energies

MDPI

Article

IoVT: Internet of Vulnerable Things? Threat Architecture, Attack Surfaces, and Vulnerabilities in Internet of Things and Its Applications towards Smart Grids

Pooja Anand [1], Yashwant Singh [1], Arvind Selwal [1], Pradeep Kumar Singh [2,*], Raluca Andreea Felseghi [3] and Maria Simona Raboaca [4,*]

1 Department of Computer Science and Information Technology, Central University of Jammu, Jammu and Kashmir, Pin 181143, India; poojaanand892@gmail.com (P.A.); yashwant.csit@cujammu.ac.in (Y.S.); arvind.csit@cujammu.ac.in (A.S.)
2 ABES Engineering College, Ghaziabad, Uttar Pradesh, Pin 201009, India
3 Faculty of Electrical Engineering and Computer Science, "Ştefancel Mare" University of Suceava, 720229 Suceava, Romania; Raluca.FELSEGHI@insta.utcluj.ro
4 National Research and Development Institute for Cryogenic and Isotopic Technologies—ICSI Rm. Valcea, Uzinei Street, No. 4, P.O. Box 7 Raureni, 240050 Valcea, Romania
* Correspondence: pradeep84cs@yahoo.com (P.K.S.); siomona.raboaca@icsi.ro (M.S.R.)

Received: 9 August 2020; Accepted: 12 September 2020; Published: 15 September 2020

Abstract: In recent years, people have witnessed numerous Internet of Things (IoT)-based attacks with the exponential increase in the number of IoT devices. Alongside this, the means to secure IoT-based applications are maturing slower than our budding dependence on them. Moreover, the vulnerabilities in an IoT system are exploited in chains to penetrate deep into the network and yield more adverse aftereffects. To mitigate these issues, this paper gives unique insights for handling the growing vulnerabilities in common IoT devices and proposes a threat architecture for IoT, addressing threats in the context of a three-layer IoT reference architecture. Furthermore, the vulnerabilities exploited at the several IoT attack surfaces and the challenges they exert are explored. Thereafter, the challenges in quantifying the IoT vulnerabilities with the existing framework are also analyzed. The study also covers a case study on the Intelligent Transportation System, covering road transport and traffic control specifically in terms of threats and vulnerabilities. Another case study on secure energy management in the Smart Grid is also presented. This case study covers the applications of Internet of Vulnerable Things (IoVT) in Smart energy Grid solutions, as there will be tremendous use of IoT in future Smart Grids to save energy and improve overall distribution. The analysis shows that the integration of the proposed architecture in existing applications alarms the developers about the embedded threats in the system.

Keywords: IoT; threats; vulnerabilities; architecture; attack surfaces; smart grid

1. Introduction

In the near future, the Internet of Things (IoT) will engage billions of smart devices (their global increase is depicted in Figure 1). It works by connecting various kinds of things to the Internet, so as to harvest data bred by sensors, and remotely control and monitor environments [1]. This makes the IoT applicable in multiple domains, leveraging various monetary and personal benefits. Thus, weaving numerous threats in people's lives, broadly in terms of security and privacy. As commercial IoT products come with ill-designed and incomplete security mechanisms, these threats could be

life-threatening as well. Moreover, being heterogeneous and resource constraint in terms of storage, energy, computation, and communication prevents them to adopt standard security mechanisms benefitted by traditional Internet-connected devices [2]. Besides this, IoT stakeholders and users are less aware of the security risks complementary with connecting their day-to-day devices to a worldwide network. Thus, providing the much larger landscape of threats to the adversaries.

In general, the things we connect to the Internet to avail smart services are commonly the vulnerable things [3]. It is found that IoT devices are shipped with known vulnerabilities to the consumers. To name a few, with outdated operating system (OS) versions, poor support for firmware and OS updates, hard-coded passwords with no mechanisms to change, holes to inject malicious code, and open Telnet ports [4]. For instance, the Mirai botnet created its army of bots by exploring the Internet by trying different combinations of default usernames and passwords to get control of these vulnerable IoT devices [5]. This attack would not have been possible if default passwords of IoT devices were changed in a timely manner. Thus, intruders easily exploit weak IoT devices, as traditional networks are safeguarded with stable defensive mechanisms.

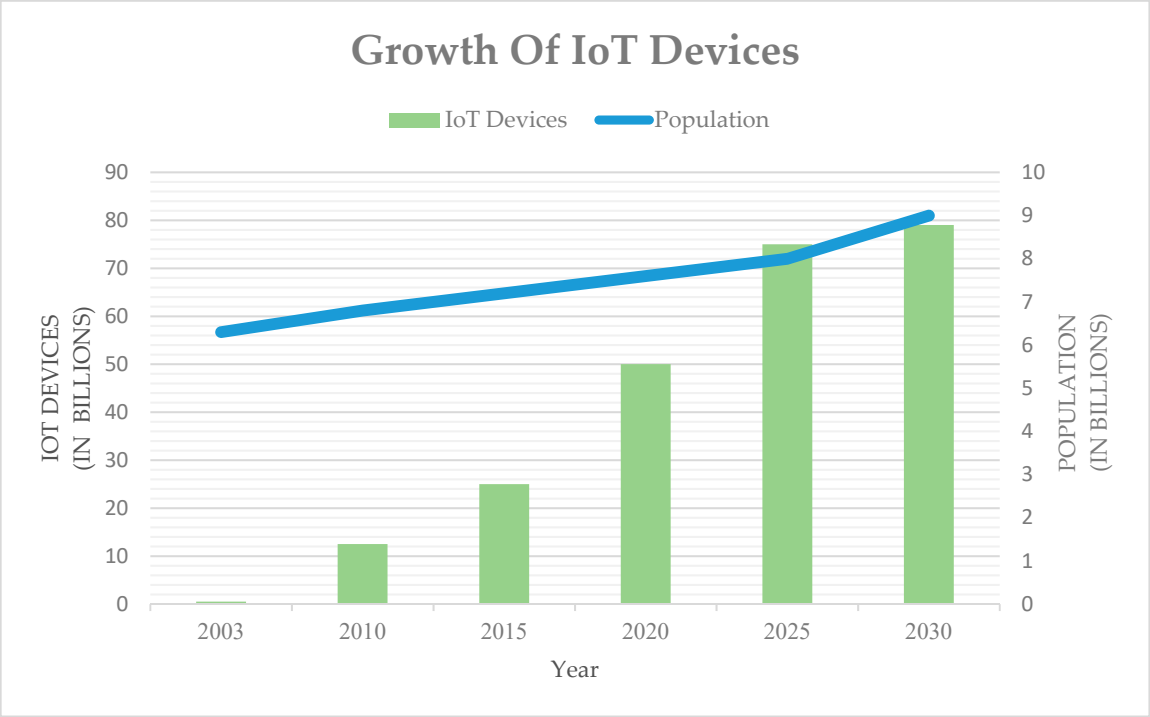

Figure 1. Growth of Internet of Things (IoT) Devices with Population [6].

In this paper, the main focus is on the "vulnerabilities in the IoT space", as these vulnerabilities of IoT devices serve as the doorway to launch numerous attacks. These vulnerabilities range from exploiting a single device to those that have enabled IoT-based botnets like Mirai. As an extension, they can even impact the well-being of human life. It is reported that 70 percent of smart devices are vulnerable to several cyberattacks [7]. Furthermore, these exploited devices are distributed world-wide with China hosting the maximum number of exploited IoT devices as depicted in Figure 2. Likewise, as per the reports by the end of 2020, compromised IoT devices will launch more than 25% of industrial attacks [8]. This rigorousness could be realized from the cyber-attacks like the Iran Nuclear System Stuxnet attack [9], a blast furnace attack at a German steel mill [10], the deadliest attack on oil facilities of Saudi Arabia, Mirai, Hajime botnet, and BrikerBot [5].

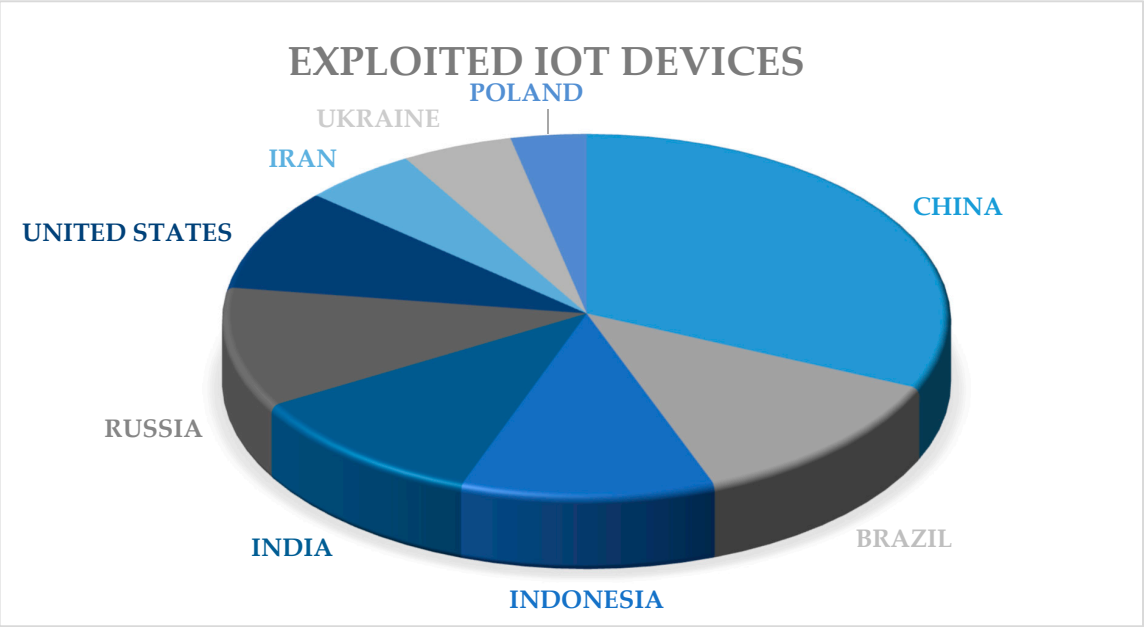

Figure 2. Distribution of Exploited IoT Devices [11].

