information

Review

Towards Securing Smart Homes: A Systematic Literature Review of Malware Detection Techniques and Recommended Prevention Approach

Omar Alshamsi *, Khaled Shaalan and Usman Butt

Faculty of Engineering and IT, British University in Dubai, Dubai 345015, United Arab Emirates; khaled.shaalan@buid.ac.ae (K.S.); usman.butt@buid.ac.ae (U.B.)
* Correspondence: 21001267@student.buid.ac.ae

Abstract: The exponential growth of the Internet of Things (IoT) sector has resulted in a surge of interconnected gadgets in smart households, thus exposing them to new cyber-attack susceptibilities. This systematic literature review investigates machine learning methodologies for detecting malware in smart homes, with a specific emphasis on identifying common threats such as denial-of-service attacks, phishing efforts, and zero-day vulnerabilities. By examining 56 publications published from 2019 to 2023, this analysis uncovers that users are the weakest link and that there is a possibility of attackers disrupting home automation systems, stealing confidential information, or causing physical harm. Machine learning approaches, namely, deep learning and ensemble approaches, are emerging as effective tools for detecting malware. In addition, this analysis highlights prevention techniques, such as early threat detection systems, intrusion detection systems, and robust authentication procedures, as crucial measures for improving smart home security. This study offers significant insights for academics and practitioners aiming to protect smart home settings from growing cybersecurity threats by summarizing the existing knowledge.

Keywords: machine learning; IoT; smart homes; malware; artificial intelligence

check for updates

Citation: Alshamsi, O.; Shaalan, K.; Butt, U. Towards Securing Smart Homes: A Systematic Literature Review of Malware Detection Techniques and Recommended Prevention Approach. *Information* **2024**, *15*, 631. https://doi.org/10.3390/info15100631

Academic Editors: Shareeful Islam, Stefano Silvestri, Zia Ush Shamszaman and Xiaokun Zhang

Received: 20 September 2024
Revised: 8 October 2024
Accepted: 10 October 2024
Published: 13 October 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The Internet of Things (IoT) industry is seeing tremendous expansion with a significant increase in networked devices and the creation of new applications in several industries. IoT is a solution that allows individuals and objects to be connected continuously and universally, utilizing any network or service [1]. It was initially used to automate individual houses for enhanced comfort and convenience and is now being expanded to develop Smart Cities. A smart network functions as a digital nervous system, linking devices to facilitate data interchange, hence enhancing automation in settings ranging from homes to huge cities [2]. According to Dell, the International Data Corporation estimates that by 2025, 41.6 billion Internet of Things devices will be operational, with the capacity to produce 79.4 zettabytes of data [3]. The present increase in home automation extends beyond simple convenience. Smart homes can enhance energy efficiency and reduce utility costs by automating functions such as lighting, temperature regulation, and security systems. Moreover, functions such as remote access and automated scheduling contribute to enhanced peace of mind and a more tailored living experience. The scope of this paper will cover smart homes because smart homes have a substantial impact on sustainability as they improve energy efficiency, support environmental cleanliness, and contribute to the advancement of intelligent and sustainable communities. These technologies provide advantages such as enhanced comfort, a variety of energy sources, and housing options that are accessible to all [4]. Sustainable Development Goal 11 focuses on sustainable cities and communities, striving to establish urban environments that are safe, resilient, and sustainable. Smart houses, as essential elements of urban ecosystems, are crucial in attaining

these goals. Smart houses immediately facilitate the achievement of SDG 11 by improving energy efficiency and reducing greenhouse gas emissions. Moreover, their proven capacity to preserve power and water corresponds with the overarching sustainability objectives of urban development, underscoring their importance in the establishment of sustainable cities and communities. However, smart homes can be a potential risk to the privacy and security of data. According to the authors of [5], the attacks on smart homes are growing. As new security flaws emerge, the ecosystem becomes increasingly unstable and susceptible. In addition, human beings are widely recognized as the most vulnerable aspect of cybersecurity.

To answer the research questions proposed, and based on smart home security, a systematic literature review was performed via the application of the PRISMA method. This approach is a rigorous one as it allows for the systematic and transparent identification, selection, evaluation, and synthesis of the relevant literature. It is designed to provide researchers with a complete methodology for obtaining primary studies in this field. This systematic literature review aimed to identify and analyze the existing research related to malware detection techniques in smart homes, to determine the different types of cyber threats that affect smart homes, and to examine the efficiency of the detected malware methods, also shedding light on the work issues that were not previously addressed in order to provide some recommendations for improving smart homes. This study is expected to make significant contributions in the field of smart home security by presenting a holistic view of existing malware detection techniques and their effectiveness, identifying common cyber threats in smart homes so that focused prevention strategies can be developed, determining research gaps, and suggesting future research directions.

In this research, we review the current literature available on the detection of malware in smart homes to accomplish the following:

- To systematically identify the common threats on smart homes;
- To analyze the methods used to detect these threats.

The findings of this research should assist in the following:

- Providing an in-depth understanding of the current machine learning methods used to detect malware in smart home environments;
- Supporting researchers in developing user-centric preventive measures, as users are often considered the weakest link in cyber security;
- Encouraging researchers to dedicate their efforts to improving the security of smart homes and actively contributing to the United Nations' Sustainable Development Goal 11 in order to promote global sustainability.

This article is organized as follows: the introduction will provide an overview and discuss the importance of this study, and the problem statement will follow; the methodology section will outline the research strategy and then give the outcomes; the discussion section will explore the findings in more detail; and the conclusion section will summarize the main points.

2. Problem Statement

With the continuous advancement of technology, home automation is set to have a significant impact on the future of comfortable and efficient living. However, IoT systems are struggling to cope with emerging security threats. Attackers are employing more diverse methods to breach security systems. In 2022, a survey was conducted [6], and the authors found that 40.3% of smart homes globally had five or more internet-connected gadgets, and 40.8% of households had at least one susceptible item that poses a danger to the whole home. The extensive data gathered by IoT devices pose significant privacy issues due to the collection of personal information, behavioral patterns, and sensitive data from individuals. The authors of [7] stated that the human factor is widely acknowledged as the most vulnerable aspect of information security, especially in relation to emerging technologies such as the IoT. Despite technological advancements, organizations still face data breaches,

underscoring the crucial influence of human factors in security incidents [7]. Smart home technologies are using Artificial Intelligence (AI) to improve energy efficiency and user experience. AI models have the potential to enhance house design, optimize energy usage, and automate a range of functions. AI has greatly enhanced the usability, convenience, and environmental sustainability of smart homes, leading to a significant improvement in quality of life [8]. However, smart homes are vulnerable to several cybersecurity risks, especially when humans interact with AI and IoT technologies. Typical security risks, such as DDoS assaults, can be identified by the use of machine learning models and can be mitigated using secure user authorization methods [8].

Smart Home Networks (SHN) face wide-ranging cybersecurity threats, where malware attacks are one of the common threats that pose a substantial risk to the security and privacy of these networked devices. Malware developers have recently shown a growing interest in IoT devices. For instance, the Mirai, Bashlite, and Silex viruses specifically targeted IoT and smart home devices [9]. Malicious software on SHNs can manifest in different forms to cause disruption, harm, or unauthorized access. Malware encompasses viruses, adware, Trojan horses, spyware, and other harmful software that can damage computers and online devices. During a malware attack, the hacker can break into the network and gain full control without detection. According to the authors of [10], human error continues to play a major role in the success of cyberattacks. Effective smart home security relies on the essential cooperation between homeowners, device makers, and internet service providers. With the ongoing expansion of the IoT ecosystem, it is crucial to prioritize the resolution of these cybersecurity concerns to protect the privacy and data of users. Machine learning (ML) is a widely used method for creating malware detection solutions. It has demonstrated promising outcomes by learning common patterns to detect new and unknown viruses. Malware detection utilizes two primary methodologies: static analysis, which scrutinizes the code of applications; and dynamic analysis, which observes the behavior of malware. Static analysis is characterized by its speed, but it is prone to being compromised by obfuscation techniques. On the other hand, dynamic analysis is more resilient, but it requires significant processing resources and is sensitive to anti-analysis methods [11].

