*IOSR Journal of Computer Engineering (IOSR-JCE)*
*e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 24, Issue 2, Ser. I (Mar. –Apr. 2022), PP 34-49*
*www.iosrjournals.org*

# E-third Eye in an IoT Smart-Living: A Systematic Review

Olebara Comfort Chinaza
*Department of Computer Science, Faculty of Physical Science, Imo State University,*
*Owerri, Imo State, Nigeria. Orcid:0000-0002-5891-4206*

***Abstract***
*The digital divide all over the world cannot be measured by the level of technical know-how alone. Many people get into the hype of new and trending technology, from Smart cars to Smart homes, syncing work, entertainment, and seeming security to a network that is one click away. This study is an attempt to expound on the extant features of digital knowledge***,** *with respect to the security consciousness of tech users. The conglomeration of various IT hardware and software to form a "Smart effect" in homes, medical fields, campuses, and various enterprises is digitalization at its peak, as there are no boundaries between man, his machines, and his environment. Despite the comfort, entertainment, and cost-effectiveness of these solutions, this research digs in to evaluate its security implications through a review of various compromises captured in research. It also reviewed some proposed schemes aimed at proffering solutions to the endemic problem, with more focus on those that have been validated by research. Popular solutions include having responsible reporting by ethical hackers, Crowdsource and SmartCrowds, learning systems that classify, cluster, or set security policies for network monitoring, as well as proof of concept generated after carefully carrying out security analysis, which serves as a guide to device manufacturers. Finally, the researcher recommends that every smart network plan be accompanied by an appropriate security consultation and implementation***,** *Companies offering smart solutions should have cyber security certified staff that will run vulnerability checks on their products before putting them on the market and also enlighten consumers on security best practices.*

***Keywords:*** *IoT, Smart Network, Vulnerability, Malware, Wireless Sensor Network, Microcontroller, Microprocessor, Espionage.*

Date of Submission: 02-03-2022 Date of Acceptance: 16-03-2022

## I. Introduction

IOT, an acronym for Internet of things, is a way of implementing technological advancements into the human environment for the purpose of solving man-and -his-environment problems. Van Kranenburg defines IoT as "a dynamic global network infrastructure that is capable of configuring itself on interoperable communication protocols where virtual and physical "things" have identities, physical attributes, virtual personalities, and use intelligent interfaces to integrate seamlessly into information networks" (cited in [1]. IoT devices and their accompanying applications are found in cities, campuses, agriculture, health, hospitality, energy saving, environmental pollution control, and many other areas where human effort is required, and data transmission/information reception is expected. They are universally available and able to integrate various devices. A single piece of software may detect and install any IoT device it senses within a certain radius of its presence. Simply put, IoT is a technology that uses sensors either embedded in passive devices such as thermistors and resistors or in intelligent sensors with embedded microcontrollers and microprocessors [2]. They have the ability to read conditions in their host environment, and perform assigned functions or transform data into useful information through electrical signaling [3].

[4] defined IoT as a system in which objects with sensors, actuators, processors, and transceivers are linked and communicate with one another to achieve a common goal. Sensing is a remote but major aspect of IoT technology, where wireless technology involves communication over a medium of space. It is an act where a device, machine, or module, generally called sensor, receives chemical, biological, or physical signals and converts them into electrical signals, which are transmitted to a computer processor [5]. The choice of sensor depends on the signal they are required to measure. [6] provides a more detailed explanation in his article "What is sensor?" Here, sensor types are identified as: active or passive, analog or digital. While active sensors need

external excitation before producing output signals, passive sensors do not need extra voltage, stimulus, or any form of excitation.

Sensor types include, but are not limited to: temperature, pressure, acceleration, proximity, image, humidity, level, gas, infrared, motion sensors, load cell sensors, proximity sensors, ultrasonic sensors, pressure sensors, light sensors, humidity, moisture, or rain sensors, accelerometers, motion sensors, gas, infrared, and many others. [6] These are the detecting agents that yield the smart technologies currently in use. Figure 1 and 2 below show sensor types and their implementation in smart Homes.

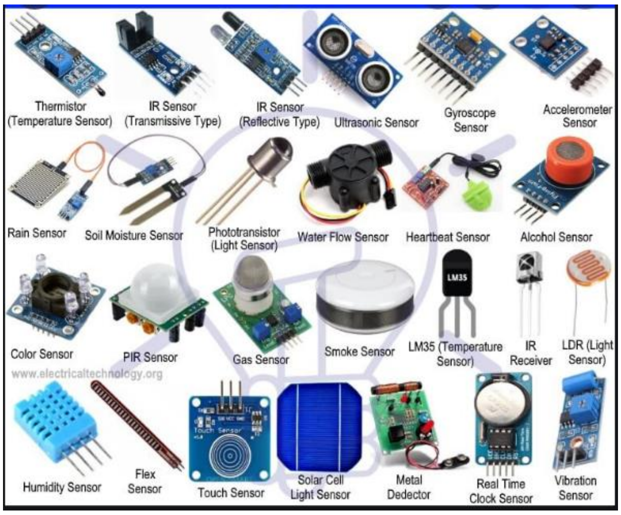

**Figure 1: Different types of sensor**
**Source:** [6]

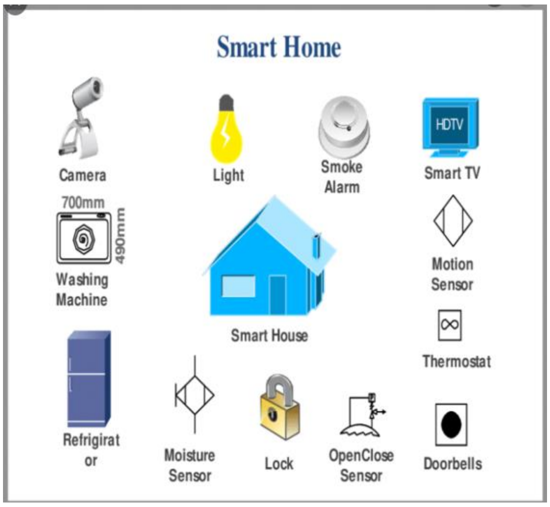

**Figure2: IoT implementation in Smart Home**
**Source:** [7]

The predatory nature of man makes him seek to be better than his competitors and other humans, hence the constant prying into people's, organizations, or nations' privacy. Many hardware, software, firmware and network systems are either built with manufacturer-installed backdoor, design-level installed backdoor, or hacker installed compromise. This is more common in recent years with integral parts of the production outsourced to third parties. The advantage of mass and cost-effective production notwithstanding, the result is an increase in espionage activities where brand owners are designers or fabricators of the various chips used in their finished products.

This paper is organized as follows: in section 1, the subject matter is introduced with the study background. Section 2 captures review of contexts in the review domain. Section 3 specifies the study methodologies and road map followed to achieve a systematic review such as the search criteria, extraction and synthesis, and related works. Section 4 captures the summary, conclusion, recommendation, and contribution to body of knowledge.

## II. Literature Review

### 2.1 Integrated Circuit Design and Fabrication

[8] carried out a quantitative study on approaches used by semiconductor firms in United States of America to make outsourcing decisions. He found that the companies had lost about 33% of their employees as a result of high labour cost, then resorted to outsourcing to offshore countries where the cost of qualified labour was considered low. According to [9], China, on the other hand, massively invested in training Integrated Circuit designers and Fabricators thereby growing the semiconductor industry astronomically (cited in [10]. [11] outlined tremendous growth in China's Integrated Circuit industry which comprises of IC Design and IC fabrication.