The main motivation for the given study is as follows:

- As per the literature reviewed, only generic threat models like STRIDE, DREAD, OCTAVE, and PASTA are given, which mainly covers the threats; no threat model specific to IoT has been given. Therefore, there is a need to devise a generic threat model for IoT because the aforementioned models have originally been devised for conventional IT systems, which are considerably different in terms of functionality and design.
- Moreover, from the studied start of the art, we found that only few works have specifically focused on threat and vulnerability modelling. Consequently, in this article, we focused on the same.
- We are also motivated to focus on the root cause of these nascent attacks and threats, namely the vulnerabilities in IoT devices taken care of by potential adversaries. The common vulnerabilities in IoT have been identified in the proposed threat architecture and few are illustrated in terms of their severity as per the Common Vulnerability Scoring System (CVSS).

The overpowering services of the IoT pervaded in our lives also empowers their consequential security flaws. For meeting their growing demands, they are flooded in the market with known vulnerabilities without giving an afterthought to their security considerations. The key contributions of this paper are as follows:

- The proposed Threat Architecture of IoT, which demonstrates various threats to be taken care of while developing an IoT system.
- The major attack surfaces in IoT are highlighted in a bottom-up fashion.
- The common vulnerabilities in IoT and their impact in terms of their exploitability as per the CVSS version 2 and CVSS version 3 by National Vulnerability Database (NVD) are illustrated.
- Lastly, two case studies are presented which covers the Intelligent Transportation System and Secure Energy management. The second case study covers the applicability of IoT and Internet of Vulnerable Things (IoVT) for smart energy grids.

This paper emphasizes the transition of the Internet of Things to the Internet of Vulnerable Things. The subsequent sections are organized as follows and depicted in Figure 3. In Section 2, we present the background for the proposed study and subsequently proposed the IoT Threat Architecture in Section 3. In Section 4, we talk about the attack surfaces in an IoT system. Thereafter, we discuss

the security vulnerabilities and their impact as a whole in Section 5. Following this, we present a case study on the intelligent transportation system in Section 6, followed by a use case in Section 7 on secure energy management in Smart Grids. Finally, we conclude the article with a view towards recommendations to cope up with growing threats and vulnerabilities in IoT.

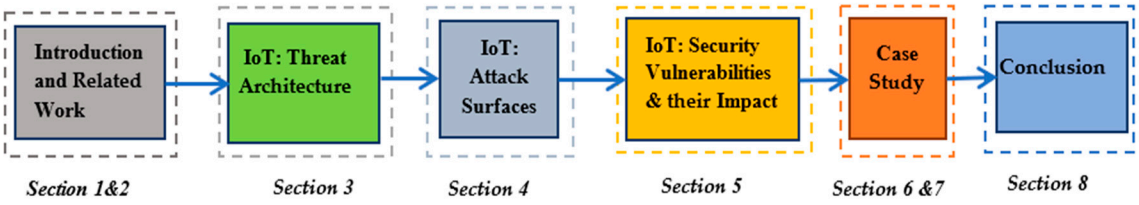

Figure 3. Roadmap of the Article.

2. Related Work

To address different aspects of security in an IoT system, several works exist in the literature. The authors have adopted a methodical approach to direct this study in a systematic way to give a clear idea of vulnerabilities in the IoT system, the root cause questioning the sustenance of IoT. The relevant articles, technical reports, blogs, tutorial papers, and white papers have been identified to conduct this study. The identified data have also undergone quality checks to extract reliable information for the proposed work. The ones with a fair number of citations are generally the preferred one. This work mainly focused on state-of-the-art research on threats, vulnerabilities, and their modelling in general and in the context of smart grids, specifically. The peer-reviewed database journals with high-quality and trustworthy research, like IEEEXplore, Springer, MDPI, Wiley, ACM, Elsevier, etc., are explored to get the relevant literature. For the search criteria, keywords like IoT Vulnerabilities, Threats, Attack surfaces, Vulnerability Scoring, Smart Grid, etc., have been used. The authors have also analyzed, cited, and acknowledged the related works as per the discussed theme of the proposed survey.

In the studied literature, the number of threat models like OCTAVE, STRIDE, DREAD, PASTA have been given to identify the threats and vulnerabilities. Some of them, like CVSS and DREAD, also score them as per the risk associated with these threats. However, it is seen that all of them are generic, none encountering the same problem in terms of IoT. Being developed for conventional IT systems, it is not worthy to use the same for IoT systems. As IoT devices are different in terms of functionality, resources, communication, constraints, and design. Therefore, a specific model must be developed to identify the threats and vulnerabilities in IoT, and to quantify them as per the loss they can cause. The different IoT architectures, security threats, and vulnerabilities are considered with respect to different layers in the reviewed literature. But none of them address the discussed issue in the correct way. A brief review in terms of relative efforts is given in Table 1 to highlight the contribution of this work. For example, Babar et al. [12] have given a security model for IoT that covers three aspects: trust, security, and privacy. The given model explores threats for communication protocols, identity management, storage, and physical threats, though it does not cover IoT-attacks against interlinked systems. In [13], intrinsic and extrinsic attack models are studied in different IoT paradigms in the context of centralization and connectivity. The authors have also examined the fuzzy-based internal/external bad actors for threats such as DoS, eavesdropping, and physical threats.

In another work, Humayed et al. [14] design a framework for cyber-physical security. The proposed framework works in three modules. The security module works upon security controls, threats, and vulnerabilities. The cyber-physical module explores components comprising cyber, physical, and their combination. The system module examines several IoT application domains for analyzing threats specific to them. Additionally, Mosenia and Jha [15] cover the security aspect of IoT in three levels in the proposed security model. In the first level, Radio-frequency identification (RFID) and sensors, i.e., edge nodes are covered. Then, the threats, vulnerabilities, and remediations for communication follow edge computing.

Yaqoob et al. [16] discussed IoT architecture in terms of key requirements with future research directions. Several parameters, including applications, network topologies, and supporting technologies are covered concerning IoT architecture. The authors have also given the IoT architectures in the context of real paradigms. In another notable work [17], IoT security is studied in multiple domains like RFid, smart home, sensor networks, smart health services, smart cities, and end-users. The threat taxonomy covering parameters like threats, IEEE standards, enabling technologies, and deployment levels are devised.

HaddadPajouh et al. [18] proposed a security architecture, called AI4SAFE-IoT, specifically focusing on the infrastructure of the edge layer of IoT. The proposed architecture comprised of AI-based security modules working on the edge layer to secure the IoT infrastructure. These modules included intelligent firewalls for web applications, threats, threat attributes, and threat hunting. On the basis of the kill chain model, the phase of the life-cycle of an attack is identified by the modules. Additionally, each module is designed to work against several threats in the context of IoT applications. In recent work, Gupta et al. [19] proposed a machine learning-based threat model covering different parameters like reliability, attacks, accuracy, and latency. The authors also designed a deep learning-based secure architecture classifying the normal data from attack data.

Table 1. A relative comparison of the proposed work with state-of-the-art works.

Author(s)	Year	Discussion	Future Work	1	2	3	4	5	6
Humayed et al. [14]	2017	The cyber-physical framework that covers threats, vulnerabilities, and action in the context of smart grid, smart cars, medical devices, and industrial control systems.	The application-specific solutions for the growing threats and vulnerabilities will be identified.	✓	✓	X	✓	✓	✓
Mosenia and Jha et al. [15]	2017	The threats, vulnerabilities, and countermeasures with respect to the edge layer of IoT.	To find solutions to proactively address the identified threats.	X	✓	X	X	X	✓
Yaqoob et al. [17]	2017	The general IoT security concerns with threats and ransomware attacks.	IoT vulnerabilities must be proactively mitigated as prevention to ransomwares.	X	✓	X	X	X	✓
Alaba et al. [20]	2017	The different IoT security scenarios, security matrix, and remediation strategies.	Secure smart applications (smart grid) with lightweight authentication.	X	✓	✓	X	X	✓
Samaila et al. [21]	2018	The threat models for different applications with their solutions.	A reliable model to find the power consumption of cryptographic schemes.	✓	X	✓	X	✓	✓
Makhdoom et al. [7]	2018	IoT attacks with approaches, malwares, and vulnerabilities.	Specific security measures for different threat environments and use cases.	X	✓	✓	X	X	✓
Xiao et al. [22]	2018	IoT threat model with machine learning security solutions.	Lessen the overhead in machine learning-based solutions.	✓	✓	X	X	X	✓
Frustaci et al. [23]	2018	Analysis of IoT layers in terms of threats.	Device-level security at the physical layer (most vulnerable).	X	✓	X	X	X	✓

Table 1. *Cont.*

Author(s)	Year	Discussion	Future Work	1	2	3	4	5	6
Koloveas et al. [24]	2019	Threat intelligence in IoT using crawler-based architecture.	To extract cyber-threat intelligence using Natural language understanding	✓	✓	X	X	X	✓
Grammatikis et al. [25]	2019	Risk analysis of threats with respect to all the layers of IoT	To detect cyber-attacks (high accuracy) with Software-defined networking (SDN).	X	✓	X	X	X	✓
Meneghello et al. [26]	2019	Security goals, threats, vulnerabilities with respect to protocols with practical implementation.	To manage the shared cryptographic keys in various protocols.	✓	✓	✓	X	X	✓
Haddadpajouh et al. [18]	2020	Edge layer-based a security architecture with threat hunting modules.	To be implemented in different practical scenarios.	✓	✓	X	✓	X	✓
Yazdinejad et al. [27]	2020	Secure file transferring and access control with blockchain in IoT.	To be compared with few more architectures.	X	✓	X	X	X	✓
Butun et al. [28]	2020	IoT security attacks with their defense mechanisms.	De-facto security standards for IoT and WSNs	X	✓	X	X	X	✓
The proposed one	2020	Threat Architecture of IoT, and secure energy management with Smart Grid.	To propose a framework for assessing and quantifying vulnerabilities in IoT.	✓	✓	✓	✓	✓	✓

Note: 1, threat architecture; 2, attack surfaces; 3, recent vulnerabilities; 4, smart transportation; 5, smart grid; 6, general threats. Notations: ✓, considered; X, not considered.