The findings of this analysis report that the successful execution of malware is due to the result of humans as the weakest link and requires to be addressed by implementing solutions such as two-factor authentication systems. Dynamic analysis approaches have shown higher effectiveness in comparison to static analysis. Decision-tree-based algorithms, namely, random forests, have achieved detection accuracies of up to 95.95% [12]. Users are the weakest factor in cybersecurity, often unintentionally enabling the infiltration of malware into networks. Although there have been significant breakthroughs, it is important to note that no one method can identify all types of malwares. This emphasizes the need for ongoing study and development in the area of malware detection. Deep learning is a prevalent machine learning technique to detect malware, and it utilizes Artificial Neural Networks (ANNs) consisting of multiple layers of artificial neurons. The weights of these neurons are adjusted iteratively to achieve the desired output [13]. This review will highlight the common machine learning approaches to detect malware in smart homes through contemporary articles from different databases. The goal of this systematic literature review is to gather a comprehensive understanding of the prevalent cyber dangers, which are mostly caused by users' mistakes because they are the weakest link in the environment, as well as the most recent techniques used for detecting these threats. Additionally, this research aims to provide recommended solutions for enhancing the security of smart homes. Therefore, the following research questions have been formulated to achieve our goal.

- RQ1: What are the common cyber threats that target smart homes?

  Answering the first question will highlight the most reported cyber threats to smart homes.
- RQ2: What methods are applied in malware detection in smart homes?

Answering the second question will identify the latest methods used in malware detection in smart homes.

- RQ3: How can smart home security be improved?

Answering the third question will cover recommended solutions to improve smart home security.

3. Research Method

A critical literature review is a crucial step that precedes any research study. It lays the foundation for accumulating knowledge, facilitating the expansion and advancement of theories, addressing research gaps, and identifying areas overlooked in previous studies. A literature review is considered a systematic literature review when it is conducted with stated research objectives, identifies and analyzes relevant research articles, and assesses their quality using specific criteria. This review is an example of evidence-based research, which is conducted in five phases:

- Selection of inclusion and exclusion criteria;
- Search terms and data sources;
- PRISMA flow diagram;
- Bias;
- Data analysis and coding strategy.

All these sections are thoroughly explained in the following subsections.

3.1. Inclusion and Exclusion Criteria

A systematic literature review (SLR) relies on a clearly defined set of criteria to identify relevant and high-quality research. This section highlights the inclusion and exclusion criteria as listed in Table 1 and it was developed to ensure that only high-quality articles are included in this work.

Table 1. Inclusion and exclusion criteria.

Inclusion	Exclusion
The paper should focus on the machine learning approach to detect an anomaly.	Papers that do not focus on machine learning approaches to detect anomalies.
The paper should focus on smart homes or IoT environments.	Papers that are not in the context of smart homes or IoT.
Papers published from 2019 to 2023.	Papers that do not fall within the range of specified publication years.
The paper should be written in English.	Papers written in languages other than English.

3.2. Search Terms and Data Sources

A detailed and thorough study of existing research was conducted using a multidimensional search method. This section outlines the comprehensive data sources used to find pertinent and high-caliber research. A mix of reputable academic databases and a generic academic search engine has been chosen to encompass a wide range of studies on this topic. The included databases are

- Emerald;
- Science Direct;
- Taylor and Francis;
- ProQuest;
- IEEE explore.

These databases have been chosen based on the relevancy of the research topic and the suitability of the keywords. The review will use Boolean operators (AND, OR) strategically to narrow the search and select relevant papers. The specified search terms are “machine learning” AND “malware” AND “smart home” OR “home automation”.

3.3. PRISMA Flow Diagram

This review utilized systematic and explicit methods to identify, select, and critically appraise relevant research. Statistical techniques were employed to integrate the results of included studies in a systematic review like PRISMA (Reporting Items for Systematic Reviews and Meta-Analyses). The PRISMA framework is universally acknowledged as a crucial instrument for carrying out systematic literature reviews in several disciplines [14]. The technique offers a systematic methodology for searching, selecting, and analyzing relevant papers. PRISMA improves the clarity and consistency of reviews by providing a defined process and criteria for reporting. PRISMA is considered to be of great importance by researchers, with an average ranking of 8.66 out of 10 for its overall relevance. PRISMA facilitates the identification of research gaps, the categorization of results, and the proposal of future research orientations [15]. The fact that it is widely used in many areas highlights its significance in consolidating and progressing knowledge across disciplines. The framework guidelines of this SLR are depicted in Figure 1.

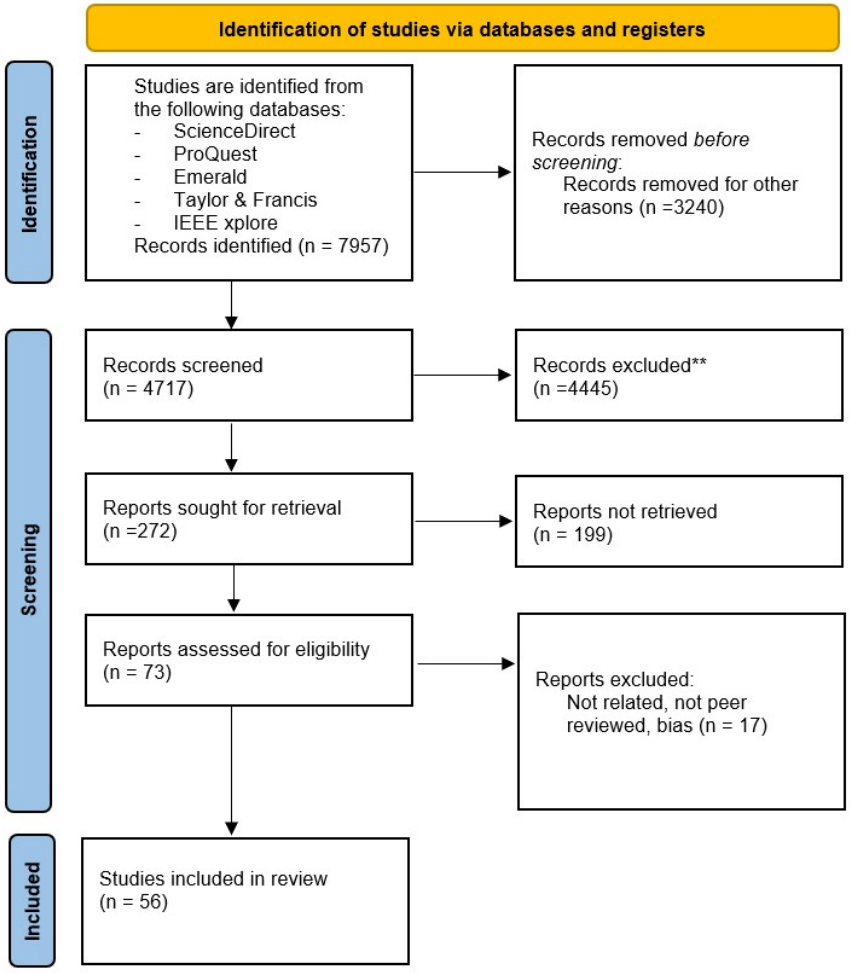


Figure 1. PRISMA framework.

3.4. Bias

Bias in research refers to systematic mistakes that have the potential to result in inaccurate or deceptive results. It may manifest at any point in the research process, ranging from the development of the study design to the final publication. Although study bias is generally detrimental, researcher bias may sometimes be advantageous when well-controlled [16]. The presence of bias in research is a significant issue as it may lead to the production of erroneous results, which, in turn, might influence the development of detrimental policies and practices. To reduce bias, researchers should use stringent method-

ologies, guarantee transparency, and employ peer review and replication. Augmenting the sample size may effectively mitigate random mistakes; however, addressing systematic bias poses a more formidable challenge. Researchers must possess knowledge of many forms of bias, including selection bias, operator bias, and publication bias, and make deliberate efforts to reduce their impact via proper research design and analysis. Controlling bias is essential for ensuring the accuracy and replicability of research. There were total of 17 papers which were excluded. This was mainly due to the fact that these papers were either not peer reviewed, lack references, or are not related to the research topic, and one of the papers was identified as biased.