The IC design industry in China is established in regions and cities, with each competing to outperform the other. Table 1 below, shows the developmental statistics by region and cities. The report also captured international competitiveness, moving from having one company at the top echelon of international players in the IC industry, to having 11 out of the 50 topmost IC companies in 2016. Table 2 is distribution of IC design companies in China. Productions by these companies include from wireless networks, fixed networks, digital media, as well as other chip related products. Its digital media products include TV chips, end-to-end solutions, IP cameras, video phones, network monitoring devices, Radio Frequency chips, 2G, 3G, 4G mobile communication basebands, tablets, imaging devices, digital televisions, IC design and verification technology, advanced Electronics Design Automation (EDA), as well as off-the-shelve design services. Cloud applications, Microcontroller units, LED chips, fingerprint sensors, audio, video Soc, digital wearables and practically all known areas of IC design and fabrication are covered by China's top ten companies. Providing low-cost labour also brings other nation's manufacturer to outsource components from China [11].

### 2.2 Discovered Compromises in Hardware and Software

Many popular hardware and software at one time or another have been found compromised. From operating systems [12], Microsoft Xbox $^{tm}$ case [13], Samsung Galaxy phone [14], Hardware TROJANS in wireless cryptographic ICs [15], Ultra-low-level backdoor for CPU hacking[16], new security threats against chips containing scan chain structures [17], iPhone 5C NAND mirroring [18], many similar backdoors have been discovered in Android either through upgrades and many compromised apps. Some IoT implementation backdoors include those found by [19] in Juniper ScreenOS, Telnet and SSH, WD mycloud, Busybox (ARM embedded Linux IP camera, those in Smart TV as reported by [20], on WikiLeaks CIA installed malware in Smart TVs. This malware named Weeping Angel could recover WI-FI keys from the TV and use same to hack the Smart TV's network. This malware also records audio when the TV seems off- a condition known as fake-off. Further reports from Washington post's on WikiLeak information page highlights that Mobile Device Branch, which is a unit in CIA produced malware to control iPhones which is America's most popular smart phone brand. Google Android was not spared either.

### 2.3 Wireless Sensor Network

Wireless Sensors have been adjudged favorable due to design features such as lower cost of installation, longer operating time, lower cost of production, and unmanned network operations [21]. This last attribute however, poses security threat, as an unmanned network operation implies absence of monitoring of infrastructure for information flow. [21]l finds this to be exploitable by attackers. [22] describes an attack surface as comprising protocols, and communication channels which they termed enablers as well as processes and data, which they termed targets (cited in [23]).

From the review so far, identifying an attack surface seems to be the main task, as integration of various points of IoT architecture make it almost impossible to avoid being hacked. Categories of interested parties range from hackers to official government security personnel and to apps that create backdoors. WSN has brought about huge technological advancement in the IoT industry. Many researches have been carried out in a bid to provide lasting solution to security issues that counter it's many advantages. [24] identifies security and privacy of WSN as most important and critical in wireless communication channel, hence the researcher reviewed published works that showed validation capabilities of their proposed methods. Some of the works reviewed by Lee are presented here as a guide to intending IoT deployers.

### 2.4 Some proposed and validated WSN security in research

[25] proposed a model that generates pseudo randomly in computationally constrained environment using stream cryptographic algorithm. Area of implementation is Microprocessor environments such as WSN and IoT (cited in [24]). [26] presented a model for Secrecy Amplifier in Arduino and TinyOS platforms and showed how the protocols work, by simulating them in a real Network (cited in [24]). [27] chose visual aspect of WSN, called Wireless Visual Sensor Networks (WVSNs), which is an encryption method for images that are received and transmitted over wireless networks and IoTs (cited in [24]. The author also reviewed works of [28], who proposed and validated Rivest-Shamir-Adleman RSA algorithm. The method of [28] is based on cryptosystems, which is a collection of cryptographic algorithms used to encrypt sensitive data whose transmission medium is not adequately secured. Implementation of this proposal is in Microcontroller MSP430, the Microcontroller unit used in most IoTs. [29] presented a security framework that ensures authentication of sensor nodes and shows resistance against hardware or software configuration anomaly (cited in [24]). Security in cloud-based WSN and IoT solutions were captured by the scheme proposed by [30] whose proposal validation provides protection against online and offline key guessing attacks perpetrated by hackers. Their scheme proved efficient for document and keyword protection (cited in [24]). Another interesting work which was presented by [31] helps to detect and recover compromised areas using block-wise and pixel-wise detection mechanism. This scheme is also applicable to Wireless Visual Sensor networks (WVSNs). Many solutions suggest using purpose-built devices which are designed to carry out specific tasks, but without an operating system. This helps to eliminate vulnerabilities associated with OS. [2] researchers suggest securing WSN by providing Bank-grade security at every level (between sensors, end points, and gateways elliptic Curve Diffie-Hellman ECDH256 encryption is proposed, between gateways and web servers, AES128 encryption and purpose-built gateways without OS is proposed,

finally, between web servers and internet browsers or mobile applications, Transport Layer Security is proposed. Figure 5 shows this proposal which has not yet been validated with real implementation.
[32], Editor -in-Chief with HD Televizja demonstrated hoe TVs can be scanned for viruses, close audio and video access points to stop eavesdropping and fake-off recordings. The demonstration was carried out on Samsung 48JU6412 series JU6400 ULTRA HDTV in Samsung 2015 lineup.

The editor notifies smart TV users of built-in antivirus that scans the memory, all connected devices and network. The user however, needs to have it activated. The procedure was given as:

### 2.5 Technologies for mitigating Malware Attacks of Computers Networks, and Infrastructure

Two technologies are available for analysis of computer systems for malware, vulnerability, or anomaly. The technologies are: Behavior-based analysis and Signature-based analysis. In behavior-based analysis, the action taken or intended action by an element's attribute is used to determine if it is malicious. Some of these actions are: rootkits installation, auto-start registration, sandbox search, listening to open ports without authorization. Signature-based detection has to do with discovering malware by experts using malware detection solutions, storing these identified malware in a malware repository [33], and using the repositories search engine to scan files packets, hash keys for matching attributes with known malware [34]. A third technology is the detection of anomalies by reading and calculating various correlations that enable analyzer compare a normal attribute such as read time of scripts. In [35], the authors carried out an experiment that uses chip programmer to record the time it takes for the chip programmer device to read the script installed inside a medium grade PIC16F887 MCU. Average of Ten read-times (obtained over a period of ten weeks) was correlated with normal read-time of the MCU obtained on first use of the device. This method follows the knowledge of hardware backdoor payloads sometimes being triggered when the device attains a set temperature threshold. Also, attackers on gaining unauthorized access to the device script stealthily add codes that perform malicious activities without altering the device original function such as LED light output. The correlation result is used to detect anomaly in the script. This agrees with [36] where authors suggests automation of a four-module framework that uses existing tools to accept user input, scan last collected and historical data using NMAP, and query National vulnerability database where a correlation analysis confirms vulnerability status of network data. It is necessary to state the difference between the terms vulnerability, anomaly, and malware presence in a computer system.
Vulnerability is a status of being exposed to unauthorized access [37]. The accessing body could be a software (botnets), hardware (hardware backdoors) [38] of both software and hardware (firmware vulnerabilities), and could be knowingly installed for espionage, or as a result of design anomalies discovered by hackers. With respect to IoT, anomalies are inconsistencies in IoT data, network, or device. It is a status where behavior analysis of these IoT domains does not corelate with a known normal behavior of the analyzed IoT domain. Malware on the other hand is made up of two words: malicious ware, where malicious signifies the intent of the attacker, and ware, the tool of attack. There are software (scripts) written in order to gain unauthorized access such as botnets (Mirai and its subsets) and hardware backdoors which are chips included in hardware IoT devices by third-party integrated circuit or other hardware (sensors, actuators) manufacturers for stealthily stealing information or causing harm to the computer of the victim.

