Received August 25, 2020, accepted September 5, 2020, date of publication September 9, 2020,
date of current version September 24, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3022842

IoT Vulnerability Assessment for Sustainable Computing: Threats, Current Solutions, and Open Challenges

POOJA ANAND[1], YASHWANT SINGH[1], ARVIND SELWAL[1], MAMOUN ALAZAB[2], (Senior Member, IEEE), SUDEEP TANWAR[3], (Member, IEEE), AND NEERAJ KUMAR[4,5,6], (Senior Member, IEEE)

[1]Department of Computer Science and Information Technology, Central University of Jammu, Jammu 181143, India
[2]College of Engineering, IT & Environment, Charles Darwin University, Casuarina, NT 0810, Australia
[3]Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmadabad 382481, India
[4]Department of Computer Science Engineering, Thapar Institute of Engineering and Technology (Deemed to be University), Patiala 147004, India
[5]Department of Computer Science and Information Engineering, Asia University, Taichung City 41354, Taiwan
[6]Department of Computer Science, King Abdul Aziz University, Jeddah 80200, Saudi Arabia

Corresponding author: Mamoun Alazab (mamoun.alazab@cdu.edu.a)

ABSTRACT Over the last few decades, sustainable computing has been widely used in areas like social computing, artificial intelligence-based agent systems, mobile computing, and Internet of Things (IoT). There are social, economic, and commercial impacts of IoT on human lives. However, IoT nodes are generally power-constrained with data transmission using an open channel, i.e., Internet which opens the gates for various types of attacks on them. In this context, several efforts are initiated to deal with the evolving security issues in IoT systems and make them self-sufficient to harvest energy for smooth functioning. Motivated by these facts, in this paper, we explore the evolving vulnerabilities in IoT devices. We provide a state-of-the-art survey that addresses multiple dimensions of the IoT realm. Moreover, we provide a general overview of IoT, Sustainable IoT, its architecture, and the Internet Engineering Task Force (IETF) protocol suite. Subsequently, we explore the open-source tools and datasets for the proliferation in research and growth of IoT. A detailed taxonomy of attacks associated with various vulnerabilities is also presented in the text. Then we have specifically focused on the IoT Vulnerability Assessment techniques followed by a case study on sustainability of Smart Agriculture. Finally, this paper outlines the emerging challenges related to IoT and its sustainability, and opening the doors for the beginners to start research in this promising area.

INDEX TERMS IoT, machine learning, sustainability, cyberattacks, vulnerabilities, security, privacy.

I. INTRODUCTION

The way Internet has reformed the world, we can hardly envisage our lives without it. We are living in the era where various objects across the globe are connected to the Internet. These objects are uniquely identifiable and can sense, actuate, and communicate without human intercession [1]. The journey of objects to smart objects is based on the amalgamation of the Internet with emanating technologies like cloud computing, embedded sensors, Wireless Sensor Networks (WSN), middleware, and Radio-frequency identification (RFID) [2]. This amalgam seeded the word IoT, a wired /wireless network of uniquely identifiable connected things that are capable of processing data and communicating with each other with or without human intervention [3]. The IoT has eased the process to monitor and control the environments by linking the physical world with the web [4].

IoT services have a major impact on the lives of people. The people-centric solutions, like IoT assistance, allow the disabled people to enjoy independence and participation in their social life [5]. Moreover, the IoT solutions assist in in-home rehabilitation for physical therapy [6]. In contrast, the Autism Glass helps autistic children to make out facial emotions of people and thus aids in social interactions [7], [8]. Additionally, IoT solutions aids in minimizing hazardous situations. For example, IoT has made the dangerous tasks of mining safer and efficient like self-driving autonomous mining tools keep the workers apart

The associate editor coordinating the review of this manuscript and approving it for publication was Zhenyu Zhou.

from hazardous zones. The location and proximity sensors also aid in the same [9]. There are several IoT sensors such as smoke, toxic gas, temperature when couple with warning systems prevent environmental disasters. These sensors can also keep a check on chemical leaks in water bodies [10]. A lot of case studies have also been reported by various research institutes in collaboration, to show the influence of IoT on natural resources [11].

The certain services provided by the IoT systems come infusion with significant security flaws. Manufacturers overlook the security considerations and produce devices that could be easily exploited. It appeared that 70 percent of Internet-connected devices are vulnerable to cyber-threats [12]. Moreover, as per the studies by the end of 2020, 25 percent of industrial attacks will be due to compromised IoT devices [13]. This severity can be seen from the number of cyber-attacks like-Mirai (2016), Hajime botnet (2016), Persirai (2017), and BrikerBot (2017) launched successfully by exploited IoT devices [14], [15]. Furthermore, privacy is also hindered. IoT based baby monitors and IoT toys [16] are played with by hackers to get sensitive information like video streaming of baby monitors [17], voice recordings of parents, and their kids (in millions), emails, passwords, etc. Easy reprogramming of IoT Device firmware is an add-on for the adversary [18]. Above all, IoT could be a severe threat to flesh and blood. The US Food and Drug Administration also confirmed the risks allied with the reconfiguration of implantable devices and their unauthorized access [19]. All this raises the alarm to take security and privacy issues as a serious matter of concern for sustainable IoT [20], [21].

On similar lines, the energy requirement for IoT devices and their communication plays a crucial role leading to sustainable IoT. Over the past decade, the digital environment and smart devices have increased energy consumption to an alarming level. The renewable sources of energy must be incorporated in energy harvesting (EH) to power widespread IoT sensors [22], [23]. Because batteries of IoT sensors have limited lifetime and its impossible to frequently charge or replace them as they need to run for an extended period of time. For example, in body sensor networks, the EH-enabled sensors along with continuously monitoring the patient can harvest the energy from the patient's body [24] or environment, like thermal energy, kinetic energy,solar energy, and radio frequency signals [25]. With energy harvesting, another promising solution to address this challenge is an efficient data transmission scheme [26]. It is found that 80% of the sensor's energy is consumed during data transmission. Moreover, EH chips are also being attacked by malicious Trojans destroying sensors and thus leading to DoS attacks. Hence, both the factors security and energy-efficiency define sustainable IoT. However, the two are the conflicting challenges for the growth and operation of IoT [27]. Because IoT nodes being power constrained need lightweight energy-efficient security mechanisms [28]. In this article, we will cover the security as a challenge for the sustenance of IoT. Specifically, the vulnerabilities in an IoT system, that serves as the doorway to numerous threats and posing a significant risk to sustainable IoT.

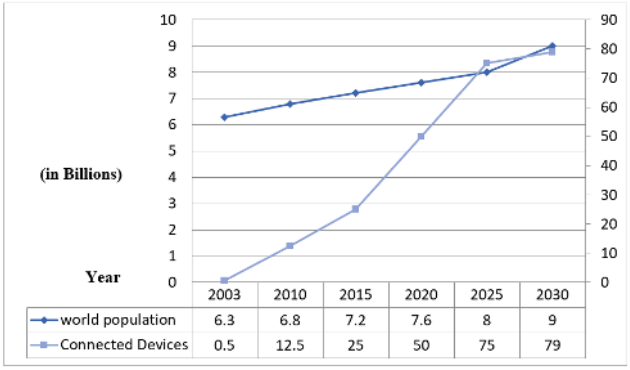

FIGURE 1. Estimation of connected devices growth in IoT [1].

The exponential growth and resource-constrained nature of IoT devices challenge confronting various IoT security issues. FIGURE 1 shows the estimated IoT enabled devices (internet-connected) will be 80 billion by the year 2030. Although several security mechanisms exist in literature to enhance the security of IoT. The existing IoT solutions either impose computational load on IoT devices or are so lightweight that they could easily be bypassed. The higher computational load will lead to early battery-depletion of smart nodes. With self energy harvesting capacity [29], the node will be more efficient to secure and sustain itself in this connected era. Moreover, to meet the long-term power budget of these constrained IoT nodes, the researchers across the globe have given their energy-efficient solutions to meet the growing challenges like security, privacy, and interoperability. For example, being resource-constrained, the IoT nodes offload their computational overhead to the edge-servers through specific channels in an energy-efficient way [30]. On similar lines, the recent works provide secure and energy-efficient solutions [31], [32]. One of such solutions is blockchain-based secure and efficient energy trading from vehicle-to-grid and the other way in Energy Internet [33].

A. SCOPE OF THIS SURVEY

The IoT architecture, protocols, growing technologies, IoT attacks, and threats have been widely studied in the reviewed literature. However, no comprehensive survey exists which has covered the IoT vulnerabilities and their assessment in context to sustainable computing. For example, Gupta *et al.* [1] have put together in their survey the historical background of the IoT, methodically studied the architecture of IoT, and variant nature of challenges it can come across. They have also weighed up permissive technologies like RFID and WSN, along with their key issues and existing solutions to grapple with. Similarly, Atzori *et al.* [34] explored IoT in multiple contexts, discussed enabling technologies and

their impacts in everyday-life. We have examined many such correlated surveys to find their contributions and illustrate how the present study progresses the state-of-the-art in terms of IoT security.

Sicari *et al.* [35] reviewed the existing state-of-the-art solutions in the field of IoT security. The authors also explored the proposals on security middlewares and solutions for mobile devices. Some ongoing international projects are also studied. Finally, they have given the future directions. One being the need of unified vision for assurance of security requirements in different environments. In contrast, Granjal *et al.* [36] provide deep insight for communication protocols in IoT, such as IEEE 802.15.4, IEEE802.15.4.e, 6LowPAN, RPL, and Constrained Application Protocol (CoAP). They also explored the security provided by these protocols in the communication stack of IoT. Moreover, research challenges and proposals for security against packet fragmentation, key management, solutions against internal attacks, and compressed security headers for the 6LoWPAN adaptation layer put forward to secure communications availing the IoT technologies forging the protocol stack.

Samaila *et al.* [37] performed survey covers to multiple security concerns such as system model, threat model. Further, they thoroughly explored nine application domains with their different models, associated assets, and security requirements. The authors also discussed solutions based on cryptographic primitives, authentication mechanisms, hardware, and specific application domains. The paper highlights the current IoT security mechanisms and open issues that need to be addressed. On similar lines, Roman *et al.* [38] analyzed the features and the security challenges in centralized and distributed IoT to cognize their sustainability in IoT. Additionally, Zhang *et al.* [39] discovered five weak areas about IoT security by mapping real IoT incidents with the existing security solutions. They are implementation loopholes, inadequate authentication, excessively privileged applications, environmental mistrust, and LAN mistrust. Moreover, the authors provided their dataset and statistics online.

In addition to this, Alaba *et al.* [40] proposed the taxonomy of IoT security, in terms of application, architecture, and communication. The authors also discussed numerous attacks launched by exploiting threats and vulnerabilities in IoT [21]. Moreover, some emerging IoT challenges related to trust, security, and infrastructure were talked about. In this way, the authors reasoned that the diversity of resource-constrained IoT devices hampers the scalability of promising security solutions. In another work, Mosenia and Jha [41] presented several attack scenarios, and their potential mitigation approaches for the Cisco 7-layer reference model [42]. The authors emphasized the significance of using a proactive approach to secure the IoT environment. They analyzed the vulnerabilities and provided necessary countermeasures for edge nodes, communication, and edge computing in an IoT system. Furthermore, they briefly described the IoT reference models, applications of IoT, and the attack vectors. Finally, they discussed two emerging security challenges – Unexpected usages of data, Exponential rise in the frequency of weak links.

Neshenko *et al.* [10] centered their work on emerging IoT security vulnerabilities. The survey presented the unique taxonomy on IoT vulnerabilities, which includes layer wise vulnerabilities, their security impact, their attack vectors, remediation strategies, and situational awareness capabilities. Furthermore, they proposed a data-driven approach for empirical assessment of IoT maliciousness. In addition, the authors drew insightful findings and inferences in various sections of the survey. On similar lines, Mahbub [43] and Srivastava *et al.* [44] presented the comprehensive work on growing security challenges in terms of vulnerabilities and threats. In another notable work, Makhdoom *et al.* [12] highlighted threats in context to IoT architecture and had given due diligence on the taxonomy of malware attacks with their attack approach. The authors also discussed the DDoS attack strategy by making a botnet of IoT motes, followed by needed security measures. The authors have given a comprehensive set of security guidelines grounded on industry best practices to apply minimum security standards in an IoT system. In the end, some open challenges, the lessons learned, and pitfalls are included within.

TABLE 1 shows the relative comparison of the proposed survey with state-of-the-art surveys. In this table, the readers could easily identify already available contributions in the state-of-the-art. They mainly centered their surveys around IoT architectures, Protocols for resource-constrained devices, enabling technologies, IoT attacks, threat modeling, and countermeasure strategies. From studied start-of-the-art, we noticed there are few surveys, which precisely emphasize on the growing IoT vulnerabilities. Furthermore, these surveys provide insight into IoT security threats and proposed solutions only from a general perspective. None of them addresses the recent trend of Machine Learning (ML) and other vulnerability assessment techniques and IoT security [45], [46]. Addressing these recent trends diverged the research towards the key tasks of discovering a pattern in enormous data, detecting outliers, extracting features for vulnerability detection, and predicting performance estimation metrics for IoT enabled systems using ML [47]. The proposed survey covers these research gaps and focuses mainly on emerging IoT vulnerabilities and various vulnerability assessment techniques to secure IoT devices for sustainable IoT [48].

B. RESEARCH CONTRIBUTIONS

Following are the contributions of this paper.

- We have presented a taxonomy that focuses on energy-efficiency and security for sustainable IoT.
- We have highlighted the benefits of the growing usage of techniques for the IoT vulnerability assessment such as machine learning, honeypots, fuzzy techniques, and penetration testing tools.

TABLE 1. A relative comparison of the proposed survey with the state-of-the-art surveys on IoT security.