3.5. Data Analysis and Coding Strategy

Thematic analysis is a research technique that involves coding data to uncover ideas, meaning, and knowledge. Thematic analysis is a technique used to examine qualitative data. The process entails recognizing and documenting patterns within a dataset, which are subsequently analyzed for their underlying significance [17]. To begin a thematic analysis, we thoroughly analyzed the data. This entails the organization and classification of information from the provided articles. Initial codes are formed by finding repeating patterns within the data. The codes are then categorized into overarching themes, facilitating a significant presentation of the results. Ultimately, these results are related to the initial research questions. Analyzing data with precision is essential to comprehending how machine learning can effectively identify malware in smart homes. In this research, a hybrid coding approach was implemented, which combines inductive and deductive methodologies, providing an effective tool for this research. Inductive coding facilitates the immediate discovery of themes and patterns from the examined papers. This methodology starts at the very beginning and may reveal new machine learning methods optimized for the various difficulties found in smart home settings. It is beneficial to recognize new data sources used for training models or advanced algorithms specialized in identifying malware that targets smart devices. Deductive coding uses predefined categories based on prior research using the search strategy keywords used in this review. This hierarchical method offers a systematic framework for examination. The studies classify machine learning techniques based on existing frameworks to facilitate comparisons and identify gaps in current approaches [18].

4. Results

The output of the systematic process resulted in 56 articles in total. In Figure 2, the papers are depicted according to their categories, which include journals and conferences. A total of 42 out of 56 articles were published in journals, while 14 out of 56 articles were published in conferences. This review analyzed papers published between 2019 and 2023. Also, the figure below displays a timeline graph, illustrating the yearly distribution of published publications from 2019 to 2023. The number of published articles remained consistent in 2019 and 2021, with a minor rise observed in 2020. There is a significant rise in the publication of articles relating to malware detection for IoT settings in 2022 and 2023, indicating a notable concentration on this topic.

The comparative analysis listed in Table 2 includes the summary of research papers related to IoT malware detection using machine learning approaches. Authors used different machine learning algorithms, such as anomaly-based, ensemble learning, deep learning, and hierarchical ensemble adversarial learning, to detect various types of malwares in Smart Homes, IoT Networks, and different types of IoT applications. Some potential benefits are that these approaches are lightweight, provide high accuracy with robustness against polymorphic or masked malware, and are successful in detecting malicious malware. On the other hand, they have some limitations, including assuming training phase or requesting context. These approaches rely on the quality of the dataset for the training mode, have a complex computational process, and lack practical deployment. In general,

this categorization reveals that machine learning techniques are promising in enhancing security in IoT against malware.

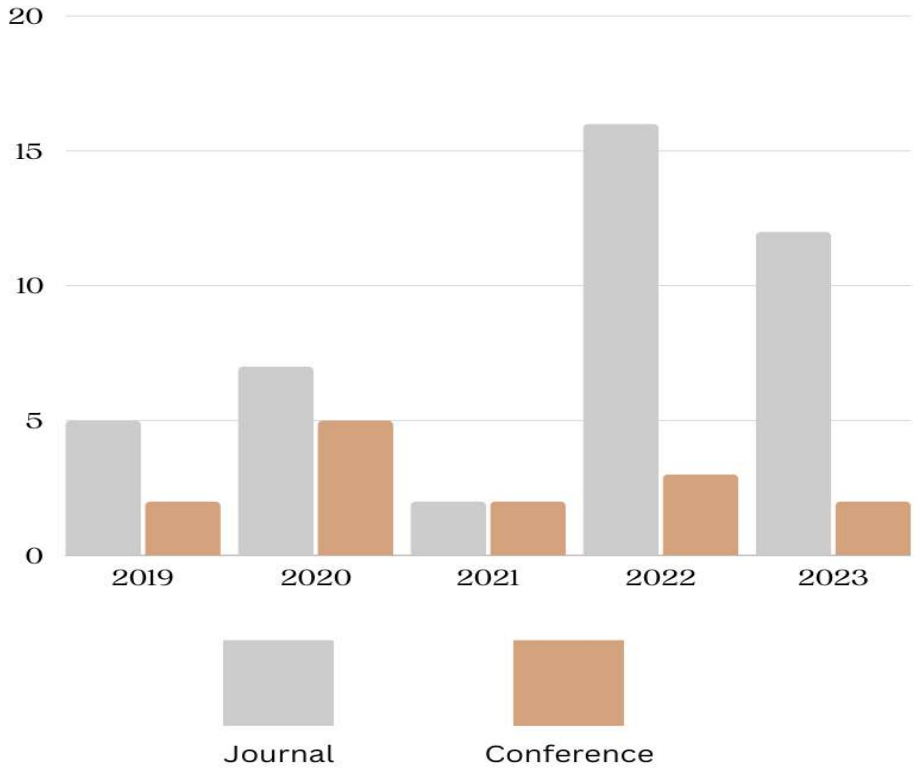


Figure 2. Timeline categorization of articles.

Table 2. Comparative analysis.

Author	Year	Technique	Environment	Advantage	Disadvantage
[19]	2021	An efficient spam detection technique using machine learning	Smart home environments	The proposed approach effectively detects spam parameters affecting IoT devices	Quality of the dataset and the need for continuous updates to the detection algorithms
[20]	2019	This paper proposes an ensemble intrusion detection technique using the AdaBoost ensemble learning method	IoT environment	The proposed technique effectively identifies malicious events by utilizing a set of features derived from MQTT, DNS, and HTTP protocols	The performance of the technique may depend on the quality and quantity of the training data used
[21]	2020	Anomaly-based Intrusion Detection System (IDS) using machine learning techniques	Smart home	Lightweight implementation is suitable for resource-constrained IoT gateways	Assumes the IoT network is not under attack during the training phase, which may not always be the case

Table 2. *Cont.*

Author	Year	Technique	Environment	Advantage	Disadvantage
[22]	2019	This paper proposes a deep learning-based intrusion detection system using feed-forward neural networks	IoT networks	High classification accuracy for both binary and multi-class classifications	The model shows confusion between certain categories of attacks, particularly reconnaissance and information theft, indicating a need for further refinement
[23]	2023	Machine Learning (ML) and Artificial Intelligence (AI) techniques for Intrusion Detection Systems (IDS) in IoT environments	Internet of Things (IoT) networks, including various applications such as industries, home automation, hospitals, and environmental monitoring	Provides a comprehensive review of IoT layers, communication protocols, and their security issues, emphasizing the necessity of IDS	Current ML-based IDS methods have not been evaluated in real-time specifically for IoTs
[24]	2020	Using deep learning techniques for detecting phishing attacks	IoT networks	Enhanced detection rates of phishing attacks through the application of deep learning	Possible computational resource requirements that could limit implementation in some environments
[25]	2020	Novel cross-architecture MTHAEL (Multi-Task Hierarchical Ensemble Adversarial Learning)	IoT	High accuracy and robustness in detecting obfuscated malware	Lack of practical implementation
[26]	2020	ensemble learning to detect attacks and anomalies	Smart home	Robustness and high accuracy	Computational complexity
[27]	2020	IDS using machine learning	IoT	Structured framework	Implementation complexity
[28]	2023	Malware detection using machine learning	IoT	High accuracy	Resource limitations

In Figure 3, a thematic analysis is depicted which graphically links the main research questions of the study with their respective findings. The first research question seeks to identify the common threats that smart homes face. The review process showed that denial-of-service attacks, phishing attacks, zero-day attacks, information theft, botnets, spam messages, worms, and brute-force attacks are the most frequent threats in smart home setups. These graphics aim to pinpoint the most common threats that smart homes face. The second research question aims to determine the existing techniques used for detecting malware in smart homes. This study shows that machine learning, deep learning algorithms, signature-based detection techniques, and ensemble learning approaches are the main methods used for this goal. Comprehending these results is essential for obtaining a thorough understanding of the latest developments in smart home malware detection. The last research question explores possible strategies for improving smart home security. This review found that early threat detection systems, intrusion detection systems, blockchain technology, and strong authentication methods are viable ways to enhance smart home security.