### 2.6 Malware Analysis Methods

Many methods exists for malware analysis after the scanning, capturing, and data preparatory processes such as feature extraction. In this work however, we draw attention to studies that make use of Machine or Deep learning, and those that use statistical methods such as correlation.

## Machine and Deep Learning

Machine Learning is a subset of Artificial intelligence that builds learning algorithms into a machine with acquired data and uses the algorithm to discover a trend in a system. When this action is replicated by machines, it is called Deep Learning. Deep Learning therefore is also a subset of AI, but has more layers than the ML.

Applying these technologies to data analysis requires the following:

### -A dataset

The dataset is a group of data that show attributes and features of an event or object being measured.

### -Machine Learning Algorithm

These are models the follow mathematical models that comb through a dataset in order to find a pattern. The data is split into two parts (Training and testing data) where the output of the training data becomes an input for testing the algorithm’s performance on the event.

Machine Learning types are: Supervised learning, Unsupervised learning, and Reinforcement learning.

### Supervised Learning

In Supervised ML, algorithm is trained with a dataset that is labeled. This implies that the variables X and Y, representing input and output variables, are present in the dataset. Algorithms in this category are: Regression, Classification, Naïve Bayesian, Random Forest, Neural Network, Support Vector Machine.

### Unsupervised Learning

In Unsupervised learning, Artificial Intelligence algorithms are used to discover patterns in datasets. The datasets here are neither unlabeled, hence the algorithm combs through the dataset looking for patterns with which output and input variables can be deduced.

### Reinforcement Learning

This is a machine learning technique where a model is trained to perceive, respond, and respond to its environment. Its response triggers of a reward or penalty policy set by the programmer. A correct decision by the model in a complex environment activates the designer’s reward policy while a wrong decision attracts penalty.

## III Methodology

This work follows a hybrid methodology in carrying out the survey of vulnerability, anomaly and malware detection researches with a view to create situational awareness of the various penetration loophole, their presentations, as well as their manifestation systems. The methods employed for the review are: Preferred Reporting Items for Systematic Reviews and Meta Analysis (PRISMA) statement, 2009’s updated version of 2020 [39]. PRISMA, though initially developed for use in health science domain updated the literature review with changes that made it adaptable to other fields such as Information system. This update is majorly in the area of being a method for qualitative review to being for both qualitative and quantitative review. The second methodology is the Information Science adapted work by[40]. The authors identified 3 types of literature reviews. The first, theoretical background gives foundational information on the context of research question so as to paint a clearer picture of the subject matter. The second type is usually presented in thesis, termed “Literature Review, helps the researcher to present contexts, theories, and empirical content in his thesis. According to the authors, the third review type is called standalone literature review, which is an article that reviews existing works or articles by following a systematic set of rules. The standalone review is the second review methodology used in this paper.

This review will follow the checklist of PRISMA for Title and Abstract writing. Both methodologies agree on the following review items:

-**Research Aim or Question: Research goal or question(s)** whose answers provide insight to the overall review.

-**Search strategy:** An outline of repositories from where reviewed studies were obtained as well as search strings used in the digital libraries.

-**Study selection:** section for reporting how reviewer carried out study as well as tools used.

-**Research Synthesis:** A reviewer’s combination of various research works for the purpose achieving his research aim or answering his research question(s).

### 3.1 Research Purpose

The purpose of this study is to carry out an exploratory study of security implications of implementing IoTs in Smart everything, with the view to provide Situation awareness report to non-tech community who may blindly deploy these cozy tech trends without adequate consideration of the security implications on themselves, their families, enterprise they work for, or their nation at large.

### 3.2 Search Strategy

Research repositories searched include ACM digital library, IEEE digital library, Research gate, and Google Scholar. The strings used in the search are [“IoT malware”] OR {“IoT vulnerability”] OR [“IoT backdoor”] OR [“IoT machine learning-based malware detection”] OR [“IoT deep learning-based malware detection”] OR [“IoT static analysis”] OR [“IoT dynamic analysis”] OR [“IoT hybrid analysis”] OR [“IoT vulnerability detection”]. ACM digital library search yielded 93 results when all search strings were entered while IEEE digital library search yielded 2400 results. Tools used include Sci Hub and openknowledgemap..

### 3.3 Study Selection Criteria

Selection criteria follows the research purpose which was captured by the search strings used. Articles that addressed IoT vulnerabilities, anomalies, malware, and general challenges, as well as detection and prevention methods for the aforementioned IoT challenges formed major selection criteria. The search string made the research vast, hence search results related to dynamic, hybrid, and static analysis were removed from the search so as to have manageable research. Focus was therefore on:

-Vulnerabilities, anomalies, and malware attacks in IoT ecosystem: Studies that analyze and create situational report.

-Mitigation Technologies such as Signature, Behavior or policy-based.

-Solution oriented analysis such as Machine/Deep Learning-based or statistics-based (Correlation).

A total of 78 papers were used in different sections of this paper with the most being from IEEE (17 articles) followed by ACM (14 articles). The low number of works from these source stem from the fact that most articles in the digital library require purchase and membership could only give access to few, hence highest priority was given to most relevant to present study. 46 other works made up of peer reviewed papers, Universities Laboratory Experiments, Google Scholar, blogs, YouTube videos. The diversity of the study sources gave deeper insight required to paint the overall picture of IoT security challenges. Tool for citation and reference management is Mendeley, Web importer and desktop MS-word plug-in.

### 3.4 Data Extraction and Synthesis

This section gives a breakdown of articles captured in the research. The IoT part (application, device, network or firmware) they focused on or the challenge addressed. Table1 below