Koloveas et al. [24] presented a crawler-based architecture working on data gathered from social, clear, and dark web to provide threat intelligence in IoT. The architecture worked in two phases, based on machine learning and statistical language. In another notable work [29], the authors proposed a security architecture based upon the mechanisms for trust evaluation and service template working on edge and cloud level. In the proposed architecture, the design of the edge network claimed a reduction in energy consumption. The cloud services for IoT are also improved with templates for service-parsing and service-parameter on the edge platform and cloud, respectively. On similar lines, Bakhshi et al. [30] focused on security issues and threats in the context of cloud computing in IoT covering abstraction levels for Microsoft Azure and Cisco reference architectures.

Dawoud et al. [31] proposed an SDN-based security architecture for IoT covering large IoT deployment, like smart cities, with huge network traffic and security concerns. The authors claimed that the enhanced security of SDN will boost the security of SDN-based architecture for IoT. The deep-learning-based approaches are used for intrusion detection in the network. On the similar lines, Sharma et al. [32] presented a distributed blockchain SDN-based architecture, DistBlockNet for securing the IoT. The proposed architecture combined the features of both blockchain and SDN to provide a trusted IoT environment. Moreover, no recommendations and reviews are needed by the administrator, as the architecture automatically get adapted to the new threat landscape. The authors claimed that the proposed architecture could detect real-time attacks in an IoT system with fewer overheads.

Additionally, Yazdinejad et al. [27] proposed a cluster architecture comprising of SDN controllers with blockchain for efficient network management in an IoT system. The proposed architecture worked with efficient blockchains in terms of energy consumption and computation. With blockchains, the given architecture provided secure file transferring and access control in IoT. In another notable work, Meneghello et al. [26] highlighted the security challenges related to security goals and threats in

an IoT system. The authors also discussed the existing security mechanisms with their loopholes for IoT services. The attack surfaces for common communication technologies for IoT (BLE and LoRaWAN), and their practical implementation to analyze their security features, were also part of the study.

3. IoT: Threat Architecture

This section discusses the threats at various layers of generic IoT, as depicted in Figure 4. The components of an IoT System include different types of sensors and actuators, a smartphone with an associated application installed in it, the web interface for the smart environment, the servers the IoT devices interact with, and the requisite communications within the IoT system. Table 2 summarizes the threats (TH) imposed on various layers of IoT architecture along with their impact and successfully launched attacks. It is observed that the IoT devices are easy to get control of and thus leading to all the DoS attacks these days. Like the generic architecture, the proposed threat architecture also includes three layers: (i) perception layer, (ii) network layer, and (iii) application layer. The description of each layer is as follows.

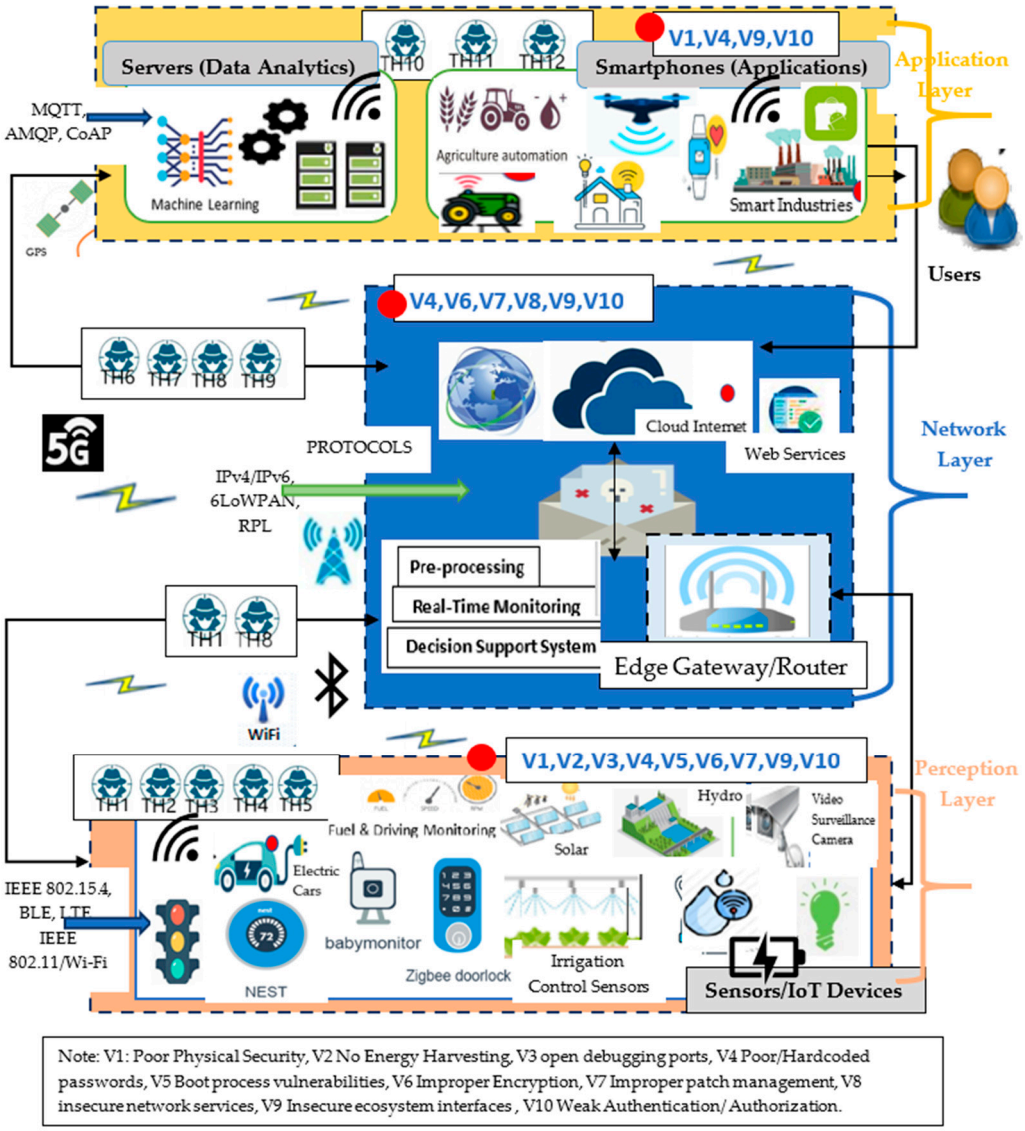

Figure 4. Threat Architecture of Internet of Things.

Table 2. Threats and their Impact.

Threat Id	Layer	Threat Imposed	Impact	Real Attack
TH1	P	Can update the firmware with malicious code	It can take control of the device.	PsycoBoT
TH2	P	It can access the side channel information of the device.	Can discover the secret keys.	
TH3	P	Increases the power consumption of sensor nodes thus preventing them to function/sleep.	The lesser service lifetime of the node, Node outage	Stuxnet Attack
TH4	P	It can physically access the smart device hardware and software.	Can access the hard disk, change the OS, and take control of the system	Nest Thermostat
TH5	P, N	Can add fake/Sybil nodes to the network.	It can mislead the entire system.	
TH6	N	It can listen to network traffic and intercept it. (Eavesdropping)	It can get useful information. (username & passwords)	Smart baby monitors
TH7	P, N	The fraudulent packets can be injected into the communication links.	It can mislead the entire system.	
TH8	P, N	An adversary can jam the communication links.	Prevents the transmission of legitimate data and cause DoS attacks.	Mirai
TH9	N	It can also exploit the routing of packets by dropping, spoofing, redirecting, and misdirecting the packets.	It can see the encrypted communications and launch various routing attacks.	
TH10	A	It can infect the associated smart application with Malware.	It can get sensitive data from the smartphone and imitate the false actions in an IoT environment.	
TH11	A	An adversary can access the web interface and run a random JavaScript code in the prey's browser.	Private data could be theft and even smartphone could be hacked.	Persirai
TH12	A	An adversary can also escalate the privileges to access unauthorized data/functionality.	It can adversely affect the whole system.	Brickerbot

Note: P, Perception Layer; N, Network Layer; A, Application Layer.

Perception Layer: The perception layer works at the ground level. The basic function of this layer is to perceive the data from the surroundings like the humidity reading and video feeds. The devices for sensing, actuating, computation, identifying, and addressing the things work at this layer. It also performs some basic functions of the physical layer of the TCP/IP model like modulation–demodulation, frequency selection, and encryption–decryption of data [6]. The threats at the perception layer are as follows:

- **TH1.** The Integrated Circuit (IC) can be maliciously modified to exploit its basic functionality or to access the data using hardware trojan that can be triggered accordingly.
- **TH2.** An adversary can access the side channel information (e.g., power consumption, power dissipation, processing time) about the device, which can be used in multiple ways to launch various attacks. For example, they can generate secret keys using this information.

- **TH3.** An adversary can drain the battery of a sensor node by sending random packets such that the node gets exhausted at the time of actual functioning. For example, a depleted smoke detector node in a fire detection system will fail in reporting an emergency.
- **TH4.** An adversary can physically access the smart device hardware and software. Thus, they can easily tamper with hardware, extract the cryptographic secrets, access the hard disk, change the OS, modify the integrated circuits, and can take control of the system.
- **TH5.** An adversary can add a malicious node (a node clone) to an existing group of authorized nodes by replicating their identification number. For example, it can work in a passive mode to analyze the traffic or can also mislead the entire system.

Network Layer: The Network layer is the middle layer, whose purpose is to receive data from the perception layer and then forward the same to the application layer for further processing, analysis, and smart services. The perception nodes can connect to a gateway through various means like Bluetooth low energy (BLE), Zigbee, 802.15.4, long range wide area network (LoRaWAN), SigFox, Wi-Fi, near-field communication (NFC), and RFID. These options/means have a trade-off in terms of bandwidth, range, and power consumption. The gateway device is further connected to a network server or an application via 3G/4G, LTE, OFC, and satellite [15]. The threats at the network layer are

- **TH6.** An adversary can listen to the network traffic over the communication links. Thus, they can get access to control information (node configurations, shared network passwords, node identities) and extract usernames and passwords as well.
- **TH7.** The fraudulent packets can be injected into the communication links to mislead the system. For example, adding a manipulated header, checksum, and packet data.
- **TH8.** An adversary can jam the communication links. Thus, preventing the transmission of legitimate data. This could be achieved even by adding a malicious router that can refuse to route messages or can misdirect them.
- **TH9.** The adversary can also exploit the routing of packets by dropping, spoofing, redirecting, and misdirecting the packets to launch various attacks. For example, they can change the routing information and can add routing loops.