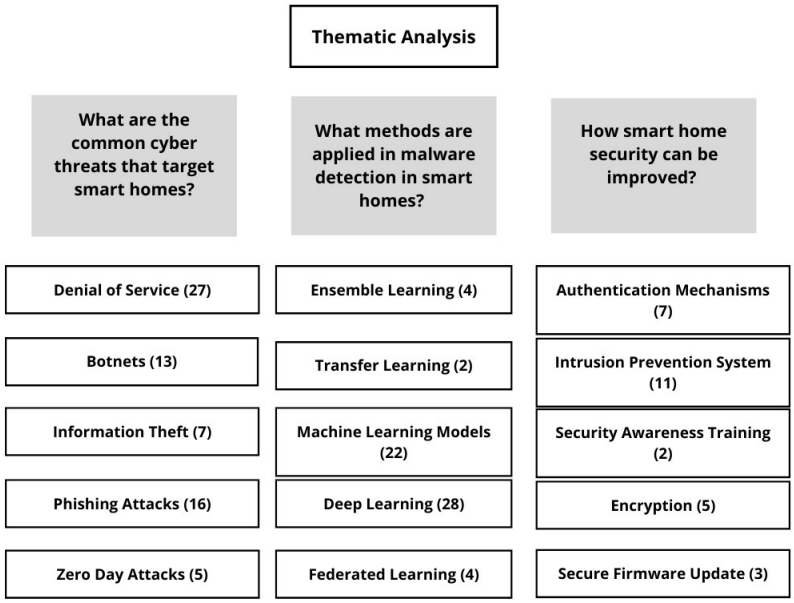


Figure 3. Thematic analysis.

5. Discussion

The systematic review procedure, outlined in the methodology section, has found relevant studies to answer the initial research questions. An in-depth analysis and combination of the results of this research offer specific answers to each question. This part analyzed the common cyber threats that target smart homes, followed by an in-depth examination of current and cutting-edge techniques for identifying malware in smart home settings, and finally, an assessment of strategies to enhance smart home security. This detailed review clarified the present knowledge of machine learning methods for detecting malware in smart homes and pinpointed areas for further research. Cause and effect analysis is performed and illustrated in Figure 4, utilizing a fishbone framework. Malware poses a significant danger to smart home settings, and its spread is a multifaceted problem influenced by different causes. Privacy risks arise from poor security measures and possibly excessive data collection by devices, leading to the exposure of user data [29]. The development of efficient detection systems for smart home ecosystems is hindered by the distinct characteristics of these systems, insufficient data for different device types, and the constantly evolving approaches of malware developers. Current techniques may be too general, concentrating on generic IoT settings rather than the distinct features of smart homes. Outdated virus types and delays in implementing security updates worsen the situation, making older systems more susceptible. Despite using machine learning, current techniques may only be capable of recognizing known dangers, without the capacity to proactively block malware from infiltrating the system entirely [30].

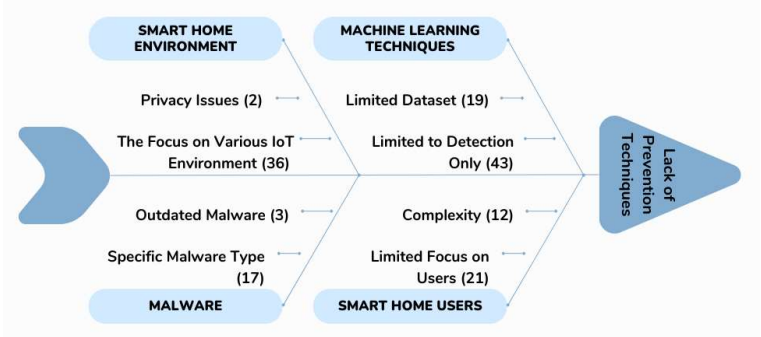


Figure 4. Fishbone framework.

5.1. Smart Home Adversarial Threat Model

The smart home threat model depicted in Figure 5 presents a scenario in which attackers with different degrees of expertise, ranging from inexperienced hackers to government entities, take advantage of vulnerabilities in the networked devices of a smart home. These vulnerabilities may occur due to obsolete software on smart devices, making them prone to known attacks [31]. Malicious individuals may also use email phishing or social engineering strategies to deceive people into compromising their security. Inadequate setup of smart home devices, such as the use of weak passwords or unsecured network connections, might provide attackers with convenient entry points. The impacts of a successful assault may be significant, including the theft of personal data such as camera video or use habits, as well as the total loss of control over a home's operations [32]. Consider a scenario when a malicious individual gains unauthorized access to a smart home, therefore denying entry, disabling the illumination, or even manipulating essential functionalities such as thermostats or household equipment. Fortunately, homeowners may reduce these dangers by using robust security systems like multi-factor authentication and complicated passwords. Consistently upgrading software and instructing users on smart home security best practices are essential measures in establishing a safe and robust smart home environment.

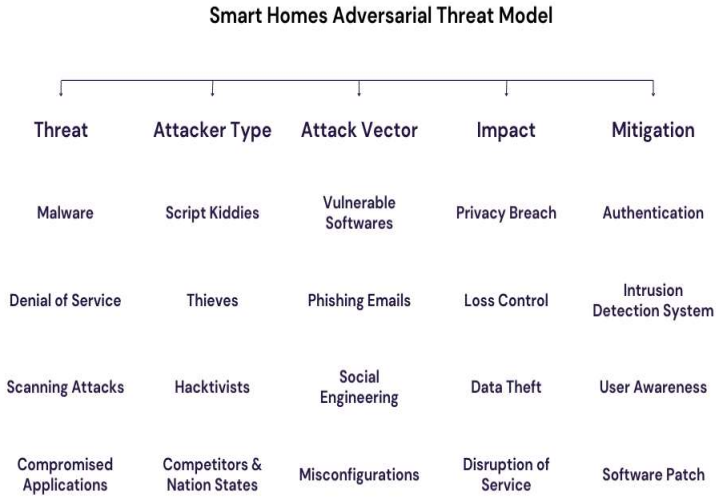


Figure 5. Adversarial threat model.

5.2. What Are the Common Cyber Threats That Target Smart Homes?

Malware is a common cyber threat capable of threatening the security of smart homes. Such malware includes viruses, worms, Trojans, ransomware, spyware, and many other forms of malware, as listed in Table 3. This malware can take advantage of vulnerabilities in smart home devices, networks, or applications to gain unauthorized access to smart home devices or controls, steal sensitive data pertaining to the user and the device, disrupt operation, or use them as part of a botnet for launching large-scale attacks. The presence of malware in smart homes increases with the increased number and complexity of connected devices as well as user's possible operational errors or negligence [33]. Understanding the kinds of malware present in smart home environments is essential to formulating appropriate security solutions [34]. Once we know the specific characteristics and behaviors of potential smart home malware, we can then identify and study various machine learning and deep learning techniques to determine which are most suitable to detect and mitigate them and, subsequently, design effective malware detection systems with higher detection accuracy and lower detection of false positives/negatives for smart home. Identifying these dangers also enables researchers to sharpen their attention and create effective means of reducing these hazards. Enhanced comprehension of cyber dangers enables the creation of strong security protocols for smart homes, protecting privacy, safety, and the physical integrity of residences.

Table 3. Summary of reviewed articles.