#### 3.4.1 IoT Vulnerabilities

Vulnerabilities are flaws in design, software or hardware, that allow malicious activities to be carried out in a system. They could be intentional or unintentional. The action taken by a hacker who discovers a vulnerability could result in demand for ransom (ransomware), malware attack, or information to design owner in exchange for an incentive (Crowdsource). The work by [41] observed that many IoT device manufacturers no longer provide support or patches for discovered vulnerabilities as a result of high maintenance cost. The authors developed a cloud-based framework that controls network flow in an IoT ecosystem. According to [41], manufacturers’ lack of support and failure to provide updates and patches for consumer products give room for vulnerabilities to be exploited. [42] and [43] find IoTs to provide vulnerabilities in infrastructure which lead to increased attack on Industry 4.0 IoT devices and leakage of sensitive information. While [42] attributes it to high demand for the IoT devices industrialist and carried out an analysis of security vulnerabilities in Industrial Internet of things, [43] considers traditional security measures such as operating system update, software patches, and antivirus as not being sufficient. They suggest a diversity of IoT devices such as found in IoT in network embedded systems, require security policies, specialized attack learning signature, and some enforcement mechanism to enable cross-device dependencies instead of traditional honeypot security. [44] agrees that traditional security is not sufficient as it offers only perimeter defense while IoTs working inside the network core. The authors considered pairing of associated devices working in a user’s trust zone, and identifying the devices through their behavior. These behaviors are used to detect compromised IoT devices and remove them from a larger network. An investigative study by [45] reveal feasible ways through which IoT system can be in infected. They find the prevalence and universality of IoT devices as tools for gaining control of devices in an IoT ecosystem and demanding ransom from vulnerable device owners by carrying out denial of service (DOS/DDOS) activities. The authors therefore developed IoT vulnerabilities proof of concept which serve as guide to future manufacturers. [46] highlighted a side of vulnerabilities which result from misconfiguration of IoT devices. The authors perform an internet level IPv4 scan that revealed over 1.5million misconfigured IoT devices such as: unauthenticated protocol setting, weak password. Further deploying six honeypots for one month showed >200 000 attacks comprising of DOS, multistage, and infected online hosts attacks. For [47] choosing a disassembler that detect, analyze, and defuse malware sound impracticable as existing disassemblers have varying configurations for expected task, they therefore proposed a combination of disassemblers which can be useful in troubleshooting IoT systems. The work of [48] agrees with [45] with respect to responsible reporting, but extend the process to include engaging multiple hackers and individual to find vulnerabilities in software products in exchange for an incentive, a program known as bug bounty. In bug bounty manufacturers recognize and pay monetary compensation to individual without being compelled as in ransomware. Dominik et al [49] blame manufacturers for too many vulnerabilities in the devices attributing this to their focus on producing low-cost products performing one function or another while neglecting their security concerns. These products interact with critical devices in a network and become the gateway into the network. The authors developed an intercepting function with which they replace execve address (file pointed to by the system call function execve() ) in the system call table. They also compute SHA256-digest from the program's binary, then use intercepting function and computed SHA256 to match a whitelist repository of permitted programs. [50] however, noted that IoT technologies such as sensing and machine -to-machine communication are not new. While the former has been used in floor manufacturing, the later is evident in the internet, which existed long before the advent of IoT technology. The authors analysed behaviour of IoT protocols such as Wi-Fi and Blue Tooth, used n-gram to characterize normal behaviour and employed machine learning classifiers to develop models that detect abnormal behaviour. For [36] and [51], early detection of vulnerabilities with the help of network scanners should be a policy in IoT management. The two works implemented a modulated framework that detects malware before a full attack occurs. While [36] presents Internet Protocol network scanning using multiple tools such as ShoVAT (Shodan-based Vulnerability Assessment Tool) security scanning tool [52] and Shodan search engine [53], and correlate their result to ascertain their vulnerability status, [51] implements a similar early detection that uses machine learning for classification, repository of traffic features, a module for policy setting and a last module for sub-sampling on a large network such as enterprise networks and ISPs. In [54], studies that focus on attack of public network endpoints are analyzed. The authors achieved this by analyzing endpoints acting as dropzones and their targets to gain insight into the ecosystem dynamics, then reverse-engineered thousands of IoT malware samples, extracted behaviour-based strings to obtain IP addresses. Shodan, a search engine for internet connected devices [53] and Censys attack surface management tools [55] are used to obtain information about endpoint for masked IP addresses. Implementing SmartCrowd [56], just like the CrowdSource system implemented by [48] and [26] is another means of alerting manufacturers on discovered vulnerabilities in the products without negative impact on the consumers, or making the manufacturers incur higher overhead costs through ransom payments. The authors in [56] implemented an decentralized automated system that allows third-party SmartCrowds analyze vulnerability in IoT systems using blockchain technology and get incentive in return. Their implementation was validated by the analysis of two IoT apps (Samsung connect and Samsung Smart Home by six third-party SmartCrowds (VirusTotal, Quixxi, Andrototal, Jag.alibaba, Ostorlab,and htbridge). The result showed third-party security vendors discover varying number of high, medium, and low vulnerabilities on each IoT application. This agrees with the work of [57] on the numerous vulnerabilities that are contained within the IoT ecosystem following its existence in an unprotected environment consisting of sensors, robots, applications, servers, communication devices etcetera. To check interaction vulnerabilities, [57] developed a programmable counter-attack application that detects DDOS attacks by generating counter values of network parameters. Also, device security attacks, sensor failures as well as communication noise form what is construed as anomaly [58], and to detect these anomalies, the authors in [58] developed a framework that integrates IoT event detection with anomaly detection instead of running them independently. The framework EDS (event Detection System) is concerned with the identification of events that are of interest, such as flood, intruder who gains unauthorized access, and ADS (Anomaly Detection System) concerned with identification of activities that may deter the successful completion of a system's function. Their framework implemented three components for each of EDS and ADS: Rule-based component, Machine Learning component, and a decision-making component. Testing the framework using real life applications and NSL-KDD dataset show high performance, efficient and real-time processing of the proposed framework. Other application domain detection mechanism is in the area of writing script that search for open ports that are vulnerable to DDOS or DOS attacks and also check IoT device data encryption [59]. Imane *et al* in [60] x-rayed different security threats on IoT by categorizing the threats as: data & network/privacy/system & IoT on the one hand, and application's domain like smart home & smart city.

### 3.4.2 Vulnerability/Anomaly /Malware Solutions that implement Artificial Intelligence or its subsets (ML/DL)

For [61], fingerprinting compromised IoT devices and divulging discovered cyber threat intelligence on unsafe IoT devices goes a long way to guiding consumers IoT devices choice as well as making manufacturers, application developer and service providers work harder towards IoT security provisioning. To validate the proposed method, the authors developed a data-driven technique that collects network traffic, analyses of internet through scanning (ZMap), banner grabbing (ZGrab), and characteristics labelling. The over 3 terabyte of network

traffic captured is trained using 3 machine learning classifiers (support vector machine, Random Forest, and Gaussian Naïve Bayes) and utilized in compromised devices fingerprinting. Similar shallow machine learning classification methods (k-Nearest Neighbors (k-NN), Gaussian Naïve Bayes, and Random Forest algorithms were adopted by [51] in learning application layer protocol ingress/egress traffic captured at the wireless access gateway. The study by [62] underscored a new attack pattern, "the insider attack", that exploits IPV6 routing protocol vulnerabilities. The authors demonstrated detection of this attack termed "loophole" by using classifiers to distinguish attack and normal network data, then working on nine-features extracted from the data. Machine learning (XGBoost, Random Forest and Support Vector Machine) and deep learning (Neural networks and Long Short Term Memory) for classifying attack and network data and comparison of detection accuracy performance. In [61], [51] and[62] the authors validate their classification algorithm by calculating variables that make-up machine learning validation metrics such as precision, recall, F-score (F-measure), and Area Under Receiver Operating Characteristic Curve (AUC-ROC). Precision is the ratio of correctly classified IoT devices over all IoT devices in the system and it is used to calculate classifier's ability to make correct classifications. Recall is the ratio of correctly classified IoT devices over total IoT device that are present in the test dataset and demonstrates a classifier's ability to identify maximum number of correct labels. F-measure if the combination of weighted averages of precision and recall. AUC-ROC is used for performance measurement. Other studies that implemented Artificial intelligence or any of its subsets (ML and DL) in vulnerability, anomaly, or malware detection at host, network, application, or device level include:
Reinforcement learning, [58], [63]
Neural network [64] , [65], [62], [66], [67]
Classification: [51], [68], [69], [70], [66]
Clustering unsupervised machine learning: [71], [72], [68]
Recursive Feature Elimination: [69]

### 3.4.3 Related Works

In this section, we present some related works. The criteria for the selection of these works are: Title string such as ["IoT" + "vulnerability" OR "Malware" OR "Anomaly" + "detection" + "Survey" OR "Review" OR "Analysis"]. To this end, the following works were identified related to this paper. The authors in [73] carried out a survey of researches where deep learning algorithms were deployed in solving IoT security challenges through monitoring behavior of features that constitute element(s) of interest in the domain being investigated. Similarly, [74] reviewed IoT attack models and solutions that were deployed using machine learning technique. IoT-based Smart Grid communications are not left out in the massive attack of computer systems and associated technologies. In [75], the authors carried out a survey of studies in the area of security threats that target energy big data. They created situational awareness of this emerging security attack and also highlight challenges of carrying out research in management of energy big data. A survey of IoT vulnerabilities reviewed by different researchers target various IoT contents such as protocols, technologies, applications domain, context awareness, legal frameworks, attacks, security protocols, intrusion detection, and access points was carried out by [76]. The authors highlighted various IoT vulnerabilities studies, with studies grouped by investigation domain, and year of study. A similar vulnerability study surveyed for works that aim to detect firmware vulnerabilities was carried out by [77]. Firmware detection researches captured in the survey include static analysis, symbiotic execution, fuzzing on emulators, and comprehensive testing.