Application Layer: The application layer is the topmost layer in the IoT architecture which provides smart services to its users in the form of smart home autonomous services, health statistics, business intelligence, industrial automation, smart irrigation, environmental monitoring, and smart city sharing services. It provides an interface for the user to interact with the IoT system. The major concerns at this layer are in the context of security and privacy of user information, and storage and processing of raw data received from the sensors. The Application developers mainly focus on service delivery and efficiency and have less to do with security. Thus, they get more compromised, and more often their services are denied to the authentic users [23]. The threats at the application layer are

- **TH10.** The malware can easily compromise the IoT enabled devices by using weak authentication /authorization process of applications. Thus, linking those infected devices to create a botnet to launch more severe attacks.
- **TH11.** An adversary can run a random JavaScript code in the prey's browser. Thus, private data could be theft and even smartphone could be hacked.
- **TH12.** An adversary can also escalate the privileges to access unauthorized data/functionality. For example, the threshold of health monitoring devices to give an alarm could be changed.

4. IoT: Attack Surfaces

The numerous cyber-security challenges [33] are imposed by the growing attack surfaces in IoT. Moreover, these challenges are the system's own intrinsic vulnerabilities exposing the system to several attacks. The attack surfaces may include device firmware, different interfaces (web, administrative,

physical), hardware, device memory, system applications, and network services as shown in Figure 5. Additionally, the full-duplex communication links open the multiple paths for network attacks over the communication protocols. For example, most of the smart devices are receptive to IP misconfiguration leading to unusual behaviour and hence declines the system's overall performance. Furthermore, the amalgam of IoT with cloud computing increases IoT services with exposure to the global gateway as well as open networks. Along with IP spoofing, gateways are perfect points for malicious threats, intrusions, man-in-the-middle attacks, DDoS, and injection attacks. Additionally, most of the IoT applications being web or mobile-based, are developed using application programming interface (API) (PHP, XML, and Java) and an unpatched API leads to several malicious attacks. Thus, the challenges IoT Attack surfaces (AS) impose should be taken into consideration by those looking to implement IoT Technologies, developers, and security researchers [34].

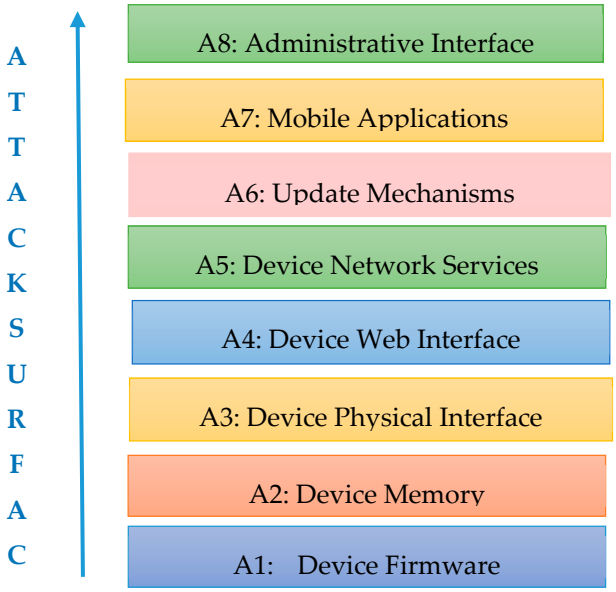

Figure 5. Attack Surfaces in an IoT System [33–35].

- **AS1. Device Firmware:** By getting access to this attack surface, the potential adversary can get hardcoded credentials, encryption keys, sensitive URL's, firmware version, and the last date when it got updated. They can also get vulnerable services like ssh, tftp, and web, and can even create backdoor accounts through firmware.
- **AS2. Device Memory/Information:** This includes data gathered by different sensors, different security keys, security certificates, device information, and user information. Thus, the device should not store passwords and usernames in clear text, encryption keys, and third-party credentials in its memory. Though in most of the devices encryption keys and passwords are even hardcoded.
- **AS3. Device Physical Interface:** Through device physical interface, the adversary can get the device id, escalate the privileges, reset the device to an insecure state, can extract the firmware and storage media.
- **AS4. Device/Cloud Web Interface:** The intruder can exploit the web interface of the device/cloud using SQL injection, can get the user's default credentials, their username, and weak passwords. Furthermore, they can misuse an insecure password recovery mechanism, no two-factor authentication, can do cross-site scripting, and cross-site forgery.
- **AS5. Device Network services:** The attacker can misuse the network services to launch attacks like DoS, buffer overflow, and replay attack. The attacker can block the Over-the-air (OTA)

firmware update, can analyze and see the network traffic within the LAN/WAN, thus hindering the privacy and integrity of information flowing through the network.

- **AS6. Update Mechanism:** A potential adversary can launch many attacks by exploiting the weak update mechanisms of IoT devices. The remote attacker could take advantage of loopholes like sending updates without encryption, unsigned updates, writable update location, no update verification, enabling malicious updates, missing adequate update mechanism, and no procedure for manual updates.
- **AS7. Mobile Applications:** An attacker can take undue advantage by malicious use of mobile applications. The mobile applications are implicitly trusted by device/ cloud, and thus an attacker can find out usernames, weak passwords, known default credentials, can access insecure data storage, log file information, and unencrypted traffic. Furthermore, they can misuse an insecure password recovery mechanism, no two-factor authentication, and no-account lockout mechanisms.
- **AS8. Administrative Interface:** The intruder can exploit the administrative interface of an IoT system using SQL injection, can get the user's default credentials, their username, and weak passwords. Likewise, they can misuse poor account lockout mechanisms, logging details, no two-factor authentication, and the encryption process. They can also do cross-site scripting and cross-site forgery.

5. IoT: Security Vulnerabilities and Challenges

The zero-day vulnerabilities and hacking tools are in great demand for Internet-based crimes. IoT being an integral part of today's society is exploited more by adversaries for maximum damage. Moreover, their resource-constrained nature and poor security mechanisms make them more vulnerable. Significant research has been devoted to devising security mechanisms to address the growing security concerns in IoT. In this direction, IoT vulnerabilities must be handled seriously to slow down the pace of IoT attacks. Various tools such as Dojo [35], Nessus [36], and Shodan [37] have been developed to find out the vulnerabilities in an IoT system [38]. Further, for quantifying these vulnerabilities, the CVSS framework is used in vulnerability modelling. However, the unique features of IoT systems are not addressed even by the current version of CVSS, i.e., CVSSv3. This is because CVSS has originally been devised for conventional IT systems, which are considerably different in terms of functionality and design. Consequently, the method of scoring of attack vectors and attack complexity must be different for an IoT system and IT system. For example, IoT sensors being in outer layers are more vulnerable than firewall-protected IT nodes.

Another factor found includes human safety, as we are having more dependence on IoT. As our routine life is merged with IoT, more risks are imposed on human lives. The decisions which were earlier made by humans are now taken by IoT systems. At times, incorrect decisions may lead to huge losses for humans. Hence, the criticality of IoT vulnerability is too dependant on the absence of human safety measures. Table 3 summarizes various factors based on which CVSS quantifies IoT vulnerabilities. It is found that CVSS considers only three security features namely confidentiality, integrity, and availability. As analyzed in Table 3, according to CVSS version 3.0, the poor cryptographic mechanisms for IoT devices are the most exploited one with the CVSS score 10.0 and it affects all the three in a Confidentiality, Integrity, and Availability (CIA) Triad. On similar lines, buffer overflow, improper access control, code injection, and escalated privileges do the same. Furthermore, most of these vulnerabilities used the network as the attack vector. But for IoT, more factors need to be explored to quantify IoT vulnerabilities in an efficient manner. Further research must be carried out to design a framework specifically for quantifying IoT vulnerabilities. Some of these vulnerabilities taken from the NVD database and summarized in Table 2 are described as follows [39,40]:

- **CVE-2020-4207** This is a buffer overflow vulnerability exploited in IoT Message Gateway (IBM Watson) 2.0.0.x, 5.0.0.0, 5.0.0.1, and 5.0.0.2. The remote attacker overflowed a buffer by sending a specific content in the HTTP request and caused improper bounds checking. By this, an adversary can execute arbitrary code on the device or initiate a denial of service condition.

- **CVE-2019-11063** This vulnerability causes broken access control in the Smart Home app (Android versions up to 3.0.42_190515, iOS versions up to 2.0.22). By exploiting this vulnerability, an attacker with no authentication can list all user accounts and also control IoT devices that come in the same local area network of its gateway.
- **CVE-2018-9995** This vulnerability allows the remote attackers to easily bypass the authentication process via a "Cookie: uid=admin" header, and can get the credentials within JSON data as a response to their request. It is found in various rebranded versions of the initial TBK DVR4104 and DVR4216 series (Novo, CeNova, QSee, Pulnix, XVR 5 in 1, Securus, Night OWL, DVR Login, HVR Login, and MDVR Login).
- **CVE-2017-6780** This vulnerability results in Memory Exhaustion, causing the system to temporarily undergo a denial of service (DoS) state. By exploiting this vulnerability, an unauthenticated remote attacker causes the system to shut down temporarily by sending a large number of TCP packets to set of open listening ports on victim devices.
- **CVE-2017-7243** It permits the remote attackers to create a denial of service condition (DTLS peer crash) in Eclipse IoT by forwarding a "Change cipher spec" packet with no pre-handshake. (Eclipse tinydtls 0.8.2)
- **CVE-2017-7911** This vulnerability was found in the Cyber-Vision Kaa IoT Platform (Version 0.7.4). It allows an attacker to remotely execute code on the system. This comes under insufficient encapsulation.
- **CVE-2016-0866** Through unspecified vectors, the remote attackers can inject arbitrary web script in Smart Grid Light-House (Tollgrade) Sensor Management System (SMS) Software EMS before 5.1, and 4.1.0 Build 16. This comes under cross-site scripting vulnerability.
- **CVE-2015-2884** The remote attackers directly obtain the sensitive information (related to yoics.net URLs, cam_service_enable.cgi, and stream.m3u8 URIs) via a request in Philips In.Sight B120/37.
- **CVE-2015-2886** An adversary got sensitive information related to the ibabycloud.com service in iBaby M6.
- **CVE-2015-2889** This vulnerability in Internet Viewing System and Summer Baby Zoom Wi-Fi Monitor lets the remote attackers get privileges by manually entering the Settings URL.
- **CVE-2015-0739** By exploiting this vulnerability, the authenticated remote users uploaded Baseboard Management Controller (BMC) file via unspecified vectors (Bug ID CSCus87938) in Lights-Out Management (LOM) implementation in Cisco Fire SIGHT System Software 5.3.0 on Sourcefire 3D Sensor devices.
- **CVE-2014-9234** Through the Directory traversal vulnerability, the remote attackers could easily read arbitrary files in D-Link IP camera DCS-2103 with firmware 1.0.0.
- **CVE-2013-6952** The hardcoded GPG key in the Belkin WeMo Home Automation firmware (before 3949) allows remote attackers to easily spoof firmware updates and can also execute arbitrary code through crafted signed data.