Authors	Threats	Approach
[35]	Botnets	Decision tree, K-nearest neighbor, and random forest
[19]	Spam	Bayesian Generalized Linear Model (BGLM) and boosted linear and eXtreme Gradient Boosting (XGBoost)
[20]	Exploits and worms	Ensemble learning and statistical flow features
[21]	Brute force attacks, zero-day attacks, and port scanning attacks	Isolation Forest
[22]	Probing attacks, denial-of-service attacks, and information theft	Feed-forward neural networks
[23]	DDoS attacks, ransomware, eavesdropping, and denial-of-service attacks	Machine learning and Signature-based detection
[24]	Phishing attacks	Feed-forward neural network
[25]	Malware	Ensemble learning
[26]	Distributed denial-of-service attacks, data probing, and spying	Ensemble learning
[27]	Dos, eavesdropping, man-in-the-middle attacks, and routing attacks	Signature-based approaches, specification-based approaches, and machine learning approaches
[28]	Malware	Isolation Forest and K-means clustering
[36]	DDos	Machine learning (logistic regression (LR), K-nearest neighbours (KNN), decision trees (DT), support vector machines (SVM), naive bayes, and random forest) and deep learning
[37]	Physical attacks, malicious code upload, data transmit attacks, and DoS attacks	Machine learning and deep learning
[38]	Botnets	Classification and Regression Tree (CART)
[39]	Spoofing, DoS, and probing attacks	Autoencoder and isolation forest
[40]	Unauthorized access, data breaches, malware attacks, DoS, and network intrusions	Hybrid Convolutional Neural Network with Long Short-Term Memory (CNN-LSTM)
[41]	Spyware, worms, ransomware, viruses, and crypto miners	CliqueNet model
[42]	DoS, MiTM, botnet, and information leakage	Federated Ensemble Learning (FEI) and adversarial machine learning
[43]	DdoS, malware behavior, and network attacks.	K Nearest Neighbor (KNN)
[44]	Zero-day attacks, DDoS, malware, and data breaches	Fast Region-Based Convolution Neural Network (Fast R-CNN)
[45]	Malware	Deep CNN and Xception CNN
[46]	Adware, virus, trojan, worm, and backdoor	Random forest voting of fine-tuning CNN
[47]	MiTM, DoS, and botnets	CNN and LSTM
[48]	Adware, spyware, trojans, and rootkits.	CNN-based transfer learning model
[49]	Malware	Random forest
[50]	Trojan horse, worms, viruses, spyware, ransomware, and DDoS.	CNN
[51]	Malware	Federated Markov chains
[52]	Cybercrime	Logistic Regression (LR), random forest, Gradient Boosting Machine (GBM), and artificial neural networks (ANN)
[53]	Botnet	Bidirectional-Gated Recurrent Unit-Convolutional Neural Network (Bi-GRU-CNN)

Table 3. *Cont.*

Authors	Threats	Approach
[54]	Malware, DoS, unauthorized access, data breaches, and network reconnaissance	Shallow Multilayer Perceptron (MLP), Deep Neural Network (DNN), CNN, and LSTM
[55]	MITM, DDoS, false data injection, intrusion vulnerabilities, zero-day attacks, and routing attacks	Distributed deep learning, Support Vector Machines (SVMs), Extreme Learning Machines (ELMs), Clustering based on Self-Organized Ant Colony Network (CSOACN), and unsupervised Optimum-Path Forest (OPF) classifier.
[56]	Adversarial setups, data poisoning attacks, model poisoning attacks, and Byzantine adversaries	Federated learning
[57]	Port scanning and DDoS	NB, DT, and SVM
[58]	Unauthorized access, data breaches, and malware injection	Reinforcement learning
[59]	Android malware	CNN and Convolutional Recurrent Neural Network (CRNN)
[60]	DDoS	Multi-Layer Perceptron (MLP)
[61]	DoS, sybil attack, selective forwarding attacks, wormhole attacks, blackhole attacks, sinkhole attacks, jamming attacks, and false data injection attacks	Convolutional Neural Network (CNN)
[62]	DDoS and ransomware	Deep Recurrent Neural Networks (RNNs), Lightweight Convolutional Neural Networks (CNNs), and graph-based methods
[63]	Ransomware	Self-supervised malware detection system, GAN-based self-supervised malware detection system and adversarial self-supervised malware detection system
[64]	Viruses, Trojans, worms, bots, backdoors, spams, spyware, and ransomware	Machine learning classifier
[65]	Malware within the context of IoT applications such as malicious code and commands	Convolutional Neural Network (CNN)
[66]	DoS, DDoS, keylogging, OS fingerprinting, service scanning	Logistic Regression (LR), Naive Bayes (NB), Decision Tree (DT), k-Nearest Neighbors (KNN), Support Vector Machines (SVM), Neural Networks (NN), and Random Forest (RF)
[67]	Trojen horses, adware, spyware, worms, viruses and ransomewares	K-Neariest Neighbors (KNN), Support Vector Machine (SVM) and Logistic Regression (LR)
[68]	DoS, DDoS, and Botnet	LSTM
[69]	DDoS and botnet	Bidirectional long- and short-term memory (LSTM) neural network
[70]	DDoS, brute force, DoS, HTTP flooding, ACK flooding, port scanning, and ARP spoofing	Decision Trees (DT), AdaBoost, and gradient boosting trees
[71]	Botnet	Isolation forest and deep autoencoder
[72]	Botnets and DDoS	Hidden Markov model (HMM)
[73]	Poer scanning, DDoS, DoS, information theft, and keylogging	Recurrent Neural Network (RNN)
[74]	Zero-day attacks	Support Vector Machine (SVM)
[75]	Botnets and DDoS	CNN
[76]	Spyware, worms, logic bombs, viruses, rootkits, trojan horses, adware, backdoors, ransomware, and bots	K-means, DT, and hybrid model
[77]	DDoS and botnet	CNN

Table 3. *Cont.*

Authors	Threats	Approach
[78]	Evasive malware, second-generation malware, and basic malicious software	SVM, NB, and DT
[79]	Backdoors, spyware, trojans, and worms	Artificial Immune System (AIS)
[80]	Zero-day botnet	Deep Neural Network (DNN)

5.3. What Methods Are Applied in Malware Detection in Smart Homes?

With the increasing popularity of smart home devices, strong security measures are essential to counteract malware risks. Researchers have created a variety of methods to detect and prevent harmful advanced methods like exploiting software vulnerabilities, deploying malicious code, and integrating compromised devices into extensive botnets [81]. Attackers may attempt to steal personal information via methods such as data breaches, intercepting device communications, or gaining physical access to carry out data transfer assaults. Denial-of-service attacks may interrupt actions in these interconnected systems. Machine learning is crucial in this battle. Machine learning models can identify anomalies in device behavior that may indicate malware by studying historical data that includes both benign and malicious activities. Decision trees are commonly used algorithms in this field for anomaly detection due to their ability to provide transparent decision-making frameworks. K-nearest neighbors detect suspicious activity by analyzing a device's behavior in relation to its nearest neighbors based on historical actions and network traffic patterns. Random forests leverage the advantages of multiple decision trees to provide enhanced accuracy and resilience. Isolation forests, a type of anomaly detection algorithm, are effective at identifying outliers that differ greatly from normal behavior patterns, possibly suggesting malware infection [82]. Deep learning, a complex method based on the human brain's structure and function, is being used for smart home malware detection, going beyond traditional machine learning. Feed-forward neural networks, a form of deep learning structure, can examine large quantities of network traffic data to detect subtle patterns that suggest malicious behavior. These networks are proficient at understanding intricate connections within data, which could result in more precise and flexible malware detection when compared to conventional machine learning techniques. Some detection methods utilize a combination of approaches. Signature-based detection, based on predetermined patterns of identified malware, can be combined with machine learning to enhance overall efficiency. Machine learning can detect new malware variants without assigned signatures, while signature-based detection is effective for identifying known threats. This demonstrates the continuous development of malware detection techniques as researchers aim to anticipate ever-changing threats in the smart home environment.