### 3.5 Synthesis Result

Table 1 below is used to summarize various studies in IoT security challenges as reflected in investigation domain (network traffic, device, firmware, application, or protocols), type (vulnerability, anomaly, or malware), as well as researcher's action (inform, detect, prevent or removal). While vulnerability and anomaly are connected with the keyword "threat", malware or botnets are linked with the keyword "attack".

**Table 1: Some IoT security challenges captured in research to detect. Prevent, or Create Awareness**

| Year | Study | Investigation | Mit. Tech. | Tool | Action | Domain | Implementation |
|---|---|---|---|---|---|---|---|
| 2019 | [36] | Vulnerability | Signature | application | Detection | Network | Modulated network scanning & database querying |
| 2017 | [41] | Vulnerability exploitation | Signature | Cloud service with vulnerability mitigation policies, security appliance, synchronization and communication mechanism | Prevention | Network | Cloud-based framework to control network flow by activating vulnerability mitigation policy that blocks Source IPs of verified malware servers. |
| 2020 | [42] | Studies in IIOT vulnerabilities | Signature/ Behavior | Used Mirai malware script in a server, default username & Password | Analysis | Industrial Internet of Things | Analysis of security vulnerabilities in IIOT to create situational awareness, test analysis knowledge to access to IIOT system using Mirai botnet. |
| 2015 | [43] | IoT network security | Signature | Policies, Learning mechanism for normal & attack profiles, enforcement rule set | Prevention | Network | Suggest attack learning signature to effect cross-device dependencies. |
| 2018 | [44] | Compromised Devices IoT in | Behavior-based | Context-based pairing,<br>ML algorithm | Detection/Prevention/ Removal | IoT Network core | Pairing associated devices working in user's trust zone, identifying compromised devices, removing them from larger networks |
| 2020 | [45] | Vulnerabilities in devices | Signature/ Behavior | Proof of Concept | Prevention | IoT Devices | Investigate feasible ways for infecting IoT devices. & Dev. vulnerabilities Proof of concept to warn manufacturers |
| 2021 | [46] | Vulnerabilities from Device misconfigurations | Signature/ Behavior | Six honey- pots | Prevention | IoT Devices | Scanning of internet network(IPV4) to reveal attacks from device misconfiguration |
| 2021 | [47] | Malware | - | Multiple disassemblers | Detection/Analyze/Defuse | IoT Ecosystems | Combining Disassemblers for IoT system troubleshooting |

| Year | Study | Investigation | Mit. Tech. | Tool | Action | Domain | Implementation |
|---|---|---|---|---|---|---|---|
| 2019 | [48] | vulnerabilities | Signature/ Behavior | Responsible reporting | Prevention | IoT Ecosystem | Engage hackers to discover vulnerabilities in exchange for incentives |
| 2019 | [49] | Anomaly-based malware attack | Signature/ Behavior | Intercept function, binary computation &signature repository | Prevention | Application | Locates system call table & replaces execve's address with intercepting function, computes SHA256-digest and uses it with intercepting function to match whitelist repository of malware |
| 2020 | [50] | Anomaly analysis | Behavior | Network traffic capturer, Fingerprinting data structure, ML | Detection | IoT Protocols | Capture Wi-Fi & Bluetooth traffic, map Wi-Fi traffic into observation flow and n-gram into representation for analysis, build model with which normal traffic behavior is characterized. |
| 2019 | [51] | Malware | Signature | ML classifier& constructor, feature vector database, and Policy module | Detection | Network traffic | Develop a four-module detection system that capture & classify network traffic, construct a training model from feature vectors stored in packet traffic database, then test new traffic for malware. Policy is also set as guide for classifying newly detected malware. |
| 2019 | [54] | Malware | Signature/ Behavior | Decompiler for reverse engineering, Shodan internet search engine for connected devices, Censys attack management tool. | Detection/ Prevention | IoT devices, IoT networks | Analyzed IoT endpoints which act as dropzones as well as their targets, reverse-engineer malware samples to extract behavior-based strings to obtain IP addresses, used internet connected devices search engine and attack surface management tool to obtain the IP addresses information |
| 2019 | [56] | Vulnerability/ Anomaly/ Malware | Signature/ Behavior | Free style | Detection/inform | IoT ecosystem | A platform that uses block-chain technology to manage third-party security detection for worthy incentives |
| 2020 | [57] | Vulnerability | Not available | Counter values of different network parameters | Detection | Network | Software Defined framework, an application based on counter values of different network parameters for DDOS attack detection |

| **Year** | **Study** | **Investigation** | **Mit. Tech.** | **Tool** | **Action** | **Domain** | **Implementation** |
|---|---|---|---|---|---|---|---|
| 2021 | [58] | Anomaly detection | Rule-base event detection, | ADS/EDS/ ML | Prevention/ detection | IoT ecosystem | Integrate event detection and anomaly detection into IoT systems for speed and reliability |
| 2021 | [59] | Vulnerability Prevention | Not available | Malware detection script | Rasberry Pi<br>Camera<br>Rasbian OS<br>PyCham<br>IDE<br>Python | Application/ Network | The authors wrote an attack script which they used to identify vulnerabilities which lead to brute-force attack and scan for open ports, detect if machine is vulnerable to DOS or DDOS |

## IV Summary, Conclusion, Recommendation and Contribution

A critical study of semi-conductors' design and fabrications origin, revealed great investments and provision of low- cost functional semi-conductor products such as sensors, actuators, MCUs, network and communications devices. This poses security challenges since high demand of these products has resulted in manufacturers focusing on producing functional devices while security is given little no attention. active version and qualified labor by China, ex-rayed vulnerabilities, anomalies, and malware attacks of IoT ecosystem. The ecosystem is made up of communicating IoT devices, the connecting internet network, various protocols, application platform them enable them to communicate. The following are popular actions taken to mitigate various attacks, anomalies, or vulnerabilities in the IoT ecosystem:

1. Vulderability, anomaly, and malwares have greatly increased because of the prevalence of the system following its many benefits.
2. The conglomeration of systems from different manufacturers whose products are aimed at providing functional and uniform services to consumers from differs societal strata (from a poor user of fire safety system, health monitoring wearable, to the rich person who uses a smartly monitored a pacemaker.
3. The summarized solutions range from vulnerability detection in network application, device or entire ecosystem, by standard methods such as network scanning, traffic capturing, or vulnerability open port search, feature extraction, characterization of feature, classification, model building and testing cleaning preprocessing and model building and training and utilizing captured or imported datasets. This study therefore gives an overall insight into the risks associated with the deployment of IoT ecosystem where is to provide a guide to people planning on deploying smart systems that require transmission of sensitive or classified information.
4. Having a trust zone where related (save devices) can be paired
5. Following any of Signature or Behavior mitigation technologies
6. Following Machine learning or Statistics analysis methods
7. Availability of Malware repositories such as VirusTotal, Quixxi, Androtootal, Jag.Alibaba, Ostorlab, Htbridge, & Shodan
8. Availability of datasets which may be used independently as historical dataset to gain insight or together with freshly captured data. Some of the datasets used in the various studies reviewed are:

Machine learning is the most used detection/prevention method as it allows feature selection, classification, data cleaning as well as model building for malware and normal and attack data. Despite good performance of classifiers (Supervised learning) and clustering algorithms, Reinforcement learning applications prove highly effective in vulnerability discovery as that use algorithms that enable them comb through the available system and discover an anomaly.