Author(s)	Year	Discussion	Challenge(s)	1	2	3	4	5	6	7	8	9
Roman *et al.* [38]	2013	Analyzed the security challenges in Centralized and distributed IoT to recognize their sustainability in IoT.	To add security and trust in IoT system.	X	X	X	X	X	X	X	✓	✓
Jing *et al.* [49]	2014	Analyzed the security issues and the cross-layer heterogeneous integration issues in IoT.	To develop overall security architecture, Lightweight security policies, and to handle huge heterogeneous data.	✓	X	X	X	X	X	X	✓	✓
J.Granjal *et al.* [36]	2015	Discussed security against packet fragmentation, key management, internal attacks, and compressed security headers for 6LoWPAN.	To enhance the CoAP security.	X	✓	X	X	X	X	X	X	✓
Sicari *et al.* [35]	2015	Security of middlewares, solutions for securing mobile devices, and ongoing projects.	The need of unified vision for assuring security requirements in IoT.	X	X	X	X	X	X	X	X	✓
Ahlmeyer *et al.* [50]	2016	Discussed existing security frameworks like COBIT and proposed their own security Framework.	Lack of security standardization and no IoT laws and regulations exists nationally and worldwide.	X	X	X	X	X	X	X	X	✓
Nia *et al.* [41]	2016	Analyzed the vulnerabilities and provided countermeasures concerning edge nodes and edge computing in an IoT system.	There is an unexpected usage of user data and an exponential rise in the frequency of weak links.	✓	X	X	X	X	X	✓	✓	✓
Alaba *et al.* [40]	2017	Presented existing IoT security scenarios, IoT Security Matrix, and their countermeasures.	To develop Secure Smart Grid (SG) and Lightweight Authentication schemes.	✓	X	X	X	X	X	✓	X	✓
Oracevic *et al.* [51]	2017	security challenges of IoT with present security solutions.	Discussed challenges like standardization for heterogeneous devices, vulnerabilities in IoT, and energy consumption of security schemes.	✓	X	X	X	X	X	X	X	✓
Zhang *et al.* [39]	2017	Discovered five weak areas namely implementation loopholes, inadequate authentication, excessively privileged applications, environmental mistrust, and LAN mistrust.	Lack of security mechanisms in connected cars, and lack of protection on IoT user interaction points.	X	X	X	X	X	X	✓	✓	✓
Samaila *et al.* [37]	2018	Explored system model, threat model and proposed solutions based on cryptographic primitives, authentication, and access control protocols.	To develop Nano-electronic security primitives (resource-efficient) and a reliable model to evaluate the energy consumption of cryptographic schemes.	✓	✓	X	X	X	X	✓	✓	✓
Makhdoom *et al.* [12]	2018	Focused on the anatomy of malware attacks with their attack approach.	Discussed challenges to Fog computing in reference to IoT.	✓	✓	X	X	X	X	✓	✓	✓
Frustaci *et al.* [52]	2018	Analyzed the layers of IoT system and concluded that the perception layer is the most vulnerable one .	To deal with the heterogeneous nature of the IoT environment with reliable security solutions.	✓	✓	X	X	X	X	X	✓	✓
Xiao *et al.* [53]	2018	Discussed IoT threat model and ML-based solutions.	To reduce the overheads in ML techniques.	X	X	X	X	✓	✓	X	✓	✓
Neshenko *et al.* [10]	2019	A proposed data-driven approach to provide IoT-specific malicious signatures, and presented a taxonomy of IoT vulnerabilities.	To develop identification techniques for exploited and vulnerable IoT devices. Automatic remediation of IoT software vulnerabilities.	X	X	X	X	X	X	✓	✓	✓
Hussain *et al.* [54]	2020	Machine learning and deep learning based solutions to address various security issues in IoT networks.	Challenges related to IoT data, deep learning, and competence of security solutions.	X	X	X	X	✓	✓	X	✓	✓
Butun *et al.* [55]	2020	Comprehensive review of IoT and WSN security attacks and their defense mechanisms.	No de-facto cyber-security standard for IoT and WSN.	X	X	X	X	X	✓	X	✓	✓
The proposed survey	2020	IoT Security Vulnerabilities,Vulnerability Assessment Techniques, and Sustainable IoT.	Lack of Machine Learning based Vulnerability assessment platform and unexpected usage of IoT data.	✓	✓	✓	✓	✓	✓	✓	✓	✓

Note:1,architecture;2,protocol suite;3,open-source datasets;4,open-source tools;5,machine learning;6,ml based IoT security solutions;7,vulnerabilities;8,attacks;9,open issues and emerging challenges. Notations: ✓, considered; X, not considered.

- A case study on Sustainable Smart Agriculture has been presented.
- Finally, various open issues and future recommendations to ensure secure and sustainable IoT infrastructure for the end-users have been given.

C. METHODS AND MATERIALS

The proper methodology is adopted to conduct this survey in an appropriate manner to give a detailed analysis of two critical pillars, security, and energy for sustainable IoT. Several relevant articles, studies, and publications are identified to do this systematic review. The quality checks are carried out on the identified data before extracting the required information for the conducted survey. The papers with good citations are mainly focused. In this study, we specifically focused on state-of-the-art research on various technologies for assessing IoT vulnerabilities in an energy-efficient manner for sustainable IoT. Thereafter, to outline the current challenges and open issues questioning the sustenance of IoT. The high quality and trustable peer-reviewed journals and conferences like Wiley, ACM, Springer, IEEEXplore, Science Direct are preferred to get the relevant literature. The government reports, white papers, tutorial papers, technical blogs, and books are also referred for the same. For the search criteria, we have used keywords like Vulnerabilities in IoT, IoT Threats and Attacks, Vulnerability Assessment, Energy Harvesting, and Sustainable IoT. We have analysed

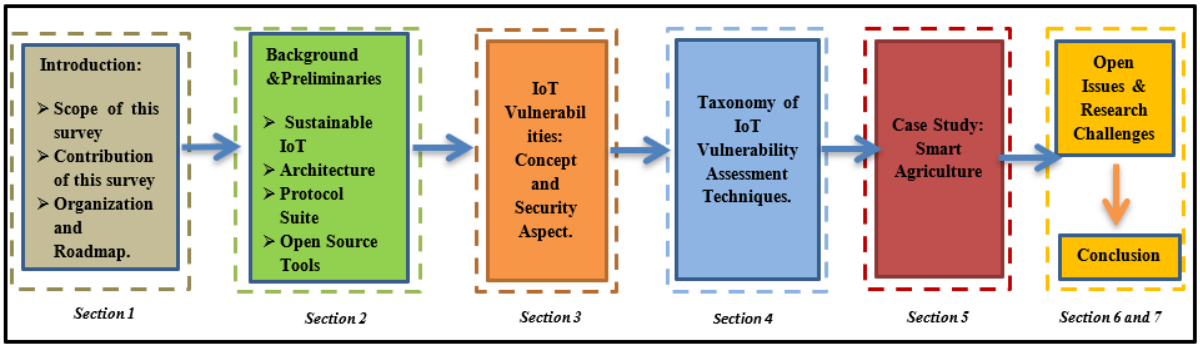

FIGURE 2. Roadmap of the proposed survey.

and acknowledged various works related to the discussed theme of the proposed survey.

D. ORGANIZATION AND ROADMAP

FIGURE 2 shows the roadmap of the proposed survey. The acronyms used in the paper are described in TABLE 2. The rest of the paper is organised as follows. Section II provides the overview of IoT, which includes sustainable IoT, the architecture of IoT, its protocol suite, and open source tools for IoT. IoT security vulnerabilities are discussed in Section III. The taxonomy of IoT vulnerability assessment techniques is discussed in Section IV, followed by a case study in Section V. In Section VI, we present the findings of the paper and finally, Section VII concludes the paper.

TABLE 2. Acronyms and their meanings.

Acronym	Explanation
ANN	Artificial Neural Network
AR	Accuracy Rate
CIA	Confidentiality, Integrity, Availability
CoAP	Constrained Application Protocol
DDoS	Distributed denial-Of-Service
FAR	False Alarm Rate
FPR	False Positive Rate
HTTP	Hypertext Transfer Protocol
ICS	Industrial Control System
IEEE	Institute of Electrical And Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
LoWPAN	Low Power Wireless Personal Area Network
MQTT	Message Queuing Telemetry Transport
PR	Precision Rate
PUF	Physical Unclonable Function
RFID	Radio-frequency Identification
RNN	Recurrent Neural Network
SDN	Software Defined Networking
SVM	Support Vector Machine
TPR	True Positive Rate
UDP	User Datagram Protocol
WSN	Wireless Sensor Networks

II. BACKGROUND AND PRELIMINARIES

This section focuses on the background and importance of security in IoT. This section is bifurcated into three subsections. Firstly, we discuss IoT architecture. Secondly, we discuss the protocol suite for IoT. In the third subsection, we focused on open source tools and datasets. Kevin Ashton firstly proposed IoT in 1999, and he referred the IoT as ''uniquely identifiable interoperable connected objects with RFID technology'' [56]. Around the early 1980s, the intelligent/smart coke machine was connected to the Internet to take the invoice of the list of coke drinks available, and this brought the concept of interlinking among the smart things [1]. The IoT, being an emanating world network of uniquely referable computing devices within the existing Internet infrastructure, is renewing our lives and the way we work by proliferating the connectivity of people and things to an unimaginable extent. In addition to diverse and profound applications of IoT, the rising security issues cause inestimable consequences [57]. TABLE 3 illustrates the main milestones allied with the evolution of IoT since 1999.

A. SUSTAINABLE IoT

Though IoT has become an integral part of our lives, there are a huge number of devices which have no mechanisms for energy harvesting and security. These two factors must be prerequisites at the design phase and all the aspects of their life-cycle (sensors) must be addressed right from deployment to their disposal. Thus, for sustainable IoT, energy sustainability and security sustainability are two critical pillars. The sustainable IoT is very well represented in FIGURE 3, where energy sources are used as a supply for IoT end nodes and security solutions preventing the malfunctioning of an IoT system. Being power-constrained, IoT end nodes are the weakest point in an end-to-end system. The energy efficiency solutions in terms of power consumption and data transmission have become the present need for sustainable IoT. As IoT revolves around data, the fate of IoT depends upon the security and privacy of the same [59]. The recent security breaches depict that even resource-constrained IoT end nodes with limited functionality induce substantial risk to the whole system. This is because of the connected nature of the IoT devices which provides a large attack surface, forming numerous attack points for the adversaries.

TABLE 3. Growth of in the usage of IoT-enabled devices.

Events	Period
The term IoT was formulated; Message Queuing Telemetry Transport (MQTT) was developed [1]	1999
First IoT enabled refrigerator publicized by LG.	2000
Industry University Cooperative Research Center was established by the National Science Foundation, the USA for predictive analytics technology (IoT based).	2001
Near Field Communication was announced to develop in cooperation with Sony & Philips.	2002
IoT was cited in “the Guardian". Large scale deployment of RFID	2003
AT &T and other carriers offered Wi-Fi hotspots.	2004
The first report on IoT was published by the UN’s ITU.	2005
“Wibree" Bluetooth Smart Technology was introduced by Nokia.	2006
European Research Cluster on IoT, a European Union based organization was founded. Wireless HART standard approved and IETF 6LoWPANâĂŹs RFC4944 issued [58].	2007
More internet-connected devices than people. IETF workgroup ROLL and IEEE802.15.4e workgroup formed [38].	2008
"Google Apps" the first browser-based cloud application was launched.	2009
"ioBridge" an IoT company developed the first online Tide Monitoring System.IEEE and IEFT based protocols ratified [58].	2010
Global Standards Initiative was created for IoT.	2011
IPv6 launched	2012
“Internet.org" was formed. ZigBee 1.0 standard approved and Time Synchronized Mesh Protocol 1.1 conveyed.	2013
The incubation council for IoT was made.	2014
Internet Of Things Security Foundation was made.	2015
Mirai attack was launched and Amazon Echo was developed.	2016
IoT terms database was made by IoT One (provides information about Industrial Internet of Things).	2017
Microsoft announced Azure Sphere and Azure Digital Twins, Government of California passed an IoT Cyber Security Law. The first 5G network was turned on.	2018
Wide deployment of 5G	2019

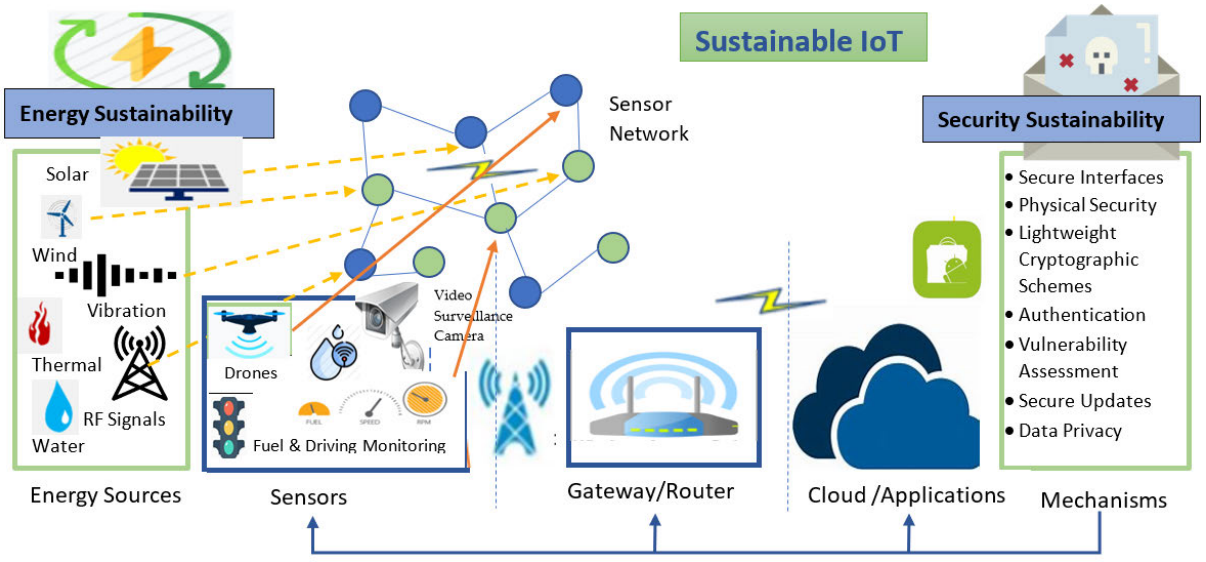

FIGURE 3. Sustainable IoT.