Table 3. IoT Vulnerabilities and their Impact.

CVid	Vulnerability Type	Attack Vector	Affected Products	CVSS Score (10)	CWE Name	Exploitability Subscore	C	I	A	User Interaction
CVE-2020-4207	Improper bound checking while handling failed HTTP request.	Network	IBM Watson IoT Message Gateway	9.8 $	Classic Buffer Overflow	3.9	✓	✓	✓	X
CVE-2019-11063	Broken Access Control	Adjacent	Smart Home application	8.8 $	Improper Access Control	2.8	✓	✓	✓	X
CVE-2018-9995	Bypass a restriction	Network	Tbkvision -Tbk-dvr4104-Firmware	9.8 $		3.9	✓	✓	✓	X
CVE-2015-2886	Predictable Information Leak	Network	iBaby M6	7.5 $	Information Exposure	3.9	✓	X	X	X
CVE-2015-2884	Direct Browsing	Network	Philips In. Sight B120/37	7.5 $	Information Exposure	3.9	✓	X	X	X
CVE-2017-7911	Execute code	Network	Cyber vision KAA IoT platform	8.8 $	Code Injection	2.8	✓	✓	✓	X
CVE-2017-6780	DoS	Network	Cisco Connected Grid Network Management System, IoT field Network Director	7.5 $	Resource Allocation without limit/throttling.	3.9	X	X	✓	X
CVE-2016-0866	Cross-Site -Scripting	Network	Tollgrade Smart Grid Light House Management	6.1 $	Improper Neutralization of Input in Web Page Generation	2.8	X	✓	X	✓
CVE-2017-7243	Denial of Service	Network	Eclipse Tinydtls Application	7.5 $	Null Pointer Dereference	3.9	X	X	✓	X
CVE-2015-2889	Gained privileges via manual entry of a Settings URL.	Network	Summer Baby Zoom Wifi Monitor & Internet Viewing System	8.8 $	Privileges, Permissions, and Access Controls	2.8	✓	✓	✓	X
CVE-2015-0739	BMC file uploads via unspecified vectors	Network	Cisco Foresight System Software	4.0 *	Improper Input Validation	8.0 *	X	✓	X	X
CVE-2014-9234	Directory /Path Traversal	Network	D-Link-Dcs-2103-Hd-Cube-Network-Camera-Firmware	5.0 *	Improper Limitation of a Pathname to a Restricted Directory	10.0 *	✓	X	X	X
CVE-2013-6952	Spoof Firmware Updates	Network	Belkin WeMo Home Automation firmware before 394	10.0 *	Cryptographic Issues	10.0 *	✓	✓	✓	X

Note: C, impact on confidentiality; I, impact on integrity; A, impact on availability; U, user interaction required; *, CVSS version 2.0; $, CVSS version 3.0. Notations: ✓, yes; **X**, no.

6. Case Study 1: Smart Transportation

In this section, we discuss a use-case of the Intelligent Transportation System installed in various cities across the world.

Intelligent Transportation System

An intelligent transportation system (ITS) [41] is an advanced application that makes use of various technologies for sensing, communication, analysis, and controlling the entire transportation system to make better decisions for efficient traffic management. However, ITS is not only about connected cars and smart road infrastructures; smart air traffic systems, railways and maritime also come under this domain. In these systems, real-time data about the traffic conditions, video feeds, the location and speed of vehicles, and schedule delays are collected by widespread sensors across the city. The collected data is transmitted via the existing communication channels from sensors to a data analytic center. In the data analytic center, data undergo pre-processing for further analysis. The useful insights and predictions are made and then communicated to end-users.

As turned up in Figure 6, IoT devices are an integral part of the ITS system, relaying insightful information for numerous services. These services are provided by working on factors like improving traffic safety, traffic congestion, reducing air pollution, and increasing energy efficiency. The vehicles can choose their route in a better way by knowing real-time traffic conditions. It provides insights to the government like where the new mobility options are required, and maintenance is needed. Moreover, the traffic signals can automatically adjust their timer based on real-time traffic conditions. Thus, preventing traffic congestion and pollution. Additionally, it enriches the public with prior information about transportation, enhancing their comfort and safety. The pedestrians connect to the ITS with their mobile phones. While utilizing public transportation and smart parking system, they get the useful information, for example; parking space, traffic updates, hazards, weather conditions, bus schedules, the present location of the bus, the next destination, seat availability, delays, passenger density, and emergency events, collected using a bed of sensors [42].

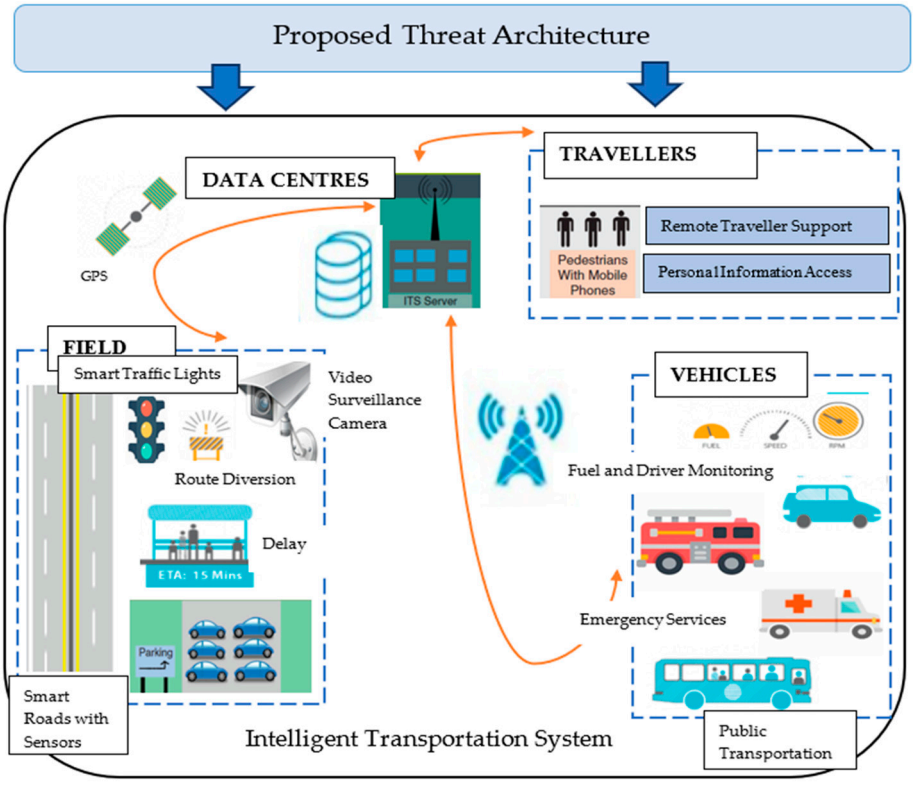

Figure 6. ITS with Proposed Threat Architecture [41–52].

In the discussed use case of ITS, the smart road transport system will be covered in terms of embedded threats and vulnerabilities [43] as depicted in Figure 7 and discussed in general in Section 3. Some real-time attacks hampering smart services and threatening human lives will also be seen. The automobiles today comprise a number of Electronic Control Units (ECU) for the better functioning of breaks, central locking systems, and airbags, along with emergency calls and infotainment [44]. These subcomponents are connected with each other and ECUs via the Controlled Area Network (CAN) bus. But these CAN buses are the most vulnerable part of the modular vehicles, as they are not integrated with any security mechanism until now. Furthermore, it is found that most of the modern vehicles are still working with insecure vulnerable CAN buses. The huge number of attacks are demonstrated in preliminary works [45]. To name a few, one can control the entire car, its speedometer, its brakes, engine everything by injecting the false command into the bus.

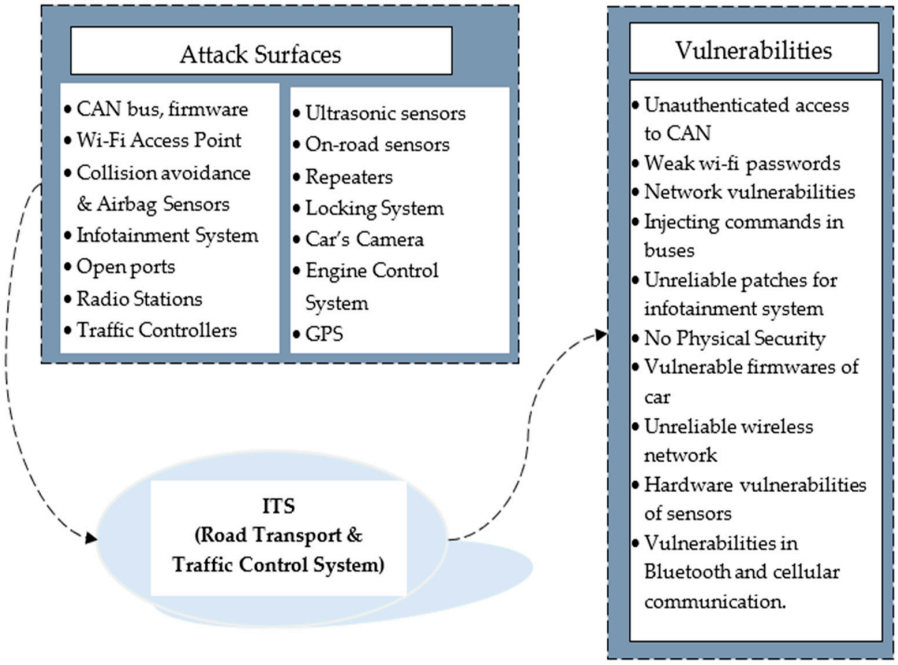

Figure 7. Attack Surfaces with known Vulnerabilities in ITS [53–57].

