Basel, Switzerland), 21*(9), 3025. https://doi.org/10.3390/s21093025

Korneeva, E., Olinder, N., & Strielkowski, W. (2021). *Consumer Attitudes to the smart home technologies and the Internet of Things (IoT).* Energies (Basel), 14(23), 7913-. https://doi.org/10.3390/en14237913

Liao, H.-J., Richard Lin, C.-H., Lin, Y.-C., & Tung, K.-Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications, 36*(1), 16–24. https://doi.org/10.1016/j.jnca.2012.09.004

Mahlous, A. R., & Sultan, P. (2023). Threat model and risk management for a smart home IoT system. *Informatica, 47*(1), 51–64. https://doi.org/10.31449/inf.v47i1.4526

Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet of Things Journal, 6*(5), 8182–8201. https://doi.org/10.1109/JIOT.2019.2935189

Moazzami, M.-M., Mashima, D., Herberg, U., Chen, W.-P., & Xing, G. (2016). SPOT: a smartphone-based control app with a device-agnostic and adaptive user-interface for IoT devices. *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, 670–673. https://doi.org/10.1145/2968219.2968345

Nemec Zlatolas, L., Feher, N., & Hölbl, M. (2022). Security perception of IoT devices in smart homes. *Journal of Cybersecurity and Privacy, 2*(1), 65–74. https://doi.org/10.3390/jcp2010005

Owasp Internet of Things Project (OWASP) (n.d.). https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10

Patil, B. M., & Burkpalli, V. (2021). A perspective view of cotton leaf image classification using machine learning algorithms using WEKA. *Advances in Human-Computer Interaction*, *2021*, 1–15. https://doi.org/10.1155/2021/9367778

Poyner, I. K., & Sherratt, R. S. (2018). Privacy and security of consumer IoT devices for the pervasive monitoring of vulnerable people. *Proceedings of the Living Internet of Things: Cybersecurity of IoT* (pp. 1–5). https://doi.org/10.1049/cp.2018.0030

Sarwar, N., Bajwa, I. S., Hussain, M. Z., Ibrahim, M., & Saleem, K. (2023). IoT network anomaly detection in smart homes using machine learning. *IEEE Access*, *11*, 119462–119480. https://doi.org/10.1109/ACCESS.2023.3325929

Shafiq, M., Gu, Z., Cheikhrouhou, O., Alhakami, W., & Hamam, H. (2022). The rise of "Internet of Things": Review and open research issues related to detection and prevention of IoT-

based security attacks. *Wireless Communications and Mobile Computing, 2022*, 1–12. https://doi.org/10.1155/2022/8669348

Statista Internet of things: The number of connected devices worldwide 2012-2025. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Stergiou, C., Psannis, K.E., Kim, B.G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems. 78*, 964–975.

Rahim, A., Zhong, Y., Ahmad, T., Ahmad, S., Pławiak, P., & Hammad, M. (2023). Enhancing smart home security: Anomaly detection and face recognition in smart home IoT devices using logit-boosted CNN models. *Sensors, 23*(15), 6979. https://doi.org/10.3390/s23156979

Rathore, S., & Park, J. H. (2018). Semi-supervised learning-based distributed attack detection framework for IoT. *Applied Soft Computing, 72,* 79–89. https://doi.org/10.1016/j.asoc.2018.07.033

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management, 14*(3), 207–222. https://doi.org/10.1111/1467-8551.00375

Vailshery, L. S. (2023, July 27). IOT connected devices by vertical 2030. Statista. https://www.statista.com/statistics/1194682/iot-connected-devices-vertically/

Vojković, G., Milenković, M., & Katulić, T. (2020). IoT and smart home data breach risks from the perspective of data protection and information security law. *Business Systems Research Journal, 11*(3), 124–135. https://doi.org/10.2478/bsrj-2020-003

Yu, T., Sekar, V., Seshan, S., Agarwal, Y., & Xu, C. (2015). Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things. *Proceedings of the 14th ACM Workshop on Hot Topics in Networks*, 1–7. https://doi.org/10.1145/2834050.2834095

Author Biography

Stephen Mujeye, Ph.D. is an assistant professor of computer systems technology at Illinois State University, Normal, Illinois. He earned a bachelor's degree with a double major in business management and business systems support specialist from Siena Heights University, Adrian, Michigan. He has a master's degree in information resource management from Central Michigan University, Mt. Pleasant, Michigan. He completed his Ph.D. in Information Systems from Nova Southeastern University. His Ph.D. dissertation was titled "An Experimental Study on the Role of Password Strength and Cognitive Load on Employee Productivity." He holds several industry certifications, including A+, Network+, CCNA, and CCNA Security. His areas of research interest are authentication methods, cyber security, mobile, and network security.