- Energy Sustainability: The overpowering IoT services infused in our lives raises the concern for the power-constrained IoT nodes for sustainable IoT. The mass deployment of IoT sensors and actuators in several sectors require a continuous power supply for a prolonged period. Because as the size of these IoT nodes being sensors or actuators is getting small, their battery size is also reducing. Thus, stores the reduced amount of energy in these end nodes. Also, the lifetime of the battery is considerably smaller than

the electronics. Moreover, the growing trend is to add more functionality to these power-constrained devices, which generally works in a wireless mode. This is a call for considerable progress in energy efficiency for both communication and computation in power-constrained IoT nodes for their sustenance [28]. Energy harvesting is one of the solutions and incorporated in several IoT application domains for wearables, bridges, road sensors, dams, mines, and drones. In many EH schemes, the energy from the surrounding environment aids in powering sensors and communication technologies. The radio frequency signals [25], solar [27], wind, water, human body [24], and piezoelectric are some of the common energy sources in EH schemes [22]. The maximum power point tracking schemes aid in extracting maximum energy from the input to boost power efficiency [60]. The inductor-less design for solar energy management [61] and several other energy management systems are designed in the literature. The bandgap-based output controller is used for output regulation with EH [62]. For boosting low input energy DC-DC converters are used as charge pumps [63]. Several wi-fi based EH schemes with efficient data transmission like CoWiFi [64] and context-awareness schemes are also designed. Though lot many efforts are made in improving the energy-efficiency in power-constrained IoT systems, but the pace does not match with the emerging IoT dependence/services.

- Security Sustainability: IoT being linked with real physical world phenomenon such as healthcare, agriculture, grids, weather, and taking decisions based on sensing and monitoring, necessitates the special concern in security [65], [66]. For sustainable IoT, data and device security both need to be taken into consideration. The data security mainly covers the integrity and confidentiality of data, whereas devices need to be protected from stealthy attacks. The common IoT security vulnerabilities hindering the sustainability of IoT remain unnoticed throughout the development and shipment period. Generally, the things which are a part of IoT to provide smart services are the vulnerable things [67]. For example, IoT components with obsolete OS versions, weak hard-coded passwords, insecure firmware updates, improper authentication mechanisms, open debugging ports, and insecure interfaces [68]. Even they impose a significant risk to human lives. As per the reports, more than 70 percent of smart devices are prone to stealthy cyber-attacks [12]. Additionally, in near future, 25% of industrial attacks [69] will be caused by compromised smart devices. This scrupulousness could be understood from industrial cyber-attacks like Stuxnet attack [70], and attack on German steel mill [71]. Thus, adversaries easily exploit resource-constrained IoT devices as other connected devices like laptops, desktops, etc. are protected with stable guarding mechanisms. In this article, the root cause of growing threats namely the security vulnerabilities in an IoT system will be covered.

For the sustainable functioning of an IoT system, the balance must be maintained among the interdependent features like energy efficiency, performance, security, and power consumption. The small battery size with a reduced amount of energy lessens the resource availability to secure these power-constrained devices. It is found that with the decrease in resources for security, there is a continuous increase in security requirements of IoT end nodes, pushing the significant research initiatives in lightweight security technologies for constrained devices. The traditional security mechanisms like cryptographic solutions developed for powered devices need more computations and thus consume more power. The state-of-the-art light-weight cryptographic schemes show that Advanced encryption standard and Elliptic curve cryptography are the most preferred one, when compared in terms of limited resources, throughput, chip area, and latency [72].

B. ARCHITECTURE OF IoT

The numbers of IoT framework have been presented by international organizations and working groups namely; International Telecommunication Union [39], Institute of Electrical and Electronics Engineers (IEEE) [40], European Telecommunications Standards Institute [41] and Cisco [42], based on variant nature of requirements of IoT environment. Even so, none of them have been standardized until now. Several research efforts are made to build IoT architecture to meet security requirements. TABLE 4 summarizes the existing IoT architecture and its related security domains. The general IoT architecture given by ITU - Telecommunication Standardization Sector Y.2002 is briefly described in [39]. In this architecture, there are three layers namely Perception Layer, Network Layer, and Application Layer.

Perception Layer: It is the lowest layer in the IoT architecture where the IoT nodes can be RFID readers, RFID tags, QR code, Bluetooth devices, GPS devices, multiple sensors like light, humidity, temperature and so on. These devices could serve different purposes [1], which are as follows.

- Gathering information from the surroundings and transmitting it to the cloud [81];
- Identifying IoT nodes uniquely;
- Actuating the IoT devices as desired based on sensed data;
- Aiding communication among IoT nodes and transmitting the data securely to the gateways.

Network Layer: It is the middle layer, which supports different communication networks like Low Energy Bluetooth, 4G-LTE,5G, ZigBee, Adhoc network, Wi-Fi network, GPRS network, etc [82], [83]. Along with heterogeneous networks, it embraces different technologies and protocols. By using communication mediums, it sends the data collected by the sensory nodes to the high-level decision-making units for initial processing, data analysis, data mining, etc. Additionally, it delivers network management functionality.

TABLE 4. A relative comparison of frameworks for IoT security.

Framework	Application Field	Main Focus	Technology	Limitations/ Future work	Reference
Software Defined Networking(SDN) Architecture	Smart Environment	To control the network of IoT devices as per the requirements.	Provides programmable network services.	Lack of reliable authentication and authorization mechanisms, and sniffing of confidential data.	Valdivieso *et al.* [73]
Smart City Architecture	Smart City	Smooth functioning of smart services	Dempster-Shafer Uncertainty Theory and Semantic Web Technologies	To include scalability and interoperability in the Smart City Architecture.	Gaur *et al.* [74]
SEA Architecture	Smart Healthcare	To improve the security in e-health services	Handshake protocol and both public-key based authentication.	It can be compromised on denial-of-Service (DoS) Attacks and provides no privacy assurance.	Moosavi *et al.* [75]
IoT Middleware Security Framework	Smart Transportation	The interoperability of IoT devices and security of middlewares.	Utilizes Light-weight security services.	Authentication protocols are not addressed and need a lightweight security solution compatibility.	Ramao *et al.* [76]
OSCAR	Smart Grid	The proposed framework for E2E security and access control in IoT, and provides secure multicasting.	Authorization servers, proxy servers, and the Cooja emulator.	Allows unauthorized access due to the latency of ECDSA.	Vucinic *et al.* [77]
SD-IoT Framework	In general, to improve the IoT Management, an SDN based architecture	security of data (produced by IoT objects) has been improved.	Sensor Network Clusters, Database pool rs, APIs.	Not tested in different IoT environments .	Y.Jararweh *et al.* [78]
Black SDN Architecture	Smart City	To handle the vulnerabilities in IoT Systems.	Uses encryption to secure payload and metadata.	Faced complications in Routing.	Chakrabarty *et al.* [79]
Deep Learning-based SDN Architecture	Secure IoT architecture	Focuses on massive IoT deployment featuring security in vast network traffic.	RBM and deep learning.	Practical implementation of proposed SDN architecture.	A. Dawoud *et al.* [80]

Application Layer: It is the topmost layer of IoT architecture, which provides IoT based services to the users globally by using different devices like laptops, mobiles, and personal digital assistants. It provides an interface through which the user can interact with its system. IoT has a wide range of application domains. These include commercial applications, industrial applications, applications specific to people, and consumer-oriented applications as shown in FIGURE 4.

C. PROTOCOL SUITE FOR IoT

IoT being a realm of resource-constrained motes, cannot rely on TCP/IP protocols such as IPv4, TCP, and Hypertext Transfer Protocol (HTTP). Relying on them may lead to wastage

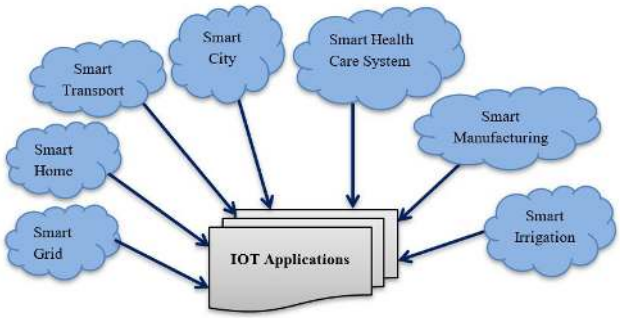

FIGURE 4. Major applications of IoT.

of energy during transmission in the form of voluble meta-data, protocol overheads, and non-optimized communication patterns. The working groups of standardization bodies IEEE and IETF have put forward the communication protocols for resource-constrained devices [58]. The formalized protocol stack proposed by the author as shown in FIGURE 5.

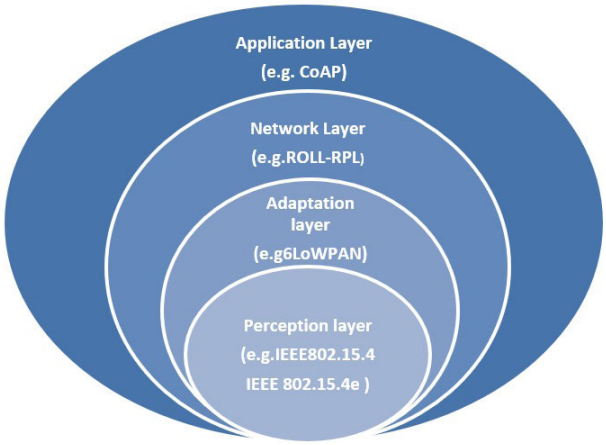

FIGURE 5. IETF protocol suite for IoT [58].

- *Perception Layer IEEE 802.15.4 and IEEE 802.15.4e*: They reinforce low power communications at the bottom-most layers [58]. IEEE 802.15.4 PHY uses Offset Quadrature Phase Shift Keying for modulation with a 2 Mbps data rate on the 2.4-2.485 GHz frequency band. This is the most widely used band. Direct Sequence Spread Spectrum is used for robustness. It provides quid pro quo between energy efficiency, data rate, and range marked at LAN. It also characterizes the MAC Protocol, which tells how motes can communicate with each other and defines the header for MAC. Albeit, IEEE 802.15.4 MAC protocol becomes inappropriate in multi-hop networking. It becomes inapt due to a 100 percent duty cycle, which makes the lifespan of low-power radios reduced to a great extent [58].
  To redesign the IEEE 802.15.4 Mac protocol, the IEEE 802.15.4e working group was made in 2008. While preserving very low duty cycles, it endowed high reliability through time synchronization and channel hopping, using a scheme originally propounded in the form of TSMP [36]. Wireless Hart [84] is also based on this protocol. In TCHP, devices synchronize as per slot frame structure, and a set of slots iterating over time. A schedule is followed by each device that states what to do in every slot. A mote can sleep, receive, or transmit in a particular slot. The mote keeps its radio off in a sleeping slot. For each active slot, the schedule includes the channel offset and the neighbor to whom it gets to transmit or receive. It also defines how the schedule will be executed in the Mac Layer, which may be centralized or distributed. Few modifications are also done to improve the security at the MAC layer by the IEEE 802.15.4e working group [36], [58].
- *Adaptation Layer (6LoWPAN):* To enable IP connectivity in Low Power WPANs, an adaptation layer is introduced between the network layer and lower (Physical and MAC) layers. This layer maps the services between the IP layer and the perception layer. To do the same, the 6LoWPAN working group had been established in 2007. It works on specifications for sending IPv6 packets over IEEE 802.15.4 networks. This layer mainly fragments and reassembles the data packets, because IEEE 802.15.4 supports only 127 bytes as the maximum frame size, which is considered very small to hold even the minimum value of Maximum Transmission Unit 1280 bytes and header overheads [85]. Moreover, it provides stateless IPv6 header compression, mesh routing, and simplified IPv6 neighbor discovery protocol.
- *Network Layer:* To develop the IPv6 routing protocol for Low-Power and Lossy Networks, the IETF RoLL working group was created in 2008. By utilizing routing requirements and quantitative metrics for nodes and links, RoLL developed a Routing Protocol for Low-Power And Lossy networks. It is a distance-vector routing protocol, which allows the nodes to exchange distance vectors and root with a controller to create a Destination-Oriented Directed Acyclic Graph. It aids three kinds of traffic flow: multipoint-to-point, point-to-multipoint, and point -to-point[50]. It is dealing with several issues like end-to-end throughput challenge due to the co-existence of multiple applications in one physical network, packet re-ordering, and rises in the cost of DAG creation and maintenance due to multipath routing structure, and effect of duty-cycling on end-wise latency. The number of solutions has been proposed to conquer them like Queue-aware backpressure routing algorithm, opportunistic routing and networking encoding [1], load balancing [86], and adaptive control on duty cycling [87].
- *Application Layer*: The IETF CORE group has designed CoAP, a protocol for web transfer in a constrained environment. We cannot say CoAP as a wadded form of

HTTP [88]; it's just a part of Restful specification, which makes it compatible with constrained environments. CoAP endorses datagram-oriented transport protocols, such as User Datagram Protocol (UDP). CoAP aids reliable transmission over UDP. A messaging layer is responsible for reliability and sequencing, whereas a request/response layer maps requests to responses as well as their semantics. The conspectus of the main features [58] provided by CoAP is as follows.

1) A web protocol specialized in Machine-to-Machine requirements and a constrained environment.
2) It provides Stateless HTTP mapping.
3) It supports unicast and multicast requests by binding UDP with optional reliability.
4) Enables Asynchronous message exchanges and built-in resource discovery.
5) Parsing complexity and Low header overhead.
6) Limited to simple proxy as well as caching capabilities.

D. OPEN SOURCE TOOLS AND DATASETS

There exist many open-source tools, which accelerates the growth of IoT-based applications. Moreover, open-source tools and datasets aid researchers in formulating theories, devising experimental results, and developing system models. TABLE 5 briefly describes the commonly used open-source datasets in the IoT realm. The widely-used open-source tools are as shown in FIGURE 6 and described briefly in this section.