The CAN buses being the one thing, the other open attack surfaces comprise of sensors embedded in cars and roadside, communication protocols, and vehicular infotainment systems. The connected cars with cellular data SIM cards or Wi-Fi provide multiple services, for example, automated emergency calls, smart infotainment services, remotely updating of automobile's firmware, and real-time navigation system [46]. The on-board sensors also provide insightful services, such as avoiding collisions, smart notification systems, Autonomous Driving Systems (ADS), collision avoidance, and self-regulating speed enforcement [47]. However, it is not wise to overlook the trivial security challenges merged with useful services. This severity could be realized by the following attacks [48].

- ***Communication medium:*** The adversary can manipulate different car operations as well as inject false commands just by exploiting the vulnerabilities of Wi-Fi. It is found that the user's mobile applications use the Wi-Fi access point of car for controlling its various operations. Thus, the adversary remotely enters the car with ease by just bypassing the weak authentication (password) system of the Wi-Fi [49]. Similar attacks are seen by manipulating the telematics system, Bluetooth, and radio transmitters.
- ***Infotainment System:*** A lot much can be done against smart vehicles by exploiting the vulnerabilities of the infotainment system in connection with network vulnerabilities. In one such incident, 1.4 million vehicles [50] were recalled by the manufacturer to patch the similar

vulnerability. In this attack, the adversary entered the car through the ports left open in the cellular networks to provide navigation service and Wi-Fi connection. Through the open ports and secure shell service, the remote attacker discovered as well as exploiting the vulnerabilities of several chips in the head unit and malfunction the infotainment system of Harman U-connect. Thus, they remotely controlled the car, by altering the CAN firmware connected with the infotainment [51].

- ***Sensors:*** Tesla Motors disclosed the first death in a self-driving car due to compromised sensors that were unable to make out 18-wheel truck on the highway [52]. These self-driving cars extensively rely on several sensors to feed the sub-systems for collision avoidance, lane assistance system, and adaptive cruise control. All these components being dependent on wireless connections for proper functioning provides a large landscape for remote attackers, and thus the system failures.
- ***Traffic Systems:*** The remote attackers can hamper the crucial emergency services, cause accidents, and create traffic jams by compromising the traffic control systems using the on-road sensors. For the same, the adversary exploits the data link layer vulnerabilities of radio communications [53]. Furthermore, self-propagating firmware patches could amplify such attacks, thus including numerous sensors and repeaters across the world. It is found that the traffic infrastructure also contributes to launching DoS attacks.

Thus, in general, ITS may fail in the following conditions [54,55]:

- Leakage of real-time sensitive data
- Inclusion of Sybil nodes in the network, misleading the entire ITS system.
- False control of traffic signals.
- Devices transmitting the wrong information.
- Smart nodes getting compromised. (sensors, CCTV, Automatic Vehicle Identifiers, GPS based vehicle locators)
- Hacking of smart car applications.
- Attack on remote servers.
- False firmware updates for smart cars and other road transport components.
- Connected cars getting tracked.

ITS will be more efficient by integrating the threat architecture with the existing one. The use of the proposed threat architecture in smart transportation before its deployment offers various benefits such as

- Stops leakage of data.
- Lessens the compromising of smart nodes.
- Prevents the misleading of the entire system.
- Checks on the wrong information.
- Alerts the developer for precautionary measures.
- Vulnerabilities in the smart transportation system can be identified and removed well in time before getting exploited, and thus preventing the system from several threats.

The above use-case shows that the cyber-attacks could be life threatening in ITS systems. This becomes more serious as no cyber-security policies have been formed for smart transportation, as published in the European Network and Information Security Agency (ENISA) reports [56]. However, recently ENISA has published good practices for improving the security of connected cars [57]. These practices need to be incorporated into an intelligent transportation system to leverage the maximum benefits of their services. For this, both manufacturers and consumers must be informed about security practices. Presently, the users are unaware of the consequences they will face relying on vulnerable automobiles and insecure transportation systems. Additionally, with less bothered consumers, manufacturers do not spare the budget for integrating cyber-security mechanisms in ITS.

7. Case Study 2: Secure Energy Management

In this section, we discuss a use-case of the Smart Grid installed in various cities across the world for efficient energy management.

Smart Grid

Our lives have changed manifold with technological advancements in Information and communications technology (ICT). Smart Grids are one of those benefits of such technological shifts. The electric grids supply the energy received from power plants to the consumers. This supply of energy is not on the current energy requirements and thus leading to energy wastage or shortage at the user's end. The Smart Grid aids in efficient energy management by integrating sensors at various junctions and smart meters at the end nodes. The collected data are analyzed on the servers to infer insights for dynamic load balancing. It distributes the energy as per the current needs of users as smart meters feed the data regarding the daily energy usage of the consumer. All Smart Grids aim at meeting the demand for power at the minimum cost possible. The exponential increase in the number of power-based household/daily-need appliances raises the concern for efficient energy management. Until now, it is found that the number has reached 330 million power-based appliances in the U.S. [58]. Therefore, the optimization of daily-based energy consumption has become a prime concern.

In Smart Grid, the demand response management and load forecasting tackle the aforementioned concern efficiently. In this scheme, the user can change its power usage pattern concerning load and cost information. In peak hours, the load can also be reduced and shifted accordingly at different intervals with overall less power consumption. The two-way communication with the power-suppliers, allows the consumers to efficiently use and save the electric power. It has also increased resilience by efficiently merging with microgrids and other distributed energy sources [59]. Moreover, with energy trading in energy internet, the energy generated at power grids during non-peak hours could be transferred to power banks of electric vehicles and these vehicles can transmit the energy back to the grid during peak hours. Thus, in this way, connected electric vehicles aid efficient energy management in power grids. The blockchain technology with artificial intelligence and IoT also contributes in the same [60]. The microgrids have come across as the other way to increase the efficiency of the smart grids.

A microgrid is a power grid that comparatively works at a smaller scale and can meet the demand of a particular area. They can also merge with the main power grid as they have their own power source, generally the renewable one (solar panel, wind turbines) and called the hybrid microgrids. Generally, they serve as a back-up for the main power grid in case of heavy loads and outages. The infant technologies, power-grid complexity, their huge number, and regulatory requirements hinder the growth of the smart grid. In this context, microgrids could of great aid. Being a complete power grid with an energy source, storage, and distribution at a smaller scale, they can serve as a good alternative path for the development of a smart grid. It is comparatively easier and cheaper to deploy smart technologies in a microgrid. Moreover, initially smart technologies need to fulfil the specifications for a smaller grid as microgrid works with specific load requisites. Thus, microgrids can serve as a testbed for checking the performance of Smart Grid solutions. Furthermore, smart microgrids interconnected with one another will form a much bigger smart grid [61].

Transforming electric grids into Smart Grids with IoT and other prevalent technologies widen the attack surface for power grids. The adversaries could exploit the known vulnerabilities of network and IoT devices to remotely move into the smart grid. For example, the cyber-attack on the Ukraine power grid [62] has put thousands of people in the dark with power outages. They have remotely controlled the several power stations and further launched a DoS attack, thus preventing the power engineers to know about the blackout. In this attack, the BlackEnergy trojan horse has entered the vulnerable devices and corrupted their hard drives with spear phishing. Such attacks not only put the lives of people at risk but also badly affects the economy of a country like Stuxnet. Now the organized entities and countries have got involved in cyber-attacks to break down the electrical networks of other countries. In 2018, the American Electrical network has undergone infiltration by Russia and led

to a huge number of cyber-attacks including French electrical networks [63]. Some of the significant consequences of these attacks on power grids could lead to demand-supply mismatch and thus cause load curtailment, partial/full power outage, and load shedding [64].

As turned up in Figure 8, IoT devices have become an integral part of Smart Grids relaying insightful information for reliable and efficient power services. The figure also depicts the several vulnerabilities embedded in the smart grid and getting easily exploited by the hackers for the malfunctioning of the electric power system. These vulnerabilities must be accessed and patched well in time to shrink the large landscape provided to the adversaries by interconnected electric grids. The common attack surfaces for the Smart Grid include communication protocols, customer data, grid databases, control centers, on-field components, software, and insecure smart meters, which can be seen in detail in Section 4. Some of the vulnerabilities in the smart grid system are as follows:

- The common communication protocols with known vulnerabilities are used in Smart Grids. For example, buffer overflow vulnerability in Inter-Control Center Communications *Protocol* (ICCP), used for data exchange among utility control centers.
- Smart Grids being in an unprotected environment put the great risk of physical damage to its interconnected components.
- Smart meters could easily be used as a bot using malwares/insecure remote updates. Thus, providing a local easy access point for remote attackers to comparably unreachable power grids.
- The privacy of the user can be hindered by inferring information like daily routines, consumer's presence or absence, the number of persons in a home from smart meters.