In conclusion, the researcher wishes to reiterate that this work is intended to offer Situational awareness to Cyber threat novices who happen to love technology, and have or intends to establish a smart network. Tech-philia has left many going from one tech system to another without working out the security implications for themselves, the enterprise they represent, or the country at large. Also, the work of [78] directs Cyber Security scholars on the required Certification for securing the emerging and thriving field of IoTs and Cloud networks, as well as related fields of Network, hardware and software security. With CISCO's prediction of over 50 billion IoT connections, it is evident that the E-third Eye paradigm will rise exponentially as connections increase.

**Recommendation**

The researcher recommends that:

1. multiple machine learning types may be applied to a particular detection problem so as to obtain more accurate results. Example is the use of a reinforcement learning method after classification.
2. ethical hacking, SmartCrowd, and CrowdSource responsible reporting for reward should be adopted by device manufacturers all IoT related Service providers.
3. proof of concept notes generated after careful detection experiments should be made available as guide to manufacturers and network service providers
4. for every Internet of things deployment plan, appropriate security plan must be adopted, and encryption at various levels implemented.
5. companies offering smart solutions should have Cyber security certificated staff that will enlighten consumers on security best practices.
6. cyber security should be built into schools' curriculum.
7. smart TV users should scan their TVs with better antivirus, scan each of the devices connected to a network.

**Contribution To Body of Research**

This work contributes to the body of research by explicitly highlighting procedures for carrying out standalone reviews. These steps are implemented by some review papers without giving a background knowledge to readers for its implementation. In this paper however, attempt is made to help researcher understand the expectations of scientific reviews which involve both quantitative and qualitative analysis, the need to outline search criteria, sources and number of papers utilized from each source also serve as guide for systematic reviews. Secondly, it provides a platform for enterprises and individuals to easily view security measures that have been validated by research, by providing a table (Table 1) which presents a total of 17 articles containing various detection, prevention or removal approach to IoT security, with most implementing a hybrid of security techniques. This can also be a guide to career development or provide insight for a deep dive of any of the techniques.

## References

[1] I. Butun, P. Österberg, & H. S.-I. C. S., and undefined 2019, "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures," *ieeexplore.ieee.org*, p. 1, 2019.

[2] "How to Secure Wireless Sensor Networks - Tech Briefs." https://www.techbriefs.com/component/content/article/tb/supplements/st/features/articles/28527 (accessed Feb. 28, 2022).

[3] "The Top 10 Sensor Types in IoT and their Applications." https://www.nabto.com/iot-sensor-types/ (accessed Feb. 28, 2022).

[4] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," *J. Electr. Comput. Eng.*, vol. 2017, 2017, doi: 10.1155/2017/9324035.

[5] B. C. Patel, G. R. Sinha, and N. Goel, "Introduction to sensors," *Adv. Mod. Sensors*, Nov. 2020, doi: 10.1088/978-0-7503-2707-7CH1.

[6] "What is a Sensor? Different Types of Sensors with Applications." https://www.electricaltechnology.org/2018/11/types-sensors-applications.html (accessed Mar. 01, 2022).

[7] S. B. Joseph, E. G. Dada, and M. S. Abdullahi, "Development of Internet of Things (IoT) Based Energy Consumption Monitoring and Device Control System," *NIPES J. Sci. Technol. Res.*, vol. 2, no. 3, p. 85,

2020, doi: 10.37933/nipes/2.3.2020.9.

[8] O. Mostofi, “Offshore Outsourcing of the United States Semiconductor Manufacturing : Management Approaches and Strategies,” *Walden Univ. Sch. Walden*, 2017.

[9] V. Makrakis, V. Makrakis, and L. Yuan-tu, “Informatics, Development, and Education: The Case of China,” *Educ. Technol.*, vol. 33, no. 9, pp. 31–37, 1993.

[10] Olebara C. C., “Improved Yuanpei computer science teaching: For secured development of developing countries | Journal of Emerging Technologies,” 2022. https://journals.jfppublishers.com/jet/article/view/134 (accessed Mar. 01, 2022).

[11] Lithotechsolutions, “Current Status of the Integrated Circuit Industry in China,” *J. Microelectron. Manuf.*, vol. 1, no. 1, pp. 1–8, 2018, doi: 10.33079/jomm.18010105.

[12] G. Sharma, A. Kumar, and V. Sharma, “WINDOWS OPERATING SYSTEM VULNERABILITIES,” *Int. J. Comput. Corp. Res.*, vol. 1, no. 3, 2011.

[13] A. " Bunnie and " Huang, “Keeping Secrets in Hardware: the Microsoft XBox TM Case Study,” *MIT LAB*, vol. AI Memo, 2002.

[14] K. Paul, “Replicant developers find and close Samsung Galaxy backdoor — Free Software Foundation — Working together for free software.” https://www.fsf.org/blogs/community/replicant-developers-find-and-close-samsung-galaxy-backdoor (accessed Mar. 01, 2022).

[15] Y. Jin and Y. Makris, “Hardware Trojans in Wireless Cryptographic ICs,” *IEEE Des. Test Comput.*, 2010.

[16] Joel, “Researchers find new, ultra-low-level method of hacking CPUs - and there’s no way to detect it - ExtremeTech.” https://www.extremetech.com/extreme/166580-researchers-find-new-ultra-low-level-method-of-hacking-cpus-and-theres-no-way-to-detect-it (accessed Mar. 01, 2022).

[17] J. Da Rolt, G. Di Natale, M. L. Flottes, and B. Rouzeyre, “New security threats against chips containing scan chain structures,” *2011 IEEE Int. Symp. Hardware-Oriented Secur. Trust. HOST 2011*, pp. 105–110, 2011, doi: 10.1109/HST.2011.5955005.

[18] S. Skorobogatov, “The bumpy road towards iPhone 5c NAND mirroring,” *Univ. Cambridge Comput. Lab. Cambridge*, pp. 1–10, 2016.

[19] “Hunting For Backdoors In IoT Firmware At Unprecedented Scale PDF Documents Library.” https://e-dokumen.com/document/60877_hunting-for-backdoors-in-iot-firmware-at-unprecedented-scale.html (accessed May 29, 2022).

[20] T. Brewster, “Here’s How The CIA Allegedly Hacked Samsung Smart TVs -- And How To Protect Yourself.” https://www.forbes.com/sites/thomasbrewster/2017/03/07/cia-wikileaks-samsung-smart-tv-hack-security/?sh=692f43864bcd (accessed Mar. 02, 2022).

[21] I. Butun, P. Osterberg, and H. Song, “Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures,” *IEEE Commun. Surv. Tutorials*, vol. 22, no. 1, pp. 616–644, 2020, doi: 10.1109/COMST.2019.2953364.