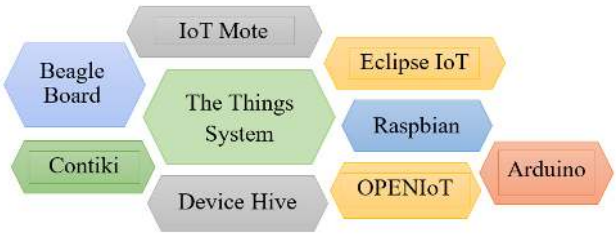

FIGURE 6. Open-source tools for IoT [89]–[93].

The Arduino is an open-source electronics platform, that helps in developing IoT systems. It consists of a microcontroller which can be programmed with the help of Arduino programming language; can take inputs which can be either a simple text message, light sensed by a sensor, a fingerprint, etc. and can produce outputs like turning on the motor, lighting an LED, sending the text message, etc. Moreover, Arduino Software could be used for the same. All Arduino boards, Arduino programming language, and Arduino Software are open-source, emancipating developers to freely design them and use them as per their individual needs [89]. Eclipse IoT is a working group of companies which run open source community for IoT. More than thirty companies are working together, namely IBM Redhat, Bosch, Kichwa coders, Eurotech, V2com, etc. It provides everything needed to build IoT solutions moving from constrained devices, gateways, cloud platforms, standards, protocols, etc [94]. It also provides IoT open source projects, resources like case studies, white papers, newsletters, and aids virtual IoT Meet up [90], [95].

Beagle Board is a non-profit corporation that makes the masses about the design and uses open-source hardware and software within embedded computing. It also provides a forum to exchange ideas. Moreover, headways towards open-source computing solutions comprising robotics, machine controls, and manufacturing tools like 3D printers. Beagle Boards are fan-less boards with power-efficient Texas processors, even expansible to desktop machines, unaccompanied by bulk, expense, or noise. The open-source designs of these boards are also available for making compatible hardware [91]. An Italian company, IoMote, which provides a range of programmable, Arduino-compatible, IoT Edge Devices so that anything can be connected to cloud easily. It empowers reliable and secure bi-directional communications between millions of IoT devices, using Mymote Cloud software, running on Microsoft Azure [102]. It provides products like X400 - an IoT Edge Gateway, Arduino-compatible easy to program and appropriate solution for high-end IoT projects that require optimal security and bidirectional real-time communication. Similarly, they have come up with XSense: NB-IoT Wireless Sensors, embedded with a large number of variant possibilities of flexible sensors for air, noise, water, and many more [103]. It provides longer battery life, global coverage, resilient with problems due to walls, and cost-efficient [104].

Arduino Ethernet Shield connects the Arduino board to the Internet with the help of Ethernet library and activates it to communicate across the world [105]. OpenIoT has come up with a platform to design and manage environments containing IoT resources. It also leverages on-demand utilities for IoT systems, for example, sensing-as-a-service [106], [107].

Contiki [108] is also an open-source operating system for IoT that connects tiny low-cost, power-efficient microcontrollers to the Internet. It supports IPv6, IPv4, with low-power wireless standards. It has provided a lightweight flash file system, called Coffee; an optional command-line shell, tailored wireless networking stack called Rime. A set of nightly regression tests are run on a daily basis in the Cooja simulator, for testing the Contiki code [109].

Raspberry Pi [110] is a card-sized affordable computer that could be used for several purposes as for learning programming, IoT projects. It is not entirely open-source, though the software and documentation are. Raspbian is an operating system for Raspberry Pi, based on the Debian distribution of Linux [111]. DeviceHive is a free, highly scalable open-source IoT platform that provides modules for data collection, processing, and analysis, visualization, device management [92], etc. For developing Smart home solutions, various Home Automation Softwares are available like Eclipse Smart Home [93] and The Thing System [112].

TABLE 5. Summary of open available IoT datasets.

Dataset	No. of instances	Description
CRAWDAD [96]	Dynamic	Acts as a place to share the data sets across the research community about the production wireless networks (and their users), location of people using mobile phones, etc.[50]
Linked Sensor Data [97]	160 million instances.	It provides datasets for sensors, built at Kno.e.sis Center, using weather data of Mesowest.
Japan Traffic Flow [98]	Passenger flow between 51 regions of the nation and cargo flow between 54 regions.	A record of cargo and passengers flow within the nation derived from Report on Cargo/Passengers Flow in Japan.
NPTLab [99]	Dynamic	It contains the profile information about the Google+ users who have links with Twitter or Facebook profiles publicly; Google+ and Twitter train/test sets.
UCI. Machine Learning Repository [100]	Dynamic(Multi-purpose dataset repository like air quality, GPS trajectories, bank marketing).	The UCI ML-based Repository contains data generators, several databases, and domain theories.
INTEL Lab Repository [101]	Instances for the period of 36 days.	This repository stores data about the environment collected using S4 Mica2Dot sensors.

III. IoT VULNERABILITIES: CONCEPT AND SECURITY ASPECT

Due to vulnerability breaches and cyber-attacks the security of IoT is in an alarming state [55], [113]. The number of unanticipated vulnerabilities and exploits are reported, that was designed to take advantage of security gaps in systems and deployment configurations. Some of them, like Mirai, BrickerBot, and Hajime, are discussed in the following subsections. Traditionally, security requirements were mainly defined by three properties: confidentiality, integrity, and availability, as coded by CIA Triad. But the security mentioned above properties of CIA Triad turned out to be insufficient in the context of security [114], [115]. A comprehensive list of security requirements known as the IAS-Octave [114] taken as an extension to CIA Triad is summarized in TABLE 6. Also, the transition from the CIA Triad to IAS-Octave is shown in FIGURE 7.

Vulnerability is a kind of a hole or flaw in a system which if left unhandled, could lead to serious threats to the whole system. These security threats could be seen concerning different layers in IoT Architecture, as shown in FIGURE 8. Talking about the sheer number of IoT application domains, which are in no way less affected by these threats, described briefly in TABLE 7. Moreover, IoT manufacturers treat security as an afterthought. Like that, IoT will lose all of its incredible potentials. The vulnerability assessment will play a significant role in protecting IoT devices from these growing threats. In the sequel, under FIGURE 9, we elaborate on the device-based proposed taxonomy of vulnerabilities in IoT devices [116].

a) *Physical Security of IoT Nodes:* The IoT nodes must be physically hardened to prevent the risks associated with the direct physical access to these unattended devices.

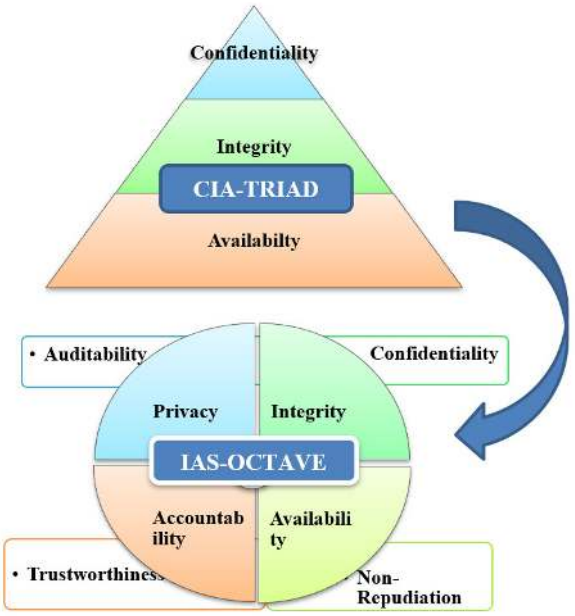

FIGURE 7. IAS-OCTAVE [114].

The adversary enters the system through USB or some other ports kept open for maintenance or configuration. He can directly access the SD card and other storage medium to get the control over operating system and gain sensitive data like embedded passwords. Thus, the lack of physical hardening can result into attacks like node cloning and side-channel attacks.

- *Node Cloning:* The clones of the IoT nodes could be made with ease as they remain in unattended surroundings. Moreover, there is no standard

TABLE 6. Security requirements.

Security Requirement	Definition
Integrity	To ensure correctness, completeness, and absence of unauthorized data manipulation.
Availability	To ensure timely and reliable access to all the system services when requested by authorized entities.
Trustworthiness	The ability to verify the identity before giving access to resources and to establish trust.
Non-Repudiation	To ensure one canâĂŹt deny the act it has done
Accountability	It makes sure each and every activity to be tracked to an individual.
Privacy	To ensure the user has control over the disclosure of his personal data
Auditability	The capability to carry out constant uninterrupted audit on all the actions.
Confidentiality	To ensure the information remains confidential by giving access to only authorized users.

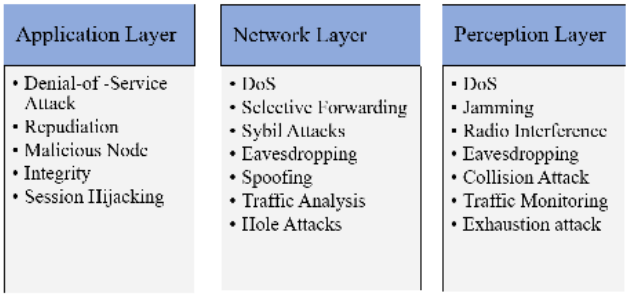

FIGURE 8. Layer oriented threats [55].

mechanism to develop IoT devices with a hardware tamper-proof. By making replicas of IoT nodes, the adversary could launch the number of attacks. He can use the credentials of compromised nodes to have access over the network [12].

- *Side-channel attacks:* These attacks aim at getting the side channel information about the device performing cryptographic operations. This information includes physical characteristics of a machine while carrying out those operations, i.e., data about the power consumption, processing time, electro-magnetic emissions, and the sounds it produces. Then this information is used to reverse engineer the cryptography system being used by the device [117].

b) *Open Debugging ports*: The potential attackers can easily exploit vulnerable network services running on the target device through open ports. The manufacturers ship most of the IoT devices without disabling their debug ports. These ports could be used to take full control over the system. The intruder could inject malicious code, modify the firmware, bypass the security, spy, and bag their data. Hence, a plethora of attacks could be launched through these open ports [118], [119]. For instance, most of the botnets like Mirai, BrickerBot exploit telnet port. BrickerBot, another IoT botnet unveiled by researchers at Radware in April 2017. This malware launched a permanent denial-of-service attack, which prevents the prey's hardware from functioning. To create a botnet, it included all the devices exploited by Mirai or other botnets. These devices were with open SSH port(22) and older versions of SSH Server. It also targeted the devices with open Telnet port (Linux /busybox based). Furthermore, it leveraged the default login credentials by consistently attempting 'root'/'vizxv. It can affect in many ways, for example, can corrupt storage [14].

c) *No energy Harvesting*: The sparse resource nature of IoT nodes makes them vulnerable to resource exhaustion attacks. Moreover, there is no mechanism to harvest the energy of these low-power IoT nodes [120]. These attacks could jam the communication channels and can cause extensive unauthorized utilization of IoT resources like bandwidth, memory, CPU time, disk space. It leads to battery drainage of IoT nodes, and they could not provide their services to legitimate users [10]. By exploiting this vulnerability, the adversary can launch the battery drainage attacks, sleep deprivation attacks, Node outage, DoS attack, etc.

- *Battery drainage attacks:* IoT nodes work with low-power battery and that too with no recharging mechanism. The intruder floods the node with so many legal requests that it ends up with exhaustion. The number of attacks can be launched by draining the energy of a node [122].
- *Node outage:* It prevents the edge nodes from performing their function in the system. The number of factors like- battery drainage, code injection, unauthorized access, sleep deprivation could lead to this attack [110].

d) *Weak Authentication Mechanisms:* Implementing strong authentication mechanisms at different interfaces like mobile, cloud, and web in the IoT ecosystem makes them more secure. The adversary targets these insecure interfaces through weak credentials and account enumeration. If anyone can access the IoT nodes without undergoing identity checks or bypassing the weak authentication system, then the adversary can exploit the system in numerous ways [123]. The adversary may launch DoS attack, steal data, and take complete control of the system. It becomes difficult to implement strong authentication mechanisms due to a lack of adequate resources for IoT devices. Under such conditions, the authentication keys must be exchanged and stored securely to ensure effective authentication. The number of attacks could be framed out by exploiting this vulnerability.

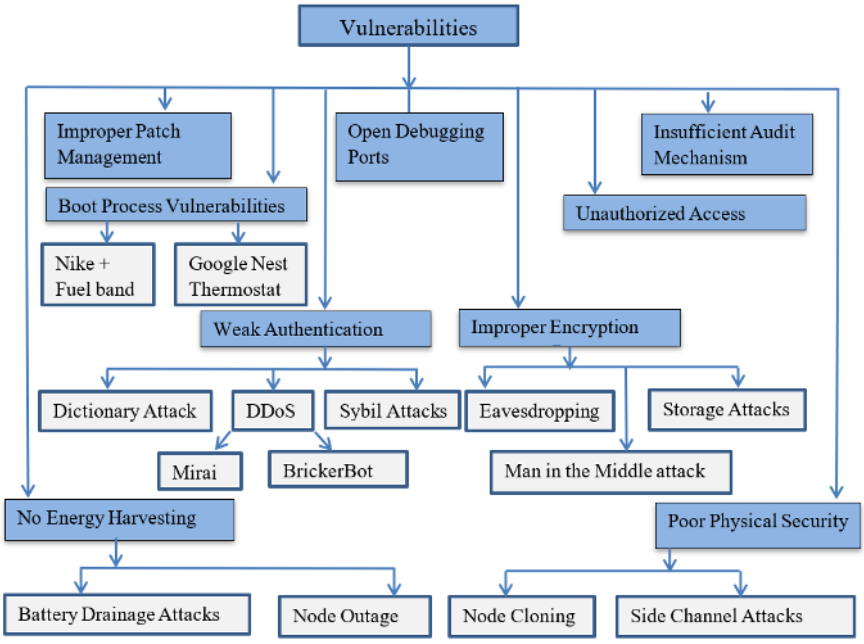

FIGURE 9. Taxonomy of vulnerabilities in IoT [10], [12], [121].