5.4. How Smart Home Security Can Be Improved?

Malware, such as viruses, Trojans, ransomware, and others (listed in Table 3), poses a major security risk to smart homes. The main threat imposed by malware is unauthorized access. By knowing the kinds of malware with which smart homes are mostly targeted and their implications, stronger security mechanisms can be developed. This knowledge can be used to design effective malware detection and prevention tools and also to make users learn best practices while configuring their smart devices and home network such that malware can be proactively handled and users' threat from malware can be reduced. Although technical improvements provide several ways to protect smart homes from malware and other dangers, the human factor is a critical part that is sometimes ignored. Users might sometimes be the most vulnerable point in the security process. Strong authentication methods are crucial in reducing this vulnerability. Two-factor authentication (2FA) is an advanced security measure that surpasses standard password-based logins. Implementing 2FA with a combination of factors like password, fingerprint scan, or code

delivered to a trusted device enhances security by making it considerably harder for unauthorized users to access a smart home system [83]. Biometric authentication, such as fingerprints, face recognition, or voice recognition, provides a safe and easy alternative to standard passwords, which are vulnerable to phishing assaults and brute force cracking. Recent research has been exploring Physical Unclonable Functions (PUFs) as a promising way to enhance authentication systems in smart homes. Static random-access memory (SRAM) PUFs use the natural manufacturing variations in a device's SRAM to create a unique fingerprint. This fingerprint is unique and cannot be readily copied or anticipated, providing a secure and device-specific identification for authentication. By incorporating SRAM PUF technology into smart home devices, the need for conventional passwords or user-generated credentials might be minimized, hence reducing the human element risk and establishing a more secure authentication environment. Enhancing smart home security may be achieved by establishing strong authentication methods, educating users, and investigating advanced technologies such as SRAM PUFs [83].

6. Summary and Conclusions

This systematic review examined three crucial study areas regarding smart home security. Examining 56 publications released from 2019 to 2023 provided significant information on the present state of risks and possible remedies. This research found a concerning variety of risks affecting smart homes. Denial-of-service attacks, phishing efforts, zero-day vulnerabilities, information theft, and many malicious software types present substantial dangers. This highlights the critical need for strong security measures. This study then examined current methods used for detecting malware. Machine learning, such as decision trees, random forests, and isolation forests, has become a major method. Feed-forward neural networks have shown potential in evaluating network traffic patterns to detect malicious activities. Signature-based detection and ensemble learning methods were recognized as useful tools. This study examined methods for improving smart home security. The results emphasize the significance of early threat warning systems, intrusion detection systems, and the promise of blockchain technology for safe data management. Strong authentication methods like multi-factor authentication (MFA) and innovative technologies such as SRAM PUFs are essential. These solutions may greatly reduce the risk related to human error, which is frequently seen as the most vulnerable point in the security system. Ultimately, this analysis provides a thorough overview of the present status of smart home security. Researchers are working on improving detection methods and suggesting new security solutions to address the existing danger.

Author Contributions: Conceptualization, O.A., K.S. and U.B.; methodology, O.A., K.S. and U.B.; validation, O.A., K.S. and U.B; writing—original draft preparation, O.A.; writing—review and editing, O.A., K.S. and U.B.; supervision, K.S. and U.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Zorgati, H.; Djemaa, R.B.; Amor, I.A.B. Finding Internet of Things resources: A state-of-the-art study. *Data Knowl. Eng.* **2022**, *140*, 102025. [CrossRef]
2. Huda, N.U.; Ahmed, I.; Adnan, M.; Ali, M.; Naeem, F. Experts and intelligent systems for smart homes' Transformation to Sustainable Smart Cities: A comprehensive review. *Expert Syst. Appl.* **2024**, *238*, 122380. [CrossRef]
3. Lucido, S.; Hummel, P. Internet of Things and Data Placement | Edge to Core and the Internet of Things | Dell Technologies Info Hub. Available online: https://infohub.delltechnologies.com/en-us/l/edge-to-core-and-the-internet-of-things-2/internet-of-things-and-data-placement/ (accessed on 9 October 2024).
4. Tetteh, N.; Amponsah, O. Sustainable adoption of smart homes from the Sub-Saharan African perspective. *Sustain. Cities Soc.* **2020**, *63*, 102434. [CrossRef]
5. Kavallieratos, G.; Chowdhury, N.; Katsikas, S.; Gkioulos, V.; Wolthusen, S. Threat analysis for smart homes. *Future Internet* **2019**, *11*, 207. [CrossRef]

6. Allifah, N.M.; Zualkernan, I.A. Ranking security of IoT-based smart home consumer devices. *IEEE Access* **2022**, *10*, 18352–18369. [CrossRef]
7. Hughes-Lartey, K.; Li, M.; Botchey, F.E.; Qin, Z. Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon* **2021**, *7*, e06522. [CrossRef]
8. Zhang, Y.; Malacaria, P.; Loukas, G.; Panaousis, E. CROSS: A framework for cyber risk optimisation in smart homes. *Comput. Secur.* **2023**, *130*, 103250. [CrossRef]
9. Linkov, V.; Zámečník, P.; Havlíčková, D.; Pai, C.W. Human factors in the cybersecurity of autonomous vehicles: Trends in current research. *Front. Psychol.* **2019**, *10*, 995. [CrossRef]
10. Gaber, M.G.; Ahmed, M.; Janicke, H. Malware detection with artificial intelligence: A systematic literature review. *ACM Comput. Surv.* **2024**, *56*, 552. [CrossRef]
11. Palša, J.; Hurtuk, J.; Chovanec, M.; Chovancová, E. Using Machine Learning Algorithms to Detect Malware by Applying Static and Dynamic Analysis Methods. *Acta Polytech. Hung.* **2022**, *19*, 177–196. [CrossRef]
12. Deldar, F.; Abadi, M. Deep learning for zero-day malware detection and classification: A survey. *ACM Comput. Surv.* **2023**, *56*, 1–37. [CrossRef]
13. Kitchenham, B.; Brereton, P.; Li, Z.; Budgen, D.; Burn, A. Repeatability of sys-tematic literature reviews. In Proceedings of the 15th Annual Conference on Evaluation & Assessment in Software Engineering (ease 2011), Durham, UK, 11–12 April 2011.
14. Dey, R.; Kassim, S.; Maurya, S.; Mahajan, R.A.; Kadia, A.; Singh, M. A Systematic Literature Review on the Islamic Capital Market: Insights Using the PRISMA Approach. *J. Electr. Syst.* **2024**, *20*, 730–746.
15. Buetow, S.; Zawaly, K. Rethinking researcher bias in health research. *J. Eval. Clin. Pract.* **2022**, *28*, 843–846. [CrossRef] [PubMed]
16. Naeem, M.; Ozuem, W.; Howell, K.; Ranfagni, S. A step-by-step process of thematic analysis to develop a conceptual model in qualitative research. *Int. J. Qual. Methods* **2023**, *22*, 16094069231205789. [CrossRef]
17. Proudfoot, K. Inductive/deductive hybrid thematic analysis in mixed methods research. *J. Mix. Methods Res.* **2023**, *17*, 308–326. [CrossRef]
18. Williams, M.; Moser, T. The art of coding and thematic exploration in qualitative research. *Int. Manag. Rev.* **2019**, *15*, 45–55.
19. Makkar, A.; Garg, S.; Kumar, N.; Hossain, M.S.; Ghoneim, A.; Alrashoud, M. An efficient spam detection technique for IoT devices using machine learning. *IEEE Trans. Ind. Inform.* **2020**, *17*, 903–912. [CrossRef]
20. Moustafa, N.; Turnbull, B.; Choo, K.K.R. An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. *IEEE Internet Things J.* **2018**, *6*, 4815–4830. [CrossRef]
21. Eskandari, M.; Janjua, Z.H.; Vecchio, M.; Antonelli, F. Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices. *IEEE Internet Things J.* **2020**, *7*, 6882–6897. [CrossRef]
22. Ge, M.; Fu, X.; Syed, N.; Baig, Z.; Teo, G.; Robles-Kelly, A. Deep learning-based intrusion detection for IoT networks. In Proceedings of the 2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC), Kyoto, Japan, 1–3 December 2019; pp. 256–25609.
23. Tabassum, A.; Erbad, A.; Guizani, M. A survey on recent approaches in intrusion detection system in IoTs. In Proceedings of the 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, 24–28 June 2019; pp. 1190–1197.
24. Saha, I.; Sarma, D.; Chakma, R.J.; Alam, M.N.; Sultana, A.; Hossain, S. Phishing attacks detection using deep learning approach. In Proceedings of the 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 20–22 August 2020; pp. 1180–1185.
25. Vasan, D.; Alazab, M.; Venkatraman, S.; Akram, J.; Qin, Z. MTHAEL: Cross-architecture IoT malware detection based on neural network advanced ensemble learning. *IEEE Trans. Comput.* **2020**, *69*, 1654–1667. [CrossRef]
26. Khare, S.; Totaro, M. Ensemble learning for detecting attacks and anomalies in iot smart home. In Proceedings of the 2020 3rd international conference on data intelligence and security (ICDIS), South Padre Island, TX, USA, 24–26 June 2020; pp. 56–63.
27. Maheswaran, N.; Logeswari, G.; Bose, S.; Anitha, T. A critical review on intrusion detection systems in IoT based on ML approach: A Survey. In Proceedings of the 2023 2nd International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN), Villupuram, India, 21–22 April 2023; pp. 1–8.
28. Baviskar, P.V.; Singh, G.; Patil, V.N. Design of Machine Learning-Based Malware Detection Methodologies in the Internet of Things Environment. In Proceedings of the 2023 International Conference for Advancement in Technology (ICONAT), Goa, India, 24–26 January 2023; pp. 1–6.
29. Adnyana, I.G.; Thalib, E.F.; Harum, M.A.; Nagas, M.A.C.; Jawa, M.W. A Discussion of Malware Attacks Targeting Smart Homes and Connected Devices: Investigating Cybersecurity Risks in Everyday Living. *J. Digit. Law Policy* **2023**, *3*, 13–25. [CrossRef]
30. He, Z.; Miari, T.; Makrani, H.M.; Aliasgari, M.; Homayoun, H.; Sayadi, H. When machine learning meets hardware cybersecurity: Delving into accurate zero-day malware detection. In Proceedings of the 2021 22nd International Symposium on Quality Electronic Design (ISQED), Santa Clara, CA, USA, 7–9 April 2021; pp. 85–90.
31. Chhetri, C.; Motti, V. Identifying vulnerabilities in security and privacy of smart home devices. In *National Cyber Summit (NCS) Research Track*; Springer International Publishing: Basel, Switzerland, 2020; pp. 211–231.
32. OConnor, T.J.; Jessee, D.; Campos, D. Through the spyglass: Towards iot companion app man-in-the-middle attacks. In Proceedings of the 14th Cyber Security Experimentation and Test Workshop, Virtual, 9 August 2021; pp. 58–62.