[22] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner, “Smart locks: Lessons for securing commodity internet of things devices,” *ASIA CCS 2016 - Proc. 11th ACM Asia Conf. Comput. Commun. Secur.*, pp. 461–472, May 2016, doi: 10.1145/2897845.2897886.

[23] D. D. López, M. B. U.-… and M. Computing, and undefined 2018, “Shielding IoT against cyber-attacks: An event-based approach using SIEM,” *hindawi.com*. https://downloads.hindawi.com/journals/wcmc/2018/3029638.pdf Accessed 2022-03-01

[24] C.-C. Lee, “Security and Privacy in Wireless Sensor Networks: Advances and Challenges,” 2020, doi: 10.3390/s20030744.

[25] T. Unkašević, Z. Banjac, and M. Milosavljević, “A Generic Model of the Pseudo-Random Generator Based on Permutations Suitable for Security Solutions in Computationally-Constrained Environments,” *Sensors 2019, Vol. 19, Page 5322*, vol. 19, no. 23, p. 5322, Dec. 2019, doi: 10.3390/S19235322.

[26] R. Ostadal, V. Matyas, P. Svenda, and L. Nemec, “Crowdsourced Security Reconstitution for Wireless Sensor Networks: Secrecy Amplification,” *Sensors (Basel).*, vol. 19, no. 22, Nov. 2019, doi: 10.3390/S19225041.

[27] Q. Shen, W. Liu, Y. Lin, and Y. Zhu, “Designing an Image Encryption Scheme Based on Compressive Sensing and Non-Uniform Quantization for Wireless Visual Sensor Networks,” *Sensors 2019, Vol. 19, Page 3081*, vol. 19, no. 14, p. 3081, Jul. 2019, doi: 10.3390/S19143081.

[28] U. Gulen, A. Alkhodary, and S. Baktir, “Implementing RSA for Wireless Sensor Nodes,” *Sensors (Basel).*, vol. 19, no. 13, Jul. 2019, doi: 10.3390/S19132864.

[29] J. Furtak, Z. Zieliński, and J. Chudzikiewicz, “A Framework for Constructing a Secure Domain of Sensor Nodes,” *Sensors (Basel).*, vol. 19, no. 12, Jun. 2019, doi: 10.3390/S19122797.

[30] B. Zhu, W. Susilo, J. Qin, F. Guo, Z. Zhao, and J. Ma, “A Secure and Efficient Data Sharing and Searching Scheme in Wireless Sensor Networks,” *Sensors (Basel).*, vol. 19, no. 11, Jun. 2019, doi: 10.3390/S19112583.

[31] C. F. Lee, J. J. Shen, Z. R. Chen, and S. Agrawal, “Self-Embedding Authentication Watermarking with Effective Tampered Location Detection and High-Quality Image Recovery,” *Sensors (Basel).*, vol. 19, no. 10, May 2019, doi: 10.3390/S19102267.

[32] D. Hlusicka, “How to scan Samsung Smart TV for viruses? - YouTube.” https://www.youtube.com/watch?v=wLyQoKPZWtM (accessed Mar. 02, 2022).

[33] “Advanced Malware Detection - Signatures vs. Behavior Analysis - Infosecurity Magazine.” https://www.infosecurity-magazine.com/opinions/malware-detection-signatures/ (accessed May 24, 2022).

[34] C. C. Olebara, “Researchers ’ Cyber First-Aid,” *Journal of Emerging Technologies*, *2*(1), 42-54. Retrieved from https://journals.jozacpublishers.com/jet/article/view/195

[35] C.- Olebara, Comfort & Osuagwu, “Detection of Hardware Backdoor Through Microcontroller Read Time Analysis,” *West African J. Ind. Acad. Res.*, 2016.

[36] R. Egert, T. Grube, D. Born, and M. Muhlhauser, “Modular vulnerability indication for the IoT in IP-based networks,” *2019 IEEE Globecom Work. GC Wkshps 2019 - Proc.*, 2019, doi: 10.1109/GCWkshps45667.2019.9024519.

[37] “VULNERABILITY | meaning in the Cambridge English Dictionary.” https://dictionary.cambridge.org/dictionary/english/vulnerability (accessed May 24, 2022).

[38] C. Olebara, Comfort; Osuagwu, oliver & Chukwudebe, “Simulation of Microcontroller Behavior for Hardware Backdoor Detection,” *D U ST RIA West African J. Ind. Acad. Res.*, vol. Vol. 19, no. 2, pp. 14–22, 2018. https://www.wajiaredu.com.ng/wp-content/uploads/2019/06/West-African-Journal-of-Industrial-VOL19Prof-Nwosu.pdf

[39] M. J. Page *et al.*, “The prisma 2020 statement: An updated guideline for reporting systematic reviews,” *Med. Flum.*, vol. 57, no. 4, pp. 444–465, 2021, doi: 10.21860/medflum2021_264903.

[40] C. Okoli, “A guide to conducting a standalone systematic literature review,” *Commun. Assoc. Inf. Syst.*, vol. 37, no. 1, pp. 879–910, 2015, doi: 10.17705/1cais.03743.

[41] N. Hadar, S. Siboni, and Y. Elovici, “A lightweight vulnerability mitigation framework for IoT devices,” *IoT S P 2017 - Proc. 2017 Work. Internet Things Secur. Privacy, co-located with CCS 2017*, pp. 71–75, 2017, doi: 10.1145/3139937.3139944.

[42] X. Jiang, M. Lora, and S. Chattopadhyay, “An Experimental Analysis of Security Vulnerabilities in Industrial IoT Devices,” *ACM Trans. Internet Technol.*, vol. 20, no. 2, 2020, doi: 10.1145/3379542.

[43] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, “Handling a trillion (unfixable) flaws on a billion devices,” pp. 1–7, 2015, doi: 10.1145/2834050.2834095.

[44] M. Miettinen and A. R. Sadeghi, “Keynote: Internet of things or threats? On building trust in IoT,” *2018 Int. Conf. Hardware/Software Codesign Syst. Synth. CODES+ISSS 2018*, pp. 1–9, 2018, doi:

10.1109/CODESISSS.2018.8525931.

[45] C. Brierley, J. Pont, B. Arief, D. J. Barnes, and J. Hernandez-Castro, “PaperW8: An IoT bricking ransomware proof of concept,” *ACM Int. Conf. Proceeding Ser.*, 2020, doi: 10.1145/3407023.3407044.

[46] S. Srinivasa, J. M. Pedersen, and E. Vasilomanolakis, “Open for hire,” pp. 195–215, 2021, doi: 10.1145/3487552.3487833.

[47] S. Shaila, A. Darki, M. Faloutsos, N. Abu-Ghazaleh, and M. Sridharan, “DisCo: Combining disassemblers for improved performance,” *ACM Int. Conf. Proceeding Ser.*, pp. 148–161, 2021, doi: 10.1145/3471621.3471851.

[48] A. Y. Ding, G. L. De Jesus, and M. Janssen, “Ethical hacking for boosting IoT vulnerability management: A first look into bug bounty programs and responsible disclosure,” *ACM Int. Conf. Proceeding Ser.*, pp. 49–55, 2019, doi: 10.1145/3357767.3357774.

[49] D. Breitenbacher, I. Homoliak, Y. L. Aung, N. O. Tippenhauer, and Y. Elovici, “HADES-IoT: A practical host-based anomaly detection system for iot devices,” *AsiaCCS 2019 - Proc. 2019 ACM Asia Conf. Comput. Commun. Secur.*, pp. 479–484, 2019, doi: 10.1145/3321705.3329847.