TABLE 7. Security threats in IoT application domains.

Security Threats	Application Domain	IoT Devices
Authentication, Privacy, Eavesdropping, Authorization	Smart City	Smart homes, smart transportation, smart street lighting, location-based services, smart power generation
Privacy, Eavesdropping, Physical Attack, Tampering	Smart Grid	Smart Meters, Smart Readers, smart remote power outlets, data concentrators, power line communications
Authentication, Privacy, DoS, Authorization	Smart Health Care Systems	Sensors, Smart wearable devices, glucose monitoring system, infusion pump devices, implantable devices, databases
Jamming, Congestion, security and spectrum sharing	Intelligent(Smart) Transportation	Traffic lights, parking systems, IoT enabled cars, road sensors,public transport, computers, smartphones.
Authentication, Physical Security, Non-Repudiation, Physical Security, Authorization	Smart Manufacturing	Smart equipment, sensor networks, factory databases, computers, web servers,
Confidentiality, Integrity, Availability, Accountability	Smart Agriculture	Sensors for soil moisture, livestock monitoring, atmospheric monitors, greenhouse sensors, Aerial drones, smart irrigation controllers, smartphones
Confidentiality, Authentication, Physical Security, Non-Repudiation, Availability, Accountability, Integrity	Smart Supply Chain	Sensor Networks, web applications, Tablets, RFID tags and readers, databases, laptops, webservers, mobile applications.
Confidentiality, Availability, Accountability, Integrity, Non-Repudiation	Smart Home	Smart TVs, Smart Security Cameras, Smart Door Locks, smartphones

- *Distributed denial-of-service (DDoS) attack*: IoT nodes could easily be used as bots to target DDoS attacks. This ease imposes the risk on the Internet in terms of distributed attacks. The availability of vast no. of 24/7 insecure IoT devices, their poor maintenance, and minimally interactive user interfaces draw the intruder's intention towards them. Mirai and its variants highlight such attacks. Mirai malware was first unveiled in August 2016. In September 2016, two DDoS attacks using the Mirai malware were launched against the website of Brain Krebs, the computer security

consultant, and the French web host. The following month, it targeted the service provider Dyn and caused many sites to shut down for several hours, for example, with the use of Netflix, Twitter, GitHub, Reddit. Mirai launches the DDoS against target servers by building a network of weakly configured IoT nodes. The no. of infected nodes named bot instances was more than double within two months after the release of the Mirai source code. Even today, the same vulnerabilities of smart nodes are exploited by Mirai and its variants [14].

- *Dictionary Attack:* It is a brute force attack in which the intruder enters/access the IoT system/device by trying all the combination of characters in the dictionary to break the security. Kolias *et al.* [14] described how the dictionary attack leads to highly distributed attacks. It creates an army of millions of infected nodes by compromising their security to launch attacks like DoS, DDoS.
- *Sybil Attack:* It causes the malicious node to impersonate the real IoT node by manipulating the identity of compromised nodes. This attack adversely affects network performance. The forged device may flood channels with false packets to make the services of IoT system inaccessible to authorized users, can eavesdrop on traffic, fabricate the message and much more [124].
- *Hello flood and Homing Attacks:* In this attack, the adversary leverages the fact that the new node sends the "HELLO PACKETS" among all the neighbors when it is added to the network to indicate its arrival. At this, all the receiving nodes assume the sender node to be in their communication range. For this attack, the attacker uses the node with higher transmission power [125].

e) *Improper Encryption*: The integrity of smart applications depends upon the security of data collected by widespread sensors. The data must be safe and verifiable both at source and in transit.Most of the IoT devices use less reliable wireless communication media, for example, NB–IoT, Zigbee, SigFox, LoRa, 802.11. a, and 802.15.4. As a consequence, these devices are more susceptible to data leakage attacks [126]. It is also found that most of the IoT devices collect the personal information of users to provide essential services. In the case of e-health, misuse of this personal information can be life-threatening and, in some cases, unavailability of scathing health services [127]. Encryption is an efficient way to protect the users' data from disclosure to unauthorized users. However, the resource limitations of IoT devices makes it difficult to develop a robust crypto-algorithm. As a result, the adversary can easily dodge the deployed crypto-algorithm. This may lead to many more serious attacks [10].

f) *Unauthorized Access*: To prevent unauthorized access to an IoT system, a secure credential management system should be implemented. Today the market is flooded with IoT devices having hardcoded, weak, or default credentials. No one takes care to change the default credentials and there it creates a hole for attackers. In the most significant DDoS attack, namely Mirai, the attackers used around 60 default login credentials to turn IoT nodes as the malicious one. It reached to 1.2 TB per second [14]. Furthermore, baby monitors were shipped with hardcoded credentials, which could only be fixed by firmware patch [17].

g) *Insufficient Audit Mechanism*: There is as such no mechanism to maintain the logs of what has been done in the IoT devices and check them time to ensure their security [128]. The events like application errors, successful/failed login attempts, authentication attempts, authorization attempts should be logged in an encrypted log file.

h) *Improper patch management*: The operating system of IoT devices and their firmware must be updated regularly so as to augment its function and protect against attack vectors. Albeit it is found that in IoT devices, the manufacturers skip the automated patch-update feature. Moreover, they do not provide the security patches on time and that too may lack integrity assurance. The insecure updates may contain malicious patches which can adversely affect the devices at large [129]. To ensure the security of updates,the update file must be verified, signed, encrypted, and transmitted via a secure connection.

i) *Boot process Vulnerabilities*: During the boot process, all the three – firmware, boot loader, and boot process sequence is vulnerable to get leverage with. For instance- In an experimental setting, the researchers launched such attacks against the Nike+ fitness tracker and Nest Thermostat [130].

Google Nest Thermostat got compromised over this loophole, where the adversary loaded the thermostat with a malicious initial boot loader along with a custom full boot loader and an argument list for the onboard kernel. The arbitrary payloads like backdoor could be added later on using a custom loader. They made the processor to boot from UART or USB interface and inserted their boot loaders. They even made it possible to accept updates from a source other than Nest [128].

IV. TAXONOMY OF IoT VULNERABILITY ASSESSMENT TECHNIQUES

The unique traits of IoT devices with its growing number have made it difficult to continuously figure-out evolving IoT-specific vulnerabilities. Furthermore, attackers are getting more skilled in launching stealthy attacks. To secure IoT and to make it more resilient, the security mechanisms must include the regular vulnerability assessments as an integral

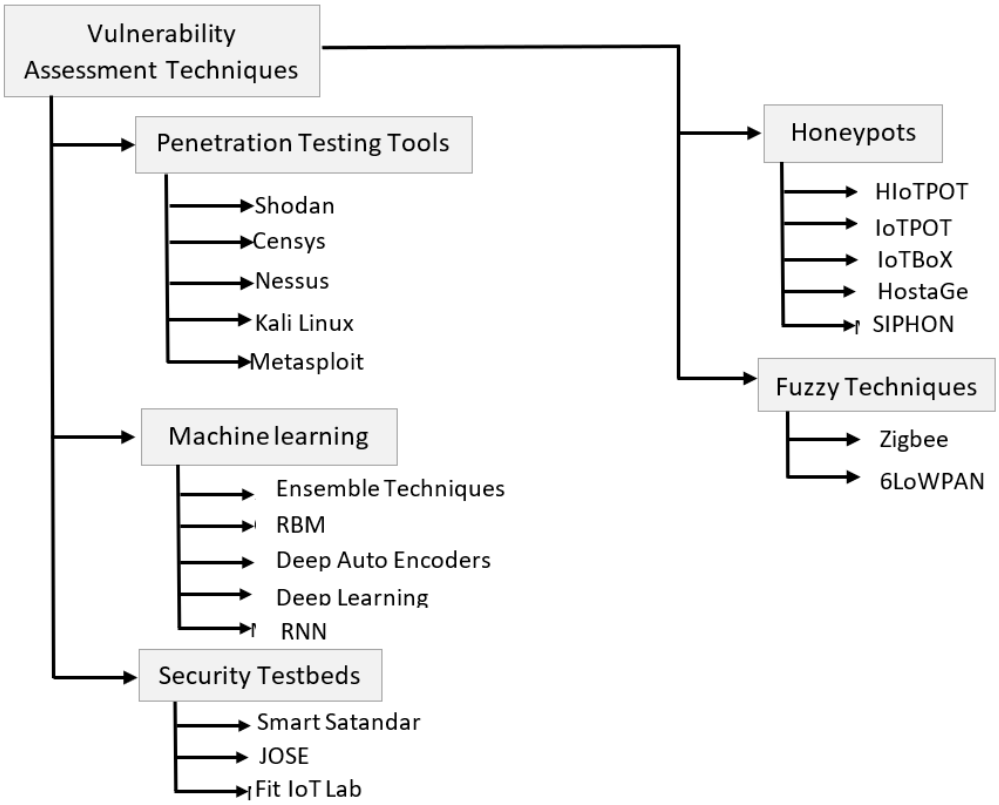

FIGURE 10. Taxonomy of IoT vulnerability assessment techniques.

part. In this context, we have explored various monitoring and security assessment strategies, which are depicted by FIGURE 10 and described as follows.

a) *Security Testbeds:* The security evaluation of a system before its deployment helps in discovering IoT vulnerabilities before their exploitation. In this context, either we can develop new testbeds or modify the existing testbeds to assess IoT vulnerabilities. Further, one such testbed designed by Tekeoglu and Tosun [131] includes software like Kali Linux, Nessus, bindwalk, and Open VAS for security tests. The proposed testbed identifies vulnerabilities by analyzing the features extracted from the network traffic. The testbed supports numerous experiments, including vulnerability scans, privacy violations, and identifying insecure protocols. The authors inferred that almost all the IoT devices run with outdated firmware versions, unnecessary open ports, and no mechanism to block the user after multiple failed login attempts.

In an alternative work, two IoT testbeds Reaves and Morris [132] based on Industrial Control System (ICS) were designed to identify vulnerabilities in different set-ups. The previous testbed works in a laboratory with physical devices, and the latter uses python scripts to emulate device behavior. The authors claim that both the virtual testbeds are inter-operable with real control systems and efficiently emulate real systems in terms of threats too. In another work, the authors [133] presented a scalable framework, named as Small-world. In this platform, several scenarios are made using simulation and virtual environments to find the vulnerabilities within the IoT system. The proposed platform consists of five layers, namely, perception, abstraction, services, API, and management layers. Further, the authors considered a case study on home automation applications using virtual and real smart devices to show the effectiveness of the proposed work. Additionally, Siboni *et al.* [134] proposed the IoT testbed integrated with multiple plugins for penetration testing. The architectural model of testbed works in four modules; a module for management and control actions, a module responsible for actual testing sequence, a module to execute a set of security tests, and the last for measurements and analysis. The Security Testing Module provides the number of plugins for security tests like Fingerprinting, Port Scanning, Process Enumeration, Communication Tampering, and Vulnerability Scan. The IoT devices are tested in multiple test scenarios in the proposed testbed. As an extension of this work, the authors plan to implement the proposed security testbed with testing systems, such as an IoT-based honeypot environment. On similar lines, Siboni *et al.* [135] proposed a testbed specifically on wearable devices. The vulnerability

assessment is also one of the modules under various IoT testbeds [136]. TABLE 8 provides an overview of the IoT testbeds.

b) *Machine Learning:* Machine learning is a part of an umbrella term AI that provides the machine with the ability to learn from experience, examples, and analogies [140]. As learning occurs, the machine becomes more intelligent and capable of making informed decisions. The objective of machine learning is to efficiently imitate human learning activities by computers such that the knowledge can be automatically discovered and acquired. Several machine learning algorithms have been widely applied to improve IoT Security. A learning algorithm is one that takes as an input a training set and tested upon the testing dataset. Some of the widely used machine learning tools for implementing learning algorithms are described in TABLE 9. In general, there are three main categories of learning: supervised, unsupervised, and reinforcement learning [141], as shown in FIGURE 11.

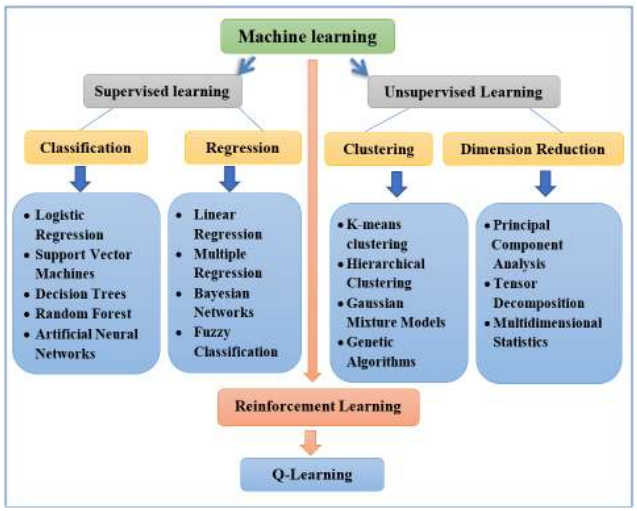

FIGURE 11. Machine learning techniques [140], [141].

The resource-constrained IoT devices can neither rely on existing security solutions nor lightweight security mechanisms. The former class suppresses the IoT nodes with computation and communication freightage. The latter opens the doors for intruders to enter with ease. Machine Learning is a promising solution at this end. Moreover, the main element in Machine Learning is data. The widespread IoT led to the generation of enormous data regularly, which can be concluded as a goldmine for machine learning. The intelligent system learns from a massive amount of data and provides high efficiency and considerable accuracy with minimum computation cost. In [47], the authors stressed the usefulness of ML in IoT in terms of its scope, security, and inferring insights from data. The significant applications of ML-like detecting outliers, pattern recognition, feature extraction, and predicted values are essentials of IoT security. The review of nascent solutions based on machine learning to cope with growing attacks are discussed in the following sub-sections and shown in FIGURE 12.