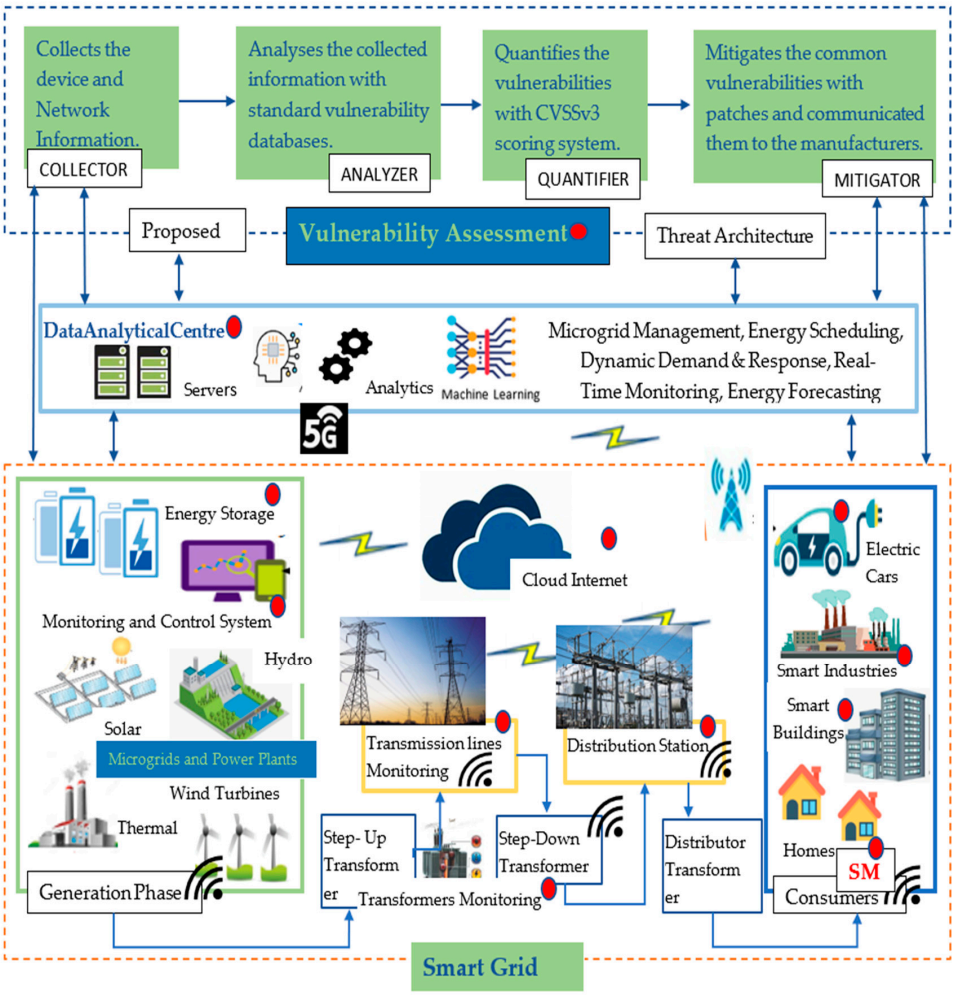

Figure 8. Secure Energy Management in Smart Grid [58–64].

A Smart Grid will be more efficient by integrating the threat architecture and vulnerability assessment module with the existing general architecture. In this use-case, the general vulnerability assessment method and threat architecture work on Smart Grids to find embedded threats and vulnerabilities. The vulnerability assessment works in four phases. The collector collects all the information about the device and network and then feeds to the analyzer. The analyzer compares the given information with vulnerability databases, and predicts the known vulnerabilities. These vulnerabilities are then scored as per their severity using quantifier with CVSSv3. The mitigator mitigates these vulnerabilities as per their priority and communicates the same to the manufacturer, system administrator, and the specific user [58–71]. The advantages of the proposed approach are as follows:

- Ensuring the privacy of smart meter's data and the two-way communication between utility providers and consumers; thus, preventing the leakage of private sensitive data of the users.
- Closing the loopholes like open ports, hardcoded/weak passwords reduce the risk of compromising of smart grid nodes.
- Prevents the malfunctioning of the entire system.
- Checks on the wrong information, being modified by the bad malicious actors.
- The developer of the components used in the Smart Grid will be communicated with the vulnerabilities and their severity, to prevent the new devices from the known vulnerabilities at the production level only.
- Vulnerabilities in the Smart Grid system can be identified and removed well in time before getting exploited, and thus preventing the system from several threats.

The proposed framework only gives the general idea of assessing the vulnerabilities and threats with their scores. The phases of this framework need to be covered in detail with proper methodology, implementation, and results. Additionally, in the proposed framework CVSSv3 is used to quantify these vulnerabilities which do not provide the appropriate way of scoring IoT vulnerabilities as discussed in Section 5. Moreover, the proper working of the analyzer to find the vulnerabilities from the collected information will also be covered in future work.

8. Conclusions

The vulnerabilities in IoT devices are playing an increasingly essential role in making the growth of IoT stagnant. Evidently, vulnerabilities in the IoT system render smart applications like intelligent transportation systems to the number of cyber threats. Therefore, it is important to assess and mitigate these threats to avail the benefits of smart services (e.g., smart traffic signals, enhanced road safety, efficient traffic management). This paper mainly presents the threat architecture of IoT which provides insights to the readers about the threats IoT is facing today. The IoT attack surfaces and major IoT vulnerabilities with their impact in terms of their exploitability are also illustrated. Finally, we present a case study to demonstrate the suitability of the proposed threat architecture in the existing one. The case study for secure energy management in power grids is also presented. This paper may also be used as a milestone to understand the usages of IoT in Smart energy Grid solutions and other related areas using sensors and analytics as well along with the security concerns and their challenges [65–71]. In addition to this, based on case study 2, it also covers the challenges of IoVT in the context of smart energy management. In the future, machine learning techniques will be explored for threat and vulnerability modelling in IoT. With intelligence, the proposed approach will be more efficient in finding new vulnerabilities and threats. Additionally, the given threat architecture will be extended with the framework to quantify these vulnerabilities with mitigations and its practical implementation in different scenarios.

Author Contributions: All authors have equal contributions. Conceptualization: P.A., Y.S., A.S., P.K.S., R.A.F. and M.S.R.; methodology, software, and validation: P.A., Y.S., A.S., P.K.S., R.A.F., and M.S.R.; formal analysis, investigation, resources, data analysis: P.A., Y.S., A.S., P.K.S., R.A.F., and M.S.R.; writing—original draft preparation, writing—review and editing: P.A., Y.S., A.S., P.K.S., R.A.F., and M.S.R.; visualization, funding acquisition: P.A., Y.S., A.S., P.K.S., R.A.F., and M.S.R. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by a grant from the Romanian Ministry of Research and Innovation, CCCDI-UEFISCDI, project number PN-III-P1-1.2-PCCDI-2017-0776/No. 36 PCCDI/15.03.2018, within PNCDI III.

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

References

1. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of things for smart cities. *IEEE Internet Things J.* **2014**, *1*, 22–32. [CrossRef]
2. Yosra, B.S. Collaborative security for the internet of things. *Int. J. Comput. Appl.* **2013**, *135*, 23–29.
3. Hypponen, M.; Nyman, L. The internet of (vulnerable) things: On hypponen's law, security engineering, and IoT legislation. *Technol. Innov. Manag. Rev.* **2017**, *7*, 5–11. [CrossRef]
4. Corser, G.; Fink, G.A.; Aledhari, M. Internet of Things (IoT) security best practices. *IEEE Internet Technol. Policy Commun. White Pap.* Available online: https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf (accessed on 9 June 2020).
5. Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and other botnets. *Computer* **2017**, *50*, 80–84. [CrossRef]
6. Gupta, B.B.; Quamara, M. An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. *Concurr. Comput. Pract. Exp.* **2018**, e4946. [CrossRef]
7. Makhdoom, I.; Abolhasan, M.; Lipman, J.; Liu, R.P.; Ni, W. Anatomy of threats to the internet of things. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 1636–1675. [CrossRef]
8. Insights, C. The CEO's guide to data security: Protect your data through innovation. *ATT Cybersecur. Insights* **2017**, *5*, 1–20.
9. Keller, J.; Sauter, D. Monitoring of stealthy attack in networked control systems. In Proceedings of the 2013 Conference on Control and Fault-Tolerant Systems (SysTol), Nice, France, 9–11 October 2013; pp. 462–467. [CrossRef]
10. Lee, R.M.; Assante, M.J.; Conway, T. German steel mill cyber attack. *SANS Ind. Control Syst.* **2014**, *30*, 1–15.
11. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale iot exploitations. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2702–2733. [CrossRef]
12. Babar, S.; Mahalle, P.; Stango, A.; Prasad, N.; Prasad, R. Proposed security model and threat taxonomy for the internet of things (IoT). *Databases Inf. Syst.* **2010**, *89*, 420–429. [CrossRef]
13. Roman, R.; Zhou, J.; Lopez, J. On the features and challenges of security and privacy in distributed internet of things. *Comput. Netw.* **2013**, *57*, 2266–2279. [CrossRef]
14. Humayed, A.; Lin, J.; Li, F.; Luo, B. Cyber-physical systems security—A survey. *IEEE Internet Things J.* **2017**, *4*, 1802–1831. [CrossRef]
15. Mosenia, A.; Jha, N.K. A comprehensive study of security of internet-of-things. *IEEE Trans. Emerg. Top. Comput.* **2017**, *5*, 586–602. [CrossRef]
16. Yaqoob, I.; Ahmed, E.; Hashem, I.A.T.; Ahmed, A.I.A.; Gani, A.; Imran, M.; Guizani, M. Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. *IEEE Wirel. Commun.* **2017**, *24*, 10–16. [CrossRef]
17. Yaqoob, I.; Ahmed, E.; Rehman, M.H.U.; Ahmed, A.I.A.; Al-Garadi, M.A.; Imran, M.; Guizani, M. The rise of ransomware and emerging security challenges in the Internet of Things. *Comput. Netw.* **2017**, *129*, 444–458. [CrossRef]
18. HaddadPajouh, H.; Khayami, R.; Dehghantanha, A.; Choo, K.-K.R.; Parizi, R.M. AI4SAFE-IoT: An AI-powered secure architecture for edge layer of Internet of things. *Neural Comput. Appl.* **2020**, *3*, 1–15. [CrossRef]