[50] P. Satam, S. Satam, S. Hariri, and A. Alshawi, “Anomaly Behavior Analysis of IoT Protocols,” *Model. Des. Secur. Internet Things*, pp. 295–330, 2020, doi: 10.1002/9781119593386.ch13.

[51] A. Kumar and T. J. Lim, “EDIMA: Early Detection of IoT Malware Network Activity Using Machine Learning Techniques,” *IEEE 5th World Forum Internet Things, WF-IoT 2019 - Conf. Proc.*, pp. 289–294, 2019, doi: 10.1109/WF-IoT.2019.8767194.

[52] B. Genge and C. Enăchescu, “ShoVAT: Shodan-based vulnerability assessment tool for Internet-facing services,” *Secur. Commun. Networks*, vol. 9, no. 15, pp. 2696–2714, 2016, doi: 10.1002/sec.1262.

[53] “Shodan Search Engine.” https://www.shodan.io/ (accessed May 24, 2022).

[54] J. Choi, A. Anwar, H. Alasmary, J. Spaulding, D. Nyang, and A. Mohaisen, “IoT malware ecosystem in the wild,” pp. 413–418, 2019, doi: 10.1145/3318216.3363379.

[55] “Censys | Industry-Leading Cloud and Internet Asset Discovery Solutions.” https://censys.io/ (accessed May 25, 2022).

[56] B. Wu *et al.*, “SmartCrowd: Decentralized and automated incentives for distributed IoT system detection,” *Proc. - Int. Conf. Distrib. Comput. Syst.*, vol. 2019-July, pp. 1106–1116, 2019, doi: 10.1109/ICDCS.2019.00113.

[57] J. Bhayo, S. Hameed, and S. A. Shah, “An Efficient Counter-Based DDoS Attack Detection Framework Leveraging Software Defined IoT (SD-IoT),” *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3043082.

[58] A. Yahyaoui, T. Abdellatif, S. Yangui, and R. Attia, “READ-IoT: Reliable Event and Anomaly Detection Framework for the Internet of Things,” *IEEE Access*, vol. 9, pp. 24168–24186, 2021, doi: 10.1109/ACCESS.2021.3056149.

[59] H. S. Shreenidhi, S. Prabakar, and P. A. Kumar, “Intrution detection system Using IoT device for safety and security,” *Proc. 2nd IEEE Int. Conf. Comput. Intell. Knowl. Econ. ICCIKE 2021*, pp. 340–344, 2021, doi: 10.1109/ICCIKE51210.2021.9410730.

[60] I. Sahmi, T. Mazri, and N. Hmina, “Study of the different security threats on the internet of things and their applications,” *ACM Int. Conf. Proceeding Ser.*, vol. Part F1481, 2019, doi: 10.1145/3320326.3320402.

[61] A. Mangino, M. S. Pour, and E. Bou-Harb, “Internet-scale Insecurity of Consumer Internet of Things,” *ACM Trans. Manag. Inf. Syst.*, vol. 11, no. 4, 2020, doi: 10.1145/3394504.

[62] M. Chowdhury, B. Ray, S. Chowdhury, and S. Rajasegarar, “A Novel Insider Attack and Machine Learning Based Detection for the Internet of Things,” *ACM Trans. Internet Things*, vol. 2, no. 4, pp. 1–23, 2021, doi: 10.1145/3466721.

[63] T. Gu, A. Abhishek, H. Fu, H. Zhang, D. Basu, and P. Mohapatra, "Towards Learning-automation IoT Attack Detection through Reinforcement Learning," *Proc. - 21st IEEE Int. Symp. a World Wireless, Mob. Multimed. Networks, WoWMoM 2020*, pp. 88–97, 2020, doi: 10.1109/WoWMoM49955.2020.00029.

[64] Y. Wang, J. Shen, J. Lin, and R. Lou, "Staged Method of Code Similarity Analysis for Firmware Vulnerability Detection," *IEEE Access*, vol. 7, pp. 14171–14185, 2019, doi: 10.1109/ACCESS.2019.2893733.

[65] A. Al-Abassi, H. Karimipour, A. Dehghantanha, and R. M. Parizi, "An ensemble deep learning-based cyber-attack detection in industrial control system," *IEEE Access*, vol. 8, pp. 83965–83973, 2020, doi: 10.1109/ACCESS.2020.2992249.

[66] M. M. Rashid, J. Kamruzzaman, M. M. Hassan, T. Imam, and S. Gordon, "Cyberattacks detection in iot-based smart city applications using machine learning techniques," *Int. J. Environ. Res. Public Health*, vol. 17, no. 24, pp. 1–21, 2020, doi: 10.3390/ijerph17249347.

[67] C. Yang *et al.*, "A convolutional neural network based classifier for uncompressed malware samples," *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 15–17, 2018, doi: 10.1145/3267494.3267496.

[68] Y. An, F. R. Yu, J. Li, J. Chen, and V. C. M. Leung, "Edge Intelligence (EI)-Enabled HTTP Anomaly Detection Framework for the Internet of Things (IoT)," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3554–3566, 2021, doi: 10.1109/JIOT.2020.3024645.

[69] I. Ullah and Q. H. Mahmoud, "A Two-Level Hybrid Model for Anomalous Activity Detection in IoT Networks," *2019 16th IEEE Annu. Consum. Commun. Netw. Conf. CCNC 2019*, pp. 1–6, 2019, doi: 10.1109/CCNC.2019.8651782.

[70] S. Haq and Y. Singh, "Botnet detection using machine learning," *PDGC 2018 - 2018 5th Int. Conf. Parallel, Distrib. Grid Comput.*, pp. 240–245, 2018, doi: 10.1109/PDGC.2018.8745912.

[71] R. P. Markiewicz and D. Sgandurra, "Clust-IT: Clustering-based intrusion detection in IoT environments," *ACM Int. Conf. Proceeding Ser.*, 2020, doi: 10.1145/3407023.3409201.

[72] H. T. Nguyen, D. H. Nguyen, Q. D. Ngo, V. H. Tran, and V. H. Le, "Towards a rooted subgraph classifier for IoT botnet detection," *ACM Int. Conf. Proceeding Ser.*, pp. 247–251, 2019, doi: 10.1145/3348445.3348474.

[73] Y. Yue, S. Li, P. Legg, and F. Li, "Deep Learning-Based Security Behaviour Analysis in IoT Environments: A Survey," *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/8873195.

[74] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT Security Techniques Based on Machine Learning," pp. 1–20, 2018.

[75] W. L. Chin, W. Li, and H. H. Chen, "Energy Big Data Security Threats in IoT-Based Smart Grid Communications," *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 70–75, 2017, doi: 10.1109/MCOM.2017.1700154.

[76] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019, doi: 10.1109/COMST.2019.2910750.

[77] W. Xie, Y. Jiang, Y. Tang, N. Ding, and Y. Gao, "Vulnerability detection in IoT firmware: A Survey," *Proc. Int. Conf. Parallel Distrib. Syst. - ICPADS*, vol. 2017-Decem, pp. 769–772, 2018, doi: 10.1109/ICPADS.2017.00104.

[78] E. C. Davri *et al.*, "Cyber security certification programmes," *Proc. 2021 IEEE Int. Conf. Cyber Secur. Resilience, CSR 2021*, pp. 428–435, Jul. 2021, doi: 10.1109/CSR51186.2021.9527974.