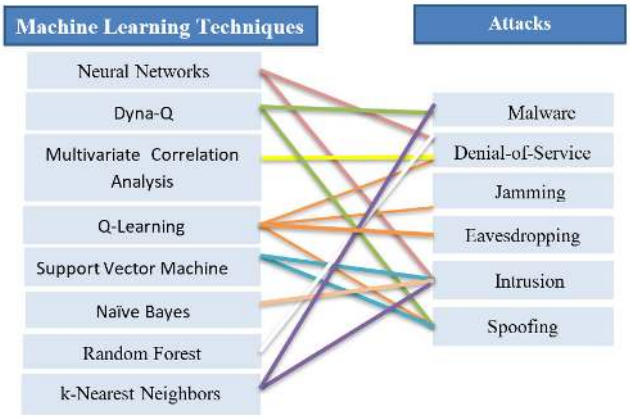

FIGURE 12. Machine learning-based IoT security techniques [142]–[147].

Azmoodeh *et al.* [148] proposed an OpCodes based deep learning method to detect malware on the Internet of Battlefield things. The authors used a class-wise information gain method for feature selection (OpCodes sequence). The VirusTotal3 Threat Intelligence platform was used to collect the malware samples between February 2015 and January 2017 [149]. Furthermore, the official IoT App stores (Pi Store 4) were used to collect goodware samples. The opcodes were extracted by using objdump. It is revealed from their research that the proposed approach with accuracy rate (AR) 99.68 percent, precision rate (PR) 98.59 percent, and recall rate (RR) 98.37 percent outperforms the other approaches [150], [151].

Hasan *et al.* [152] proposed the Multiclass Classification model for attack and anomaly detection using several ML Approaches. The proposed system gives 99.4 percent test accuracy for Random Forest, DT, and ANN. The Random Forest outperforms the remaining techniques in terms of other performance metrics. Similarly, Pajouh *et al.* [153] proposed a two-tier model for detecting suspicious behaviors. Moustafa *et al.* [154] proposed an ensemble intrusion detection technique for protecting network traffic of IoT. The authors presented an AdaBoost ensemble learning method for detecting malicious events in a network. These features are generated from protocols, namely Domain Name System, HTTP, and MQTT. The authors concluded that the given ensemble technique yields a high detection rate (DR) and a low false-positive rate in comparison to ANN, Decision Tree, and Naive Bayes. In another notable work, Kotenko *et al.* [155] proposed the Machine Learning based framework for securing

TABLE 8. IoT testbeds.

Testbed	Description	Scale	Environment
FIT IoT Lab [137]	Multi-user and multisite concurrent testbed; Located in France(across six sites); Programmable robots provide the mobility.	Medium (>2700 sensors)	Laboratory-like environment
Smart Satandar [138]	Aids Supported nodes to remotely deploy new firmware using Over-The-Air Programming; Located in Spain(Satandar); Primarily used to evaluate IoT services in the smart city domain. (smart parking, smart irrigation environmental monitoring) Âů By using their mobile devices, citizens can also en participate in sensing.	Large(>20000 sensors)	Real City
JOSE [139]	Located in Japan(Across five data centers); Primarily used for IoT service evaluation (uses Infrastructure As A Service model); Supports the concurrent execution of several IoT services; Facilitates customization and management of the service-specific virtual infrastructure and networking using SDN.	Large(exact sensor count is not identified)	Outdoor Environment
Secure IoT testbed [136]	Port Scanning for open and vulnerable ports; Fingerprinting for deviceâĂŹs information like MAC, IP address, OS, manufacturer; Vulnerability Scanning for getting the vulnerabilities of the various OS.	Medium	iTrust Lab
Security Testbed (IoT) [134]	Testing in different configurations, using the standard as well as advanced security testing; ML-based processes are engaged for monitoring IoT nodes under test.	Medium	Laboratory

TABLE 9. Some popular machine learning tools.

TOOLS	OPEN SOURCE	SUPPORTED LANGUAGES	NEURAL NETWORKS	AS GENERAL PURPOSE TOOL
Python	Yes	Python	Yes	High
R	Yes	R	Yes	Medium
Spark	Yes	Scala,R,Java,Python	Multilayer Perceptron Classifier	Medium
Matlab	No	Matlab	Yes	High
Tensor Flow	Yes	Python, C++	Yes	Low

IoT. The proposed framework is implemented on five individual basic classifiers and their different combinations. The authors have used a multi-level scheme to combine these basic classifiers. The results claim that the combined classifiers outperform the separate basic classifiers with reference to accuracy, True Positive Rate (TPR, and FPR). On similar lines, Punithavathi *et al.* [156] developed a lightweight ML-based authentication model for IoT devices using a Cancelable Biometric System. The authors used Random Projection to create a cancelable biometric template. The experimental analysis suggests that the proposed framework takes less time and has minimal error rate compared with other such techniques and thus suitable for IoT environment.

Additionally, Dawoud *et al.* [80] presented a secure framework for IoT based on SDN and Deep Learning. The authors utilized RBM to find the anomalies by using the KDD99 dataset. The simulation results depict a precision rate of over 94 percent. On similar lines, Diro and Chilamkurti [157] developed the DL-based Distributed attack detection scheme for IoT. D'Angelo *et al.* [158] applied U-BRAIN technique on real network traffic for anomaly detection. The U-Brain, being a dynamic model, can handle the missing data. The results show that the U-BRAIN technique outruns the fundamental classification methods. Kumar and Gandhi [159] used a logistic regression-based prediction model on the massive amount of data collected by wearable sensor devices for early detection of heart diseases(in IoT health monitoring system). Meidan *et al.* [160] proposed a novel approach N-BaIoT, a network-based anomaly detection strategy for IoT devices. The authors found that IoT devices are more susceptible to IoT-based botnet attacks, and these attacks must be detected instantly to isolate the compromised device from the network. This prevents the botnet from further propagating. They trained a deep autoencoder for each IoT device by using behavioral shots of benign IoT traffic. The autoencoders

are unable to reconstruct the snapshots of the traffic of compromised nodes. Moreover, they have done the performance evaluation with real-time network traffic, collected from nine infected commercial IoT devices in their lab with Mirai and Bashlite botnets.

Chatterjee *et al.* [161] proposed a Radio-Frequency based PUF authentication scheme: Physical Unclonable Functions (PUF) exploit radio frequency-based manufacturing process variations to identify wireless sensor IoT nodes uniquely [162]. The transmitters are authenticated at the receiver's end by using the deep neural networks, an in-situ machine learning-based framework. The proposed framework is simulated in MATLAB, with a 16-Quadrature Amplitude Modulation modulation scheme, and under varying channel conditions. The neural network used features like LO offset, I-Q imbalance and have 50 neurons in the hidden layer of NN, claiming 99 percent accuracy for 10,000 transmitters. The authors also compared RF-PUF with other PUFS in terms of False Alarm Rate (FAR) and False Positive Rate (FPR) given by Maes [163].

Additionally, Jagmohan *et al.* [164] designed a breath-based authentication model by using Recurrent Neural Networks (RNN). The authors used a breathing acoustics dataset. They utilized the combination of frequency wrapping and amplitude scaling to increase the number of data samples. The results of their research claim that the Long short-term memory-based model (a variant of RNN) outruns the Support Vector Machine (SVM)-based shallow classifier with reference to memory loading time, inference time, accuracy, size. Moreover, their experiments convey that RNN based models are lightweight compared to Convolution Neural Network (CNN) based models [165], [166]. The authors have also shown that the memory requirement of RNN models can be reduced by a factor of 5 by using linear quantization–based compression technique without compromising accuracy. Moreover, the performance can be improved using GPU offloading approaches.

Jayasinghe *et al.* [167] proposed a quantifiable trust accessibility model. As per the authors, trust plays a crucial role in the successful future of IoT. The authors have used a numerical method to extract basic trust features. Furthermore, they applied unsupervised machine learning algorithms: k-means clustering to label the interactions as trustworthy or untrustworthy based on the trust mentioned above attributes. They calculated the optimal cluster size using Elbow Method and further used Principal Component Analysis to reduce the size of the training matrix. To bring the data samples in the range of 0 and 1, features were normalized. They used Radial Basis Function Kernel to get the non-linear boundary which can separate the trustworthy and untrustworthy interactions and learn how to combine trust Attributes in the best way to obtain a final trust value.

In the IoT based Grid system, machine learning techniques are applied for proper analysis of the large volumes of data and thus aids in decision making to run the grid (smart). These techniques proved to be useful in a number of ways, such as the prediction of power consumption, price, power generation, detection of network intruders, future optimum schedule [151], [168], etc. Li *et al.* [169] analyzed user proclivity in a smart grid by applying machine learning techniques to find usage patterns. Remani *et al.* [170] applied reinforcement learning for scheduling residential load taking into cogitation renewable energy sources as well. For short term prediction in terms of load forecasting in smart grids, deep neural networks are used by Ryu *et al.* [171], [172]. TABLE 10 presents the summary of ML-based solutions to assess the vulnerabilities and to secure the IoT system. Moreover, Machine learning has been increasingly used in predicting vulnerabilities like Cross-Site Scripting, SQL Injection, file inclusion vulnerabilities, remote code execution in web application [139], [175]. Even some of the proposed platforms also provide the feature of vulnerability correction [139]. There is an ongoing project named the High Assurance Cyber Military Systems program, announced by DARPA in 2012 in the US to patch the vulnerabilities of IoT, particularly the military vehicles, drones, and medical equipment [35].

c) *Fuzzy Techniques:* A research direction in this realm applies fuzzy-based approaches to assess the security of IoT protocols. Lahmadi *et al.* [176] designs one such framework, which evaluates the 6LoWPAN protocol. The proposed testing suite employs the mutation algorithms on messages on the network layer, to find the deviation of actual responses of IoT nodes from the conventional ones. On similar lines, in [177], a fuzzy technique is applied on Zigbee networks to find the vulnerabilities within the network. The proposed technique is the combination of Finite State Machine with Structure-based fuzzy algorithms. After conducting a series of performance tests, the authors claim that the proposed finite state machine- based algorithm is more accurate than a structured-based algorithm. In another noticeable work, the authors have given a fuzzing tool EUFuzzer which discovers the vulnerabilities in human machine interfaces [178]. Several graph -based solutions have also been given to find the vulnerabilities and secure IoT networks [179], [180].

d) *Honeypots:* The honeypots trap the adversaries by imitating real IoT assets but having no value for them, by calculatedly creating security vulnerabilities. With the help of honeypots, we can determine the strategies and attack paths used by attackers to carry out malicious activities [181]. In context to IoT,

TABLE 10. Overview of machine learning based IoT security solutions.

Name of the Technique	Author and Year	Vulnerability/Attack addressed	Dataset Used	Performance Analysis	Limitation
U-BRAIN algorithm	Angelo *et al.* [158]	Network Anamoly Detection	NSL-KDD training set	AR = 94.10% PR = 93.60% RoC area=93.00	The need of an incremental knowledge construction and refinement process ;Periodic Retraining
Deep Learning Approach	Diro *et al.* [157]	Distributed attack detection scheme	NSL-KDD dataset	AR = 98.27% DR=96.5% FAR = 2.57%	Analysis of payload data.
OpCode-based Deep Eigenspace learning Approach	Azmoodeh *et al.* [148]	Malware Detection	Own Synthetic	AR = 99.68% PR = 98.59% RR = 98.37%	Not implemented on broader datasets.
Deep Autoencoders	Meidan *et al.* [160]	IoT Botnet Attacks	Own Synthetic	TPR=100% FPR=0.07	Features ranking using predictability level.
Deep Neural Networks	Chatterjee *et al.* [161]	An RF-PUF based Authentication scheme	Own Synthetic Dataset from 10,000 transmitters	AR = 99 %	No practical implementation of RF-PF
Recurrent Neural Networks (RNN)	Chauhan *et al.* [164]	Breathing based Authentication model	Own Synthetic	Accuracy Greater than 90%	Not implemented on larger corpus; To check the performance using GPU ofloading
k-means clustering, Principal Radial Basis Function Kernel (RBFK)	Jayasinghe *et al.* [167]	Quantifiable Trust accessibility model	Crawdad	FPR = .41% PR = 89.74% RR= 100%	Not implemented on real world IoT dataset.
Logistic Regression SVM, DT, Random Forest, ANN	Hasan *et al.* [152]	Multiclass Classification model for attack and anomaly detection	Distributed smart Space Orchestration System(DS2OS) dataset.	AR(LR)= 98.3 AR(SVM) = 98.2 AR(DT) = 99.4 AR(RF) = 99.4 AR(ANN) = 99.4	Not implemented on Big Data and real-time data; to develop a robust detection algorithm
NaÃŕve Bayes k-Nearest Neighbor	Pajouh *et al.* [153]	Intrusion Detection	NSL-KDD dataset	DR=84.86 FAR =4.86	To explore other Machine learning techniques to counter the attack. To detect intrusions on other layers.
Random Projection on Cancellable Biometric Template	Punithavathi *et al.* [156]	Authentication Framework	FVC2002, 2004 DBI & DB2	Not appropriately defined	Not implemented in real system.
Ensemble Technique(Decision Trees,ANN,NaÃŕve Bayes)	Moustafa *et al.* [154]	Intrusion Detection (botnet attacks)	UNSW-NB15 and NIMS datasets	UNSW-NB15 AR= 99.54% FPR =1.38% DR=98.93% NIMS dataset AR = 98.29% FPR=2.01% DR=97.38%	To collect relevant features from protocols other than DNS,HTTP,MQTT. To implement the proposed ensemble technique on these features.
ESFCM method	Rathore *et al.* [173]	Distributed attack Detection	NSL-KDD dataset	AR =86.53% Lower Detection Time = 11 milliseconds.	Performance could be improved.
Restricted Boltzmann Machines (RBM)	Dawoud *et al.* [80]	Intrusion Detection System	KDD99 dataset	PR=94%	No practical implementation of proposed scheme.
Multi-View Disagreement-based semi-supervised learning.	Li *et al.* [174]	To classify spam and legitimate emails.	Own Multi-view dataset(Lower error rate in intrusion detection)	Classification Accuracy=93.2%	To explore the performance using other semi-supervised learning algorithms in the proposed model To find the optimal way of constructing the Multi-View dataset.
Multiple Classifiers and their combinations.	Kotenko *et al.* [155]	Anamoly Detection	Detection_ of_IoT_botnet _atta*cks_N_BaIoT" dataset..	More accuracy is observed in case of using Combined classifiers	To examine other machine learning methods such as dynamic Bayesian networks.

honeypots, generally imitates a specific type of IoT device to further scrutinization of attack vectors in a particular environment. The IoT honeypot, namely HIoTPOT [182], finds that most of the attackers are interested in finding vulnerable devices, as per the analysis of per-day traffic.