19. Gupta, R.; Tanwar, S.; Tyagi, S.; Kumar, N. Machine learning models for secure data analytics: A taxonomy and threat model. *Comput. Commun.* **2020**, *153*, 406–440. [CrossRef]
20. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of things security: A survey. *J. Netw. Comput. Appl.* **2017**, *88*, 10–28. [CrossRef]
21. Samaila, M.G.; Neto, M.; Fernandes, D.A.B.; Freire, M.M.; Inacio, P.R.M. Challenges of securing Internet of Things devices: A survey. *Secur. Priv.* **2018**, *1*, e20. [CrossRef]
22. Xiao, L.; Wan, X.; Lu, X.; Zhang, Y.; Wu, D. IoT security techniques based on machine learning: How do IoT devices use ai to enhance security? *IEEE Signal Process. Mag.* **2018**, *35*, 41–49. [CrossRef]
23. Frustaci, M.; Pace, P.; Aloi, G.; Fortino, G. Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet Things J.* **2017**, *5*, 2483–2495. [CrossRef]
24. Koloveas, P.; Chantzios, T.; Tryfonopoulos, C.; Skiadopoulos, S. A crawler architecture for harvesting the clear, social, and dark web for iot-related cyber-threat intelligence. In Proceedings of the 2019 IEEE World Congress on Services (SERVICES), Milan, Italy, 8–13 July 2019; pp. 3–8. [CrossRef]
25. Radoglou-Grammatikis, P.; Sarigiannidis, P.; Moscholios, I. Securing the internet of things: Challenges, threats and solutions. *Internet Things* **2019**, *5*, 41–70. [CrossRef]
26. 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]
27. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Zhang, Q.; Choo, K.-K.R. An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. *IEEE Trans. Serv. Comput.* **2020**, *13*, 625–638. [CrossRef]
28. Butun, I.; Osterberg, P.; Song, H. Security of the internet of things: Vulnerabilities, attacks, and countermeasures. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 616–644. [CrossRef]
29. Wang, T.; Zhang, G.; Liu, A.; Alam Bhuiyan, Z.; Jin, Q. A secure IoT service architecture with an efficient balance dynamics based on cloud and edge computing. *IEEE Internet Things J.* **2019**, *6*, 4831–4843. [CrossRef]
30. Bakhshi, Z.; Balador, A.; Mustafa, J. Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models. In Proceedings of the 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), Barcelona, Spain, 15–18 April 2018; pp. 173–178. [CrossRef]
31. Dawoud, A.; Shahristani, S.; Raun, C. Deep learning and software-defined networks: Towards secure IoT architecture. *Internet Things* **2018**, *3–4*, 82–89. [CrossRef]
32. Sharma, P.K.; Singh, S.; Jeong, Y.-S.; Park, J.H. DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks. *IEEE Commun. Mag.* **2017**, *55*, 78–85. [CrossRef]
33. Tweneboah-Koduah, S.; Skouby, K.E.; Tadayoni, R. Cyber security threats to IoT applications and service domains. *Wirel. Pers. Commun.* **2017**, *95*, 169–185. [CrossRef]
34. IoT Attack Surface Areas OWASP. Available online: https://www.owasp.org/index.php/IoT_Attack_Surface_Areas (accessed on 2 March 2020).
35. BullGuard Press Releases, Latest News BullGuard. Available online: https://www.bullguard.com/press/press-releases/2018/dojo-by-bullguard-introduces-first-of-its-kind-int.aspx (accessed on 9 June 2020).
36. #1 Vulnerability Assessment Solution Nessus Professional TM. Available online: https://www.tenable.com/products/nessus/nessus-professional (accessed on 9 June 2020).
37. Barbieri, G.; Conti, M.; Tippenhauer, N.O.; Turrin, F. Sorry, Shodan is not Enough! Assessing ICS Security via IXP Network Traffic Analysis 2020. *arXiv* **2020**, arXiv:2007.01114.
38. Simon, K.; Moucha, C.; Keller, J. Contactless vulnerability analysis using Google and Shodan. *J. Univers. Comput. Sci.* **2017**, *23*, 404–430.
39. NVD Search and Statistics. Available online: https://nvd.nist.gov/vuln/search (accessed on 25 April 2020).
40. Hahn, D.A.; Munir, A.; Behzadan, V. Security and privacy issues in intelligent transportation systems: Classification and challenges. *IEEE Intell. Transp. Syst. Mag.* **2019**, *1*. [CrossRef]
41. Guerrero-Ibáñez, J.A.; Zeadally, S.; Contreras-Castillo, J. Sensor technologies for intelligent transportation systems. *Sensors* **2018**, *18*, 1212. [CrossRef] [PubMed]
42. Takefuji, Y. Connected vehicle security vulnerabilities. *IEEE Technol. Soc. Mag.* **2018**, *37*, 15–18. [CrossRef]
43. Liu, J.; Zhang, S.; Sun, W.; Shi, Y. In-vehicle network attacks and countermeasures: Challenges and future directions. *IEEE Netw.* **2017**, *31*, 50–58. [CrossRef]
44. Aswath, G.; Vasudevan, S.K.; Sundaram, R. Emerging security concerns for smart vehicles and proposed IoT solutions. *Int. J. Veh. Auton. Syst.* **2018**, *14*, 107. [CrossRef]

45. Huang, S.-C.; Chen, B.-H.; Chou, S.-K.; Hwang, J.-N.; Lee, K.-H. Smart car [application notes]. *IEEE Comput. Intell. Mag.* **2016**, *11*, 46–58. [CrossRef]
46. Chattopadhyay, A.; Lam, K.-Y.; Tavva, Y. Autonomous vehicle: Security by design. *IEEE Trans. Intell. Transp. Syst.* **2020**, 1–15. [CrossRef]
47. Stellios, I.; Kotzanikolaou, P.; Psarakis, M.; Alcaraz, C.; Lopez, J. A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3453–3495. [CrossRef]
48. Hacking the Mitsubishi Outlander PHEV hybrid Pen Test Partners. Available online: https://www.pentestpartners.com/security-blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/ (accessed on 5 June 2020).
49. Fiat Chrysler Recalls 1.4 Million Cars after Jeep hack BBC News. Available online: https://www.bbc.com/news/technology-33650491 (accessed on 8 June 2020).
50. Miller, C.; Valasek, C. Remote exploitation of an unaltered passenger vehicle. *Black Hat USA* **2015**, *2015*, 1–91.
51. Tesla Driver Dies in First Fatal Crash while Using Autopilot Mode Technology the Guardian. Available online: https://www.theguardian.com/technology/2016/jun/30/tesla-autopilot-death-self-driving-car-elon-musk (accessed on 8 June 2020).
52. Cerrudo, C. Hacking US traffic control system. *Present. Defcon.* **2014**, *22*, 1–28.
53. Olufowobi, H.; Bloom, G. Connected Cars: Automotive cybersecurity and privacy for smart cities. In *Smart Cities Cybersecurity and Privacy*; Elsevier: Amsterdam, The Netherlands, 2019; pp. 227–240. [CrossRef]
54. Gupta, R.; Kumari, A.; Tanwar, S. A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles. *Trans. Emerg. Telecommun. Technol.* **2020**, 1–24. [CrossRef]
55. Levy-Bencheton, C.; Darra, E. Cyber security and resilience of intelligent public transport. *ENISA Rep.* **2015**. [CrossRef]
56. Service, E.R. Smart Health, Enisa Good Practices for Security of Smart Cars. 2019. Available online: https://www.enisa.europa.eu/publications/smart-cars (accessed on 7 August 2020).
57. Kumari, A.; Vekaria, D.; Gupta, R.; Tanwar, S. Redills: Deep learning-based secure data analytic framework for smart grid systems. In Proceedings of the 2020 IEEE International Conference on Communications Workshops (ICC Workshops), Dublin, Ireland, 7–11 June 2020; pp. 1–6. [CrossRef]
58. Kumari, A.; Tanwar, S.; Tyagi, S.; Kumar, N.; Obaidat, M.S.; Rodrigues, J.J.P.C. Fog computing for smart grid systems in the 5G environment: Challenges and solutions. *IEEE Wirel. Commun.* **2019**, *26*, 47–53. [CrossRef]
59. Kumari, A.; Gupta, R.; Tanwar, S.; Kumar, N. Blockchain and AI amalgamation for energy cloud management: Challenges, solutions, and future directions. *J. Parallel Distrib. Comput.* **2020**, *143*, 148–166. [CrossRef]
60. Yoldaş, Y.; Önen, A.; Muyeen, S.M.; Vasilakos, A.V.; Alan, I. Enhancing smart grid with microgrids: Challenges and opportunities. *Renew. Sustain. Energy Rev.* **2017**, *72*, 205–214. [CrossRef]
61. Sullivan, J.E.; Kamensky, D. How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid. *Electr. J.* **2017**, *30*, 30–35. [CrossRef]
62. Risk of Cyber Security Attacks on Smart Grid BearingPoint France. Available online: https://www.bearingpoint.com/fr-fr/blogs/energie/risk-of-cyber-security-attacks-on-smart-grid/ (accessed on 7 August 2020).
63. Wadhawan, Y.; Almajali, A.; Neuman, B. A comprehensive analysis of smart grid systems against cyber-physical attacks. *Electronic* **2018**, *7*, 249. [CrossRef]
64. Singh, P.K.; Arpan, K.K.; Yashwant, S.; Maheshkumar, H.; Kolekar, S.T. *Recent Innovations in Computing*; Springer Nature: Cham, Switzerland, 2019; ISBN 978-3-030-29406-9.
65. Singh, P.K.; Panigrahi, B.K.; Suryadevara, N.K.; Sharma, S.K.; Singh, A.K. *Proceedings of ICETIT 2019*; LNEE; Springer: Cham, Germany, 2020; Volume 605, pp. 921–1038.
66. Bangotra, D.K.; Singh, Y.; Selwal, A.; Kumar, N.; Singh, P.K.; Hong, W.-C. An intelligent opportunistic routing algorithm for wireless sensor networks and its application towards e-healthcare. *Sensors* **2020**, *20*, 3887. [CrossRef]
67. Tanwar, S.; Thakkar, K.; Thakor, R.; Singh, P.K. M-Tesla-Based Security Assessment in Wireless Sensor Network. *Procedia Comput. Sci.* **2018**, *132*, 1154–1162. [CrossRef]
68. Rastogi, N.; Singh, S.K.; Singh, P.K. Privacy and Security issues in Big Data: Through Indian Prospective. In Proceedings of the 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Bhimtal, India, 23–24 February 2018; pp. 1–11. [CrossRef]
69. Bodkhe, U.; Mehta, D.; Tanwar, S.; Bhattacharya, P.; Singh, P.K.; Hong, W. A Survey on Decentralized Consensus Mechanisms for Cyber Physical Systems. *IEEE Access* **2020**, *8*, 54371–54401. [CrossRef]

70. Bhargava, B.K.; Paprzycki, M.; Kaushal, N.C.; Singh, P.K.; Hong, W.C. (Eds.) *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*; Springer Nature: Berlin/Heidelberg, Germany, 2020; Volume 1132.
71. Poongodi, M.; Hamdi, M.; Sharma, A.; Ma, M.; Singh, P.K. DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET. *IEEE Access* **2019**, *7*, 183532–183544. [CrossRef]

© 2020 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 (http://creativecommons.org/licenses/by/4.0/).