33. Datta, S. Vulnerabilities of smart homes. In *Applied Approach to Privacy and Security for the Internet of Things*; IGI Global: Hershey, PA, USA, 2020; pp. 216–240.
34. Sapalo Sicato, J.C.; Sharma, P.K.; Loia, V.; Park, J.H. VPNFilter malware analysis on cyber threat in smart home network. *Appl. Sci.* **2019**, *9*, 2763. [CrossRef]
35. Sharma, O.; Sharma, A.; Kalia, A. Windows and IoT malware visualization and classification with deep CNN and Xception CNN using Markov images. *J. Intell. Inf. Syst.* **2022**, *60*, 349–375. [CrossRef]
36. Gupta, A.; Tyagi, O.; Uniyal, V.; Singhal, S.; Jha, V. A Review on Machine Learning Techniques for DDoS Attack Detection in IoT. In Proceedings of the 2022 4th International Conference on Artificial Intelligence and Speech Technology (AIST), Delhi, India, 9–10 December 2022; pp. 1–6.
37. Sharma, P. Critical Review of Various Intrusion Detection Techniques for Internet of Things. In Proceedings of the 2nd International Conference on Data, Engineering and Applications (IDEA), Bhopal, India, 28–29 February 2020; pp. 1–6.
38. Htwe, C.S.; Thant, Y.M.; Thwin, M.M.S. Botnets attack detection using machine learning approach for iot environment. In *Journal of Physics: Conference Series*; IOP Publishing: Bristol, UK, 2020; Volume 1646.
39. Khan, A.R.; Kashif, M.; Jhaveri, R.H.; Raut, R.; Saba, T.; Bahaj, S.A. Deep learning for intrusion detection and security of Internet of things (IoT): Current analysis, challenges, and possible solutions. *Secur. Commun. Netw.* **2022**, *2022*, 4016073. [CrossRef]
40. Alkahtani, H.; Aldhyani, T.H. Intrusion detection system to advance internet of things infrastructure-based deep learning algorithms. *Complexity* **2021**, *2021*, 5579851. [CrossRef]
41. Wang, C.; Zhao, Z.; Wang, F.; Li, Q. MSAAM: A multiscale adaptive attention module for IoT malware detection and family classification. *Secur. Commun. Netw.* **2022**, *2022*, 2206917. [CrossRef]
42. Vutukuru, S.R.; Lade, S.C. SecureIoT: Novel Machine Learning Algorithms for Detecting and Preventing Attacks on IoT Devices. *J. Electr. Syst.* **2023**, *19*, 315–335. [CrossRef]
43. Zhao, Y.; Kuerban, A. MDABP: A Novel Approach to Detect Cross-Architecture IoT Malware Based on PaaS. *Sensors* **2023**, *23*, 3060. [CrossRef]
44. Aravamudhan, P. A novel adaptive network intrusion detection system for internet of things. *PLoS ONE* **2023**, *18*, e0283725. [CrossRef]
45. Sharma, S.; Guleria, K.; Tiwari, S.; Kumar, S. A deep learning based convolutional neural network model with VGG16 feature extractor for the detection of Alzheimer Disease using MRI scans. *Meas. Sens.* **2022**, *24*, 100506. [CrossRef]
46. Atitallah, S.B.; Driss, M.; Almomani, I. A novel detection and multi-classification approach for IoT-malware using random forest voting of fine-tuning convolutional neural networks. *Sensors* **2022**, *22*, 4302. [CrossRef] [PubMed]
47. Riaz, S.; Latif, S.; Usman, S.M.; Ullah, S.S.; Algarni, A.D.; Yasin, A.; Anwar, A.; Elmannai, H.; Hussain, S. Malware detection in internet of things (IoT) devices using deep learning. *Sensors* **2022**, *22*, 9305. [CrossRef] [PubMed]
48. Naeem, H.; Alshammari, B.M.; Ullah, F. Explainable Artificial Intelligence-Based IoT Device Malware Detection Mechanism Using Image Visualization and Fine-Tuned CNN-Based Transfer Learning Model. Computational Intelligence & Neuroscience. *Comput. Intell. Neurosci.* **2022**. [CrossRef]
49. Takase, H.; Kobayashi, R.; Kato, M.; Ohmura, R. A prototype implementation and evaluation of the malware detection mechanism for IoT devices using the processor information. *Int. J. Inf. Secur.* **2020**, *19*, 71–81. [CrossRef]
50. Panda, P.; CU, O.K.; Marappan, S.; Ma, S.; Veesani Nandi, D. Transfer learning for image-based malware detection for iot. *Sensors* **2023**, *23*, 3253. [CrossRef]
51. D'Angelo, G.; Farsimadan, E.; Ficco, M.; Palmieri, F.; Robustelli, A. Privacy-preserving malware detection in Android-based IoT devices through federated Markov chains. *Future Gener. Comput. Syst.* **2023**, *148*, 93–105. [CrossRef]
52. Schmitt, M. Securing the Digital World: Protecting smart infrastructures and digital industries with Artificial Intelligence (AI)-enabled malware and intrusion detection. *J. Ind. Inf. Integr.* **2023**, *36*, 100520. [CrossRef]
53. Chaganti, R.; Ravi, V.; Pham, T.D. Deep learning based cross architecture internet of things malware detection and classification. *Comput. Secur.* **2022**, *120*, 102779. [CrossRef]
54. Lazzarini, R.; Tianfield, H.; Charissis, V. A stacking ensemble of deep learning models for IoT intrusion detection. *Knowl.-Based Syst.* **2023**, *279*, 110941. [CrossRef]
55. Da Costa, K.A.; Papa, J.P.; Lisboa, C.O.; Munoz, R.; de Albuquerque, V.H.C. Internet of Things: A survey on machine learning-based intrusion detection approaches. *Comput. Netw.* **2019**, *151*, 147–157. [CrossRef]
56. Rey, V.; Sánchez, P.M.S.; Celdrán, A.H.; Bovet, G. Federated learning for malware detection in IoT devices. *Comput. Netw.* **2022**, *204*, 108693. [CrossRef]
57. Kumar, A.; Lim, T.J. EDIMA: Early detection of IoT malware network activity using machine learning techniques. In Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 15–18 April 2019; pp. 289–294.
58. Heartfield, R.; Loukas, G.; Bezemskij, A.; Panaousis, E. Self-configurable cyber-physical intrusion detection for smart homes using reinforcement learning. *IEEE Trans. Inf. Forensics Secur.* **2020**, *16*, 1720–1735. [CrossRef]
59. Ren, Z.; Wu, H.; Ning, Q.; Hussain, I.; Chen, B. End-to-end malware detection for android IoT devices using deep learning. *Ad Hoc Netw.* **2020**, *101*, 102098. [CrossRef]
60. Ahmed, S.; Khan, Z.A.; Mohsin, S.M.; Latif, S.; Aslam, S.; Mujlid, H.; Adil, M.; Najam, Z. Effective and efficient DDoS attack detection using deep learning algorithm, multi-layer perceptron. *Future Internet* **2023**, *15*, 76. [CrossRef]