One of such honeypots, IoTPOT [183], mimics Telnet services of several IoT devices to investigate the current attacks profoundly. The authors observed that the Telnet-based attacks are carried out in three phases: intrusion, contamination, and monetization. In the first phase, numerous login attempts are made by an attacker with combinations of credentials. Following this in the next phases, malware is downloaded in the device which is spread across the network to launch a DDoS attack. The authors also tracked the several malware binary files downloaded and proposed IoTBOX, for analyzing captured malware binaries. Another honeypot, HosTaGe, is designed by Vasilomanolakis *et al.* Authors of [184] target malicious activities against several protocols like Telnet, HTTP, SSH, FTP, MySQL, and SIP in ICS networks. HosTaGe also generates the attack signatures, which can be integrated into ICS for further detection and mitigation of attacks. On similar lines, the authors proposed a honeypot, Cryplh [185], to find the attacks against the PLC-based ICS.

Litchfield *et al.* [186] designed a HoneyPhy honeypot, hybrid-interaction based CPS framework, which can imitate the behavior of both IoT devices and CPS processes. The proposed honeypot comprises of three modules. A module to maintain connections and traffic, the process module to imitate the systems' dynamics, and device models to mimic CPS devices. Similarly, Guarnizo *et al.* [187] proposed the IoT-based honeypot framework, SIPHON, which attracts malicious traffic on the internet through wormholes and vulnerable IoT devices. The authors concluded with insightful inferences regarding malicious traffic, ports, target location, and user agents. Additionally, honeypots [188]

were designed to analyze attacks against a ZigBee gateway. In [189], the authors reported most of the attacks against the Zigbee-based IoT devices were the dictionary attacks.

e) *Penetration Testing and Network Discovery Tools:* Visoottiviseth *et al.* [190] developed a penetration testing tool PENTOS for IoT devices. It compiles various penetration tools like Metasploit, Kali, Nessus, Burpsuit, Cain & Abel, etc., to find the vulnerabilities. It also guides the users against OWASP's IoT vulnerabilities. There are many features in PENTOS, which aids in gathering information, scanning the web, Bluetooth analysis, and reporting. The authors paving in this way as Chen *et al.* [191] suggested the path of intelligence and modularization for penetration testing tools to discover vulnerabilities by employing offensive attacks against IoT systems. The authors carried out PT in three modules. The interface testing checks the interfaces through which multiple devices or users interact with. The transportation testing targets weak cryptographic schemes, misuse issues, and flaws in communication protocols. The system testing focuses on firmware, OS, insecure system settings, etc.

To scan the whole IoT space, Markowsky *et al.* [192] three scans: Shodan to target the Cayman DSL Routers, Masscan to target the devices affected with Heart bleed bug, and last they used Nmap with PFT to target vulnerable connected printers. The authors [193] also proposed a management platform where, after the vulnerability assessment, the information about the same is shared with the users. They start with collecting the device information and then comparing it with vulnerability information from the National Vulnerability Database. The information is collected through IP Scan, Handshake Scan, and finally, OS Fingerprinting. For sharing the information about vulnerabilities Structured Threat Information Expression standard is used.

We have seen that new vulnerabilities and attacks are evolving every day [194]. It is found that there are a few vulnerability assessment solutions based on Machine Learning. Recently Dojo by Bullguard introduced BullGuard launches intelligent IoT vulnerability scanner [195]. The dojo is available for both android and ios. It scans all the IoT nodes in the wi-fi network, analyzes the vulnerabilities and scores them according to the risks they are undergoing. This is the first machine learning-based tool. There are some other tools, for instance, Bitdefender, IotSploit, IoTScanner, Shodan [196] Censys, SeeSec –IoT Vulnerability Scanner that serve the same purpose.

V. CASE STUDY: SMART AGRICULTURE

In order to highlight the need of sustainability in Smart agriculture, we consider a case study on ''Sustainable Smart Agriculture''. The contextual analysis of the same is covered.

A. SUSTAINABLE SMART AGRICULTURE

The advanced technologies like IoT, robotics, cloud computing, artificial intelligence, unmanned aerial vehicle, and machine learning have replaced the conventional methods of farming with modern methods to maintain the supply-demand ratio. The proposed use case (Sustainable Smart Agriculture) sustainable framework is shown in FIGURE 13. The way it works could be well-understood in context to layers. The physical layer generally covers the field with several underground and above the surface sensors, drones, tractors, pesticides, and fertilizer controllers. The on-field devices communicate with each other and the local control center at the edge layer through gateways. These devices gather real-time information regarding soil, weather, livestock, energy management, and irrigation. From the edge layer, the information collected by sensors is sent to the cloud for further analysis. The useful insights inferred are sent back to the user/owner for further actions. The edge nodes provide various services like real-time monitoring, security mechanisms, energy harvesting, and prediction at the edge layer [197]. For example, ML-based models classify the events related to plants or livestock, predict the crop yield, fertilizer needed, and schedule the irrigation based on water needed by the crops. And the network layer facilitates communication among all the layers [198].

The smart services with advanced technologies provide manifold benefits to the agriculture industry but expose the risk of vulnerabilities and cyber-attacks too. For example, the surveillance drones in the field capture images of the crops, and with computer vision, the disease-prone area of the field is found. The identified affected area is then isolated and removed to further prevent the entire field from the disease. This sector being unaware about the cyber-security is more prone to cyber-threats. The intruder can remotely take control of on-field sensors, access irrigation management system, and maliciously manipulate the data in transit. With such attempts, they can destroy the field of grown crops, control the drones to damage the crops through pesticides or over fertilizers, and create an unproductive agricultural environment. Thus, less productivity even deteriorates the economy of a country [199]. The cyber-attacks targeting smart agriculture when launched in a well-coordinated manner on a large scale called agro-terrorism [200]. The data and malware injection attacks are the most prevalent attacks in smart farming. In a data injection attack, an intruder maliciously modifies the data contributing to real-time decision making and thus leads to false decisions. In malware injection attack, an adversary infects the smart device by injecting a malware, that has self-propagating like features. Consequently, malware is most likely to infect all other smart farms having similar deployments. It can turn the devices into bots, steal information, and hamper the functioning of smart machines in the field [14].

A feasible solution to overcome the aforementioned sustainability issues is the incorporation of energy harvesting techniques and vulnerability assessment in smart agriculture.

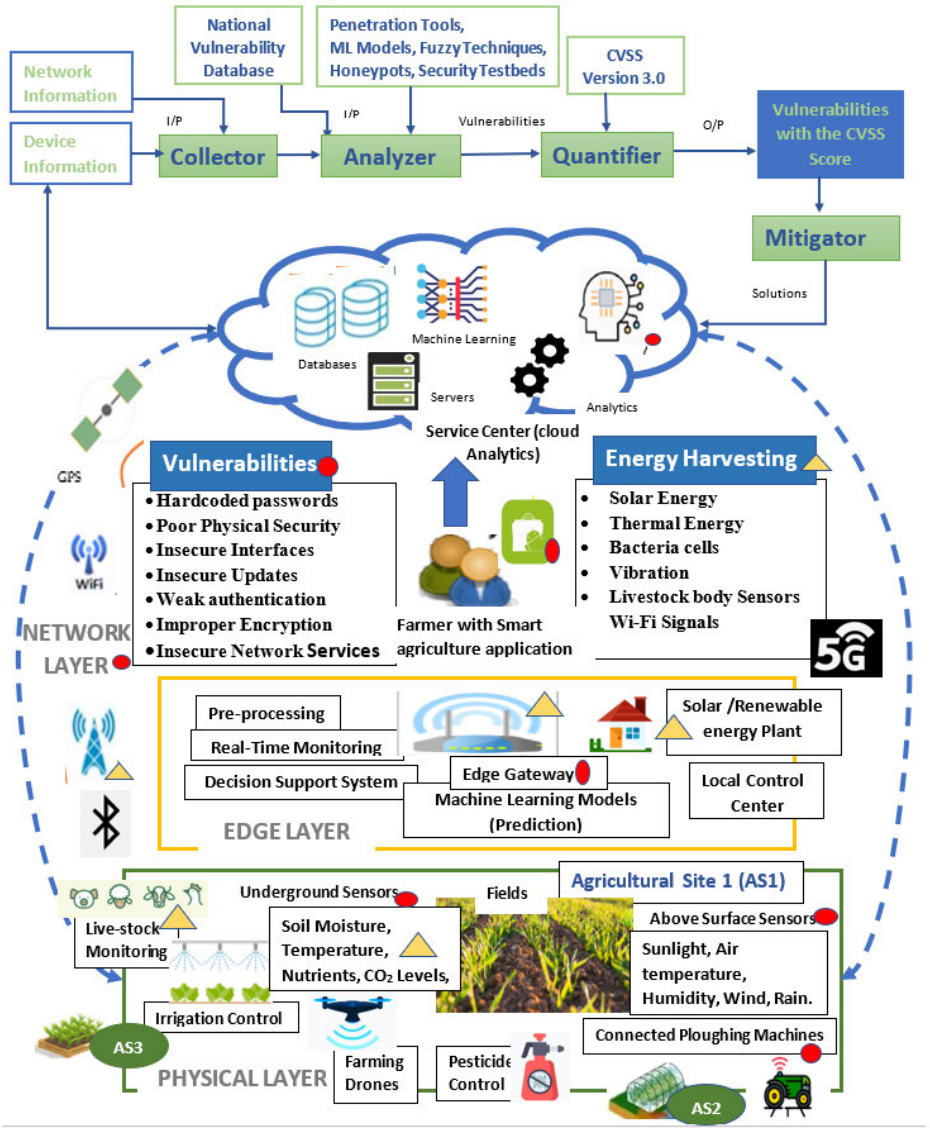

FIGURE 13. Sustainable IoT framework for sustainable smart agriculture.

The vulnerability assessment module added to the Smart Agriculture has four components namely collector, analyzer, quantifier, and mitigator. The collector collects all the information related to the device and network. The analyzer takes the collected information as input and compares the same with NVD. The multiple vulnerability assessment techniques like machine learning, network discovery tools, penetration testing tools, testbeds, machine learning models, and honeypots can also be a part of this component. The quantifier quantifies the vulnerabilities assessed by analyzer using CVSSv3 as per the risk they impose on the IoT system. The mitigator gets the vulnerabilities with their CVSS score as input and provides solutions to overcome those loopholes. It also notifies about the vulnerabilities and their remediations to the manufacturers and IoT users. The timely mitigation of the known vulnerabilities reduce the risk of the IoT system as prey to potential adversaries.

For the sustainable functioning of IoT nodes in smart farms, both the underground and above the surface sensors need the continuous power supply for sensing and communication. The ideal lifetime of sensors in an agricultural field is found to be more than 5 years. Though the power requirements have been reduced in the sensors, with the recent advancements in technology and sensor materials. But, they need continuous powering to enable communication between the underground radios and above-ground receivers. There are many EH sources like underground living plants, vibration, thermal, solar, and bacteria by way of fuel cells to harvest the energy from the surrounding sources in the field. The other way to power these energy-constrained sensors is through wireless power transfer, which can transfer both

the data and power in a full-duplex mode. For example, the above the surface nodes transfers the harvested solar energy to the underground nodes, and the other way could be the underground nodes transfers the harvested energy from bacteria and vibration to above the surface nodes. Thus, this bi-directional power transfer results in longer battery life for sustainable smart farming [201]. However, the research community needs to work on wireless RF-based underground power transfer for sustainable IoT. Additionally, the factors like maintenance, battery replacement, repair, and underground re-installation must also be worked upon. The development of smart farm technologies, therefore demands further research before wide adoption in the community. Integrating both the components in smart agriculture has several benefits:

- Reduce the risk of attacks and make the system more secure with a prior vulnerability assessment.
- Improve the lifetime of power-constrained sensor nodes with EH schemes integrated at the design phase.
- Prevents the privacy of data at storage and in transit with light-weight cryptographic schemes.
- Protect the system from misleading data injection attacks.
- Reduces the smart nodes from being compromised.
- Aware the developers with the vulnerabilities in the shipped devices.

VI. OPEN ISSUES AND RESEARCH CHALLENGES

So far, we summarized the several IoT attacks launched by exploiting common vulnerabilities in an IoT system, along with few vulnerability assessment mechanisms and ML-based solutions to secure IoT systems. Further, we discuss the emerging challenges for sustainable IoT as shown in FIGURE 14 and pinpoint some initiatives for future work, to be pursued in this vital field of IoT sustenance.

A. LACK OF SCALABLE VULNERABILITY ASSESSMENT WAY OUT IN IoT SYSTEM

The key technologies in IoT, for instance, RFID [49], WSN are themselves vulnerable to threats like node compromise, eavesdropping, tracking of devices, malware, etc. Moreover, numerous attacks are exploiting the unanticipated vulnerabilities in IoT systems. Although there are several vulnerability assessments, they are not mature enough to deal with the heterogeneous network of IoT devices. There must be an automated vulnerability assessment framework to handle device scalability and variability in various deployment contexts. Alongside, there must be the mechanism to find the unexploited vulnerable device.

Future Initiative: Transfer learning algorithms context [202] could be a potential solution at this end. Feeding the TL algorithms with IoT vulnerabilities could enhance and automate the job of vulnerability assessment so as to infer this knowledge from numerous IoT devices. Furthermore, investigating IoT-specific trust models [203] in several contexts would aid the growth of requisite IoT remediation strategies after assessing the vulnerabilities.