61. Santhosh Kumar, S.V.N.; Selvi, M.; Kannan, A. A Comprehensive Survey on Machine Learning-Based Intrusion Detection Systems for Secure Communication in Internet of Things. *Comput. Intell. Neurosci.* **2023**, *2023*, 8981988. [CrossRef]
62. Dovom, E.M.; Azmoodeh, A.; Dehghantanha, A.; Newton, D.E.; Parizi, R.M.; Karimipour, H. Fuzzy pattern tree for edge malware detection and categorization in IoT. *J. Syst. Archit.* **2019**, *97*, 1–7. [CrossRef]
63. Golmaryami, M.; Taheri, R.; Pooranian, Z.; Shojafar, M.; Xiao, P. Setti: As elf-supervised adv e rsarial malware de t ection archi t ecture in an i ot environment. *ACM Trans. Multimed. Comput. Commun. Appl. (TOMM)* **2022**, *18*, 1–21. [CrossRef]
64. Han, W.; Xue, J.; Wang, Y.; Liu, Z.; Kong, Z. MalInsight: A systematic profiling based malware detection framework. *J. Netw. Comput. Appl.* **2019**, *125*, 236–250. [CrossRef]
65. Hamza, A.A.; Abdel Halim, I.T.; Sobh, M.A.; Bahaa-Eldin, A.M. HSAS-MD analyzer: A hybrid security analysis system using model-checking technique and deep learning for malware detection in IoT apps. *Sensors* **2022**, *22*, 1079. [CrossRef]
66. Yaokumah, W.; Appati, J.K.; Kumah, D. Machine learning methods for detecting Internet-of-Things (IoT) malware. *Int. J. Cogn. Inform. Nat. Intell. (IJCINI)* **2021**, *15*, 1079. [CrossRef]
67. Ijaz, A.; Khan, A.A.; Arslan, M.; Tanzil, A.; Javed, A.; Khalid, M.A.U.; Khan, S. 2024. Innovative Machine Learning Techniques for Malware Detection. *J. Comput. Biomed. Inform.* **2024**, *7*, 403–424.
68. Ali, S.; Abusabha, O.; Ali, F.; Imran, M.; Abuhmed, T. Effective multitask deep learning for iot malware detection and identification using behavioral traffic analysis. *IEEE Trans. Netw. Serv. Manag.* **2022**, *20*, 1199–1209. [CrossRef]
69. Auliar, R.B.; Bekaroo, G. Security in iot-based smart homes: A taxonomy study of detection methods of mirai malware and countermeasures. In Proceedings of the 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Hilton, Mauritius, 7–8 October 2021; pp. 1–6.
70. Amru, M.; Kannan, R.J.; Ganesh, E.N.; Muthumarilakshmi, S.; Padmanaban, K.; Jeyapriya, J.; Murugan, S. Network intrusion detection system by applying ensemble model for smart home. *Int. J. Electr. Comput. Eng. 2088-8708* **2024**, *14*, 3485–3494. [CrossRef]
71. Shi, T.; McCann, R.A.; Huang, Y.; Wang, W.; Kong, J. Malware detection for internet of things using one-class classification. *Sensors* **2024**, *24*, 4122. [CrossRef] [PubMed]
72. Yamauchi, M.; Ohsita, Y.; Murata, M.; Ueda, K.; Kato, Y. Anomaly detection in smart home operation from user behaviors and home conditions. *IEEE Trans. Consum. Electron.* **2020**, *66*, 183–192. [CrossRef]
73. Shobana, M.; Poonkuzhali, S. A novel approach to detect IoT malware by system calls using Deep learning techniques. In Proceedings of the 2020 International Conference on Innovative Trends in Information Technology (ICITIIT), Kottayam, India, 13–14 February 2020; pp. 1–5.
74. El-Ghamry, A.; Gaber, T.; Mohammed, K.K.; Hassanien, A.E. Optimized and efficient image-based IoT malware detection method. *Electronics* **2023**, *12*, 708. [CrossRef]
75. Asam, M.; Khan, S.H.; Akbar, A.; Bibi, S.; Jamal, T.; Khan, A.; Ghafoor, U.; Bhutta, M.R. IoT malware detection architecture using a novel channel boosted and squeezed CNN. *Sci. Rep.* **2022**, *12*, 15498. [CrossRef]
76. Yadav, C.S.; Singh, J.; Yadav, A.; Pattanayak, H.S.; Kumar, R.; Khan, A.A.; Haq, M.A.; Alhussen, A.; Alharby, S. Malware analysis in IoT & android systems with defensive mechanism. *Electronics* **2022**, *11*, 2354. [CrossRef]
77. Jeon, J.; Park, J.H.; Jeong, Y.S. Dynamic analysis for IoT malware detection with convolution neural network model. *IEEE Access* **2020**, *8*, 96899–96911. [CrossRef]
78. Aboaoja, F.A.; Zainal, A.; Ghaleb, F.A.; Al-Rimy, B.A.S.; Eisa, T.A.E.; Elnour, A.A.H. Malware detection issues, challenges, and future directions: A survey. *Appl. Sci.* **2022**, *12*, 8482. [CrossRef]
79. Alrubayyi, H.; Goteng, G.; Jaber, M.; Kelly, J. Challenges of malware detection in the IoT and a review of artificial immune system approaches. *J. Sens. Actuator Netw.* **2021**, *10*, 61. [CrossRef]
80. Popoola, S.I.; Ande, R.; Adebisi, B.; Gui, G.; Hammoudeh, M.; Jogunola, O. Federated deep learning for zero-day botnet attack detection in IoT-edge devices. *IEEE Internet Things J.* **2021**, *9*, 3930–3944. [CrossRef]
81. Meneghello, F.; Calore, M.; Zucchetto, D.; Polese, M.; Zanella, A. IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet Things J.* **2019**, *6*, 8182–8201. [CrossRef]
82. Tan, X.; Yang, J.; Rahardja, S. Sparse random projection isolation forest for outlier detection. *Pattern Recognit. Lett.* **2022**, *163*, 65–73. [CrossRef]
83. Yoon, S.; Han, S.; Hwang, E. Joint heterogeneous PUF-based security-enhanced IoT authentication. *IEEE Internet Things J.* **2023**, *10*, 18082–18096. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.