B. UNEXPECTED USAGE OF IoT DATA

The IoT has enabled the ubiquitous computing, and thus deployment of IoT enabled sensors in our lives have been noticeably pervasive. These sensors collect a huge amount of data from its surroundings and transmit it to the cloud for further processing. The value of the IoT system lies in that data [204]. Although, the privacy of the collected data is of main concern, static as well as in transit. For instance, IoT based baby monitors and IoT toys were easy to play with by hackers to get sensitive information like video streaming of baby monitors [17], voice recordings of parents, and their kids(in millions), emails, passwords, etc. Recently, it is unveiled that a lot of privacy-sensitive information could be revealed from varied types of related data (user/environment) gathered by smart sensors. Thus potential adversaries could make useful insights from the collected data in an unexpected manner. For instance, privacy-sensitive information like daily routines, the number of persons in a home can be deduced by analyzing smart homes' power usage data collected using smart meters [205]. Some serious consequences that result by providing 3rd party applications access to sensors are discussed in [206]. Despite such previous attempts, the amount of sensitive information that might be deduced from probably shallow data is not well-known or well-understood yet.

Future Initiative: The privacy-friendly techniques must be incorporated into Smart Meter Architecture for making insights out of the sensitive collected data. The authors [205] suggested pertinent data selection or processing methods to minimize or avoid sensitive personal data within industrial applications.

C. LACK OF CAPABILITIES TO AWARE IoT USERS ABOUT SECURITY GUIDELINES

Further, there is a need to explore the ways to improve users' awareness about the serious consequences of numerous IoT threats. A noticeable example is a DDoS attack using Mirai malware launched in October 2016, targeted against the service provider, Dyn and shut down the hundreds of websites for several hours- Netflix, Twitter, GitHub, Reddit. Mirai launched the DDoS attack against target servers by building a network of weakly configured IoT nodes, namely botnet [207]. While the code of Mirai malware was accessible months ago, and despite some vendor's reaction, most of the end-users did not bother to update their IoT devices with security patches, thus permitting them to be part of many upcoming botnets [208]. Note that although the vendors produce the security patches, the updates need not reach the requisite destination. Even today, the same vulnerabilities of IoT devices are exploited by Mirai and its variants [14], resulting in severe consequences like full device control.

Future Initiative: There must be some mechanism to constrain the users to modify their default credentials

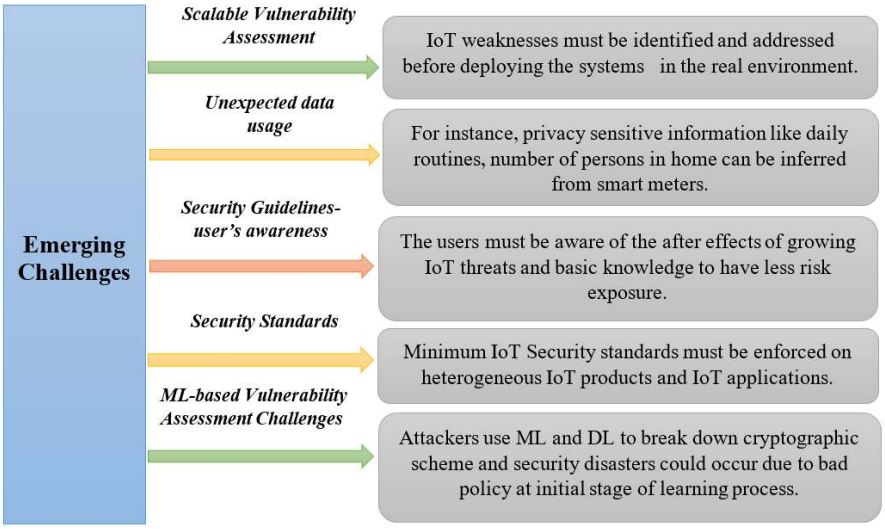

FIGURE 14. Research trends and open issues.

and automate the process of frequent firmware updates. Additionally, there must be some limit on the time gap from the moment the vulnerability discovered in producing patches and then deploying to the IoT attack victims for sustainable IoT.

D. LACK OF ENFORCEMENT OF MINIMUM IoT SECURITY STANDARDS

The need for standardization processes for different IoT products and various IoT applications question the security, interoperability, scalability, and compatibility in the IoT realm. The manufacturers supply IoT products without considering baseline IoT security standards [39], [209]. They mainly focus on their functionality, low cost, and low energy consumption. Whereas, the current status of IoT threats and growing attacks, emphasizes the incorporation of various security schemes in IoT devices. These schemes include hardware security against tampering, indispensable user authentication, data encryption at rest and transit, and OS/firmware/application security and integrity. However, the resource constraint nature of IoT devices like sensors, baby monitors, CCTV cameras, and the computation and memory overhead of traditional security schemes, conveys the necessity of lightweight security solutions for IoT devices [210].

Future Initiative: There must be an international body for enforcing minimum security standards in heterogeneous IoT products and IoT applications. Additionally, it is recommended to have transparency, communication, and collaboration among evolving IoT security standards-making bodies like IoTSF, Industrial Internet Consortium, NIST, and International Society of Automation [50].

E. ML-BASED VULNERABILITY ASSESSMENT CHALLENGES

Machine learning has shown its significance for both, one way it extracts the value from the data, and the other way used by the adversaries for malicious purposes. The features of these learning algorithms are being misused by potential adversaries to breakdown the cryptographic schemes. For instance, previous studies [211], [212] used SVM to collapse the cryptographic systems. Another study [213] concluded that RNNs could do cryptanalysis by capturing and learning the algorithmic demonstration of polyalphabetic ciphers. Additionally, researches have shown that feeding false data can compromise the training models and hence, failing the entire system. For example, if deep learning-based model for controlling the self-driving vehicles is injected with false data, the malicious user can potentially control the vehicle [54]. Moreover, there is the risk of adopting poor defense policies during the initial stage of the learning process, which can lead to security disasters in learning-based IoT security system. Additionally, supervised and unsupervised learning now and then fail to identify the malicious activities because of oversampling, not enough training data, and poor feature extraction. Hence, the ML techniques need to be integrated with back-up security mechanisms. Moreover, several existing ML techniques have exhaustive overheads, so new security schemes such as dFW must be explored for building secure IoT systems, particularly for the situations when there exists no cloud or edge computing.

Future Initiative: Applying transfer learning [214] to actual defense experiences reduces accidental exploration, increases the learning rate, and reduces the chances of having poor defense policies in the initial stage of learning. Also, ensemble ML techniques [47] prove to be more fruitful in overcoming loopholes of basic learning schemes.

VII. CONCLUSION

IoT has evolved with immense growth in participating entities, i.e., sensors, communication, and computation. IoT is in its way to transform all the major aspects of our lives from homes to health, to agriculture, to automation, to cities, to transportation, to grids and manufacturing.

This revolutionary expansion will be useless if IoT is not able to sustain in the present situation, with a void in energy-efficiency and security in the present ecosystem design. In this article, we have provided insights to the readers about the Sustainable IoT, embedded vulnerabilities in IoT devices, and vulnerability assessment techniques to assess those vulnerabilities before getting exploited. This article is divided into four parts. The first part discussed the general concepts related to IoT. In this, we begin with the background of IoT and explored many significant events related to its growth since this term emanated. We discussed the factors for the sustainability of IoT, the protocol suite, and testbeds. The second part discussed the IoT security vulnerabilities such as open ports, poor update mechanisms, and weak authentication practices serving as entry points for attackers causing malicious abuse. Then, we explore the contribution of machine learning, security testbeds, honeypots, and network discovery tools in assessing vulnerabilities in an IoT environment. We have also presented the case study on sustainable smart agriculture. Then, we listed the open issues and future initiatives for sustainable IoT. Finally, we summarize that this article provides useful insights to the research community by presenting the present-day status of such a vibrant area of research.

In future, hybrid ML techniques and deep learning will be explored in detail for Vulnerability Assessment in IoT. The attacks on EH chips and their consequences will also be studied. We will also try to cover the frameworks for quantifying the vulnerabilities in IoT and its real-time implementation in multiple scenarios.

REFERENCES

[1] B. B. Gupta and M. Quamara, "An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols," *Concurrency Comput., Pract. Exper.*, p. e4946, Sep. 2018, doi: 10.1002/cpe.4946.

[2] L. A. Amaral, F. P. Hessel, E. A. Bezerra, J. C. Corrêa, O. B. Longhi, and T. F. O. Dias, "ECloudRFID—A mobile software framework architecture for pervasive RFID-based applications," *J. Netw. Comput. Appl.*, vol. 34, no. 3, pp. 972–979, May 2011.

[3] *IEEE Internet Technology Policy Community White Paper Internet of Things (IoT) Security*. Accessed: 2020. [Online]. Available: https://www.academia.edu/32053241/Internet_Of_Things_Iot_Security_Best_Practices._IEEE_Community-led_White_Paper

[4] J. Vora, S. Tanwar, S. Tyagi, N. Kumar, and J. J. P. C. Rodrigues, "Home-based exercise system for patients using IoT enabled smart speaker," in *Proc. IEEE 19th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, Oct. 2017, pp. 1–6.

[5] M. C. Domingo, "An overview of the Internet of Things for people with disabilities," *J. Netw. Comput. Appl.*, vol. 35, no. 2, pp. 584–596, Mar. 2012.

[6] I. Bisio, A. Delfino, F. Lavagetto, and A. Sciarrone, "Enabling IoT for in-home rehabilitation: Accelerometer signals classification methods for activity and movement recognition," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 135–146, Feb. 2017.

[7] *Autism Glass Project*. Accessed: 2020. [Online]. Available: https://wall-lab.stanford.edu/projects/autism-therapy-on-glass/

[8] *Feasibility Testing of a Wearable Behavioral Aid for Social Learning in Children With Autism*. Accessed: 2020. [Online]. Available: https://www.thieme-connect.com/products/ejournals/pdf/10.1055/s-0038-1626727.pdf

[9] *Internet of Things Applications Part 2: The Mining Industry | Centric Digital*. Accessed: 2020. [Online]. Available: https://centricdigital.com/blog/digital-trends/internet-of-things-applications-pt2-the-mining-industry/

[10] 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. Surveys Tuts.*, vol. 21, no. 3, pp. 2702–2733, 3rd Quart., 2019.

[11] *Smart Cities–International Case Studies–The Living Library*. Accessed: 2020. [Online]. Available: https://thelivinglib.org/smart-cities-international-case-studies/

[12] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to the Internet of Things," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1636–1675, 2nd Quart., 2019.

[13] *The CEO's Guide to Data Security: Protect Your Data Through Innovation*. Accessed: 2020. [Online]. Available: https://www.business.att.com/content/dam/attbusiness/reports/vol5-datasecurity.pdf

[14] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[15] S. Tanwar, S. Tyagi, and S. Kumar, "The role of Internet of Things and smart grid for the development of a smart city," in *Intelligent Communication and Computational Technologies*. Y.-C. Hu, S. Tiwari, K. K. Mishra, and M. C. Trivedi, Eds. Singapore: Springer, 2018, pp. 23–33.

[16] *IoT Connected Teddy Bear Leaks Millions of Kids' Conversations, Exposed Database to Blame—Techrepublic*. Accessed: 2020. [Online]. Available: https://www.techrepublic.com/article/iot-connected-teddy-bear-leaks-millions-of-kids-conversations-exposed-database-to-blame/

[17] *Hacking IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities*. Accessed: 2020. [Online]. Available: https://www.rapid7.com/globalassets/external/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf

[18] E. Bertino and N. Islam, "Botnets and Internet of Things security," *Computer*, vol. 50, no. 2, pp. 76–79, Feb. 2017.

[19] *Battery Performance Alert and Cybersecurity Firmware Updates for Certain Abbott (Formerly St. Jude Medical) Implantable Cardiac Devices: FDA Safety Communication | FDA*. Accessed: 2020. [Online]. Available: https://www.fda.gov/medical-devices/safety-communications/battery-performance-alert-and-cybersecurity-firmware-updates-certain-abbott-formerly-st-jude-medical

[20] F. Assaderaghi, G. Chindalore, B. Ibrahim, H. de Jong, M. Joye, S. Nassar, W. Steinbauer, M. Wagner, and T. Wille, "Privacy and security: Key requirements for sustainable IoT growth," in *Proc. Symp. VLSI Technol.*, Jun. 2017, pp. T8–T13.

[21] R. Gupta, S. Tanwar, N. Kumar, and S. Tyagi, "Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review," *Comput. Electr. Eng.*, vol. 86, Sep. 2020, Art. no. 106717.

[22] O. L. A. López, H. Alves, R. D. Souza, S. Montejo-Sánchez, E. M. G. Fernández, and M. Latva-Aho, "Massive wireless energy transfer: Enabling sustainable IoT towards 6G era," *IEEE Commun. Mag.*, pp. 1–7, 2019.

[23] A. Kumari, R. Gupta, S. Tanwar, and N. Kumar, "Blockchain and AI amalgamation for energy cloud management: Challenges, solutions, and future directions," *J. Parallel Distrib. Comput.*, vol. 143, pp. 148–166, Sep. 2020.

[24] L. Guo, Z. Chen, D. Zhang, J. Liu, and J. Pan, "Sustainability in body sensor networks with transmission scheduling and energy harvesting," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9633–9644, Dec. 2019.

[25] S. Khairy, M. Han, L. X. Cai, and Y. Cheng, "Sustainable wireless IoT networks with RF energy charging over Wi-Fi (CoWiFi)," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10205–10218, Dec. 2019.

[26] U. Banerjee, C. Juvekar, S. H. Fuller, and A. P. Chandrakasan, "EeDTLS: Energy-efficient datagram transport layer security for the Internet of Things," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2017, pp. 1–6.

[27] S. K. Ram, S. R. Sahoo, B. B. Das, K. Mahapatra, and S. Mohanty, "Eternal-thing: A secure aging-aware solar-energy harvester thing for sustainable IoT," *IEEE Trans. Sustain. Comput.*, early access, Apr. 15, 2020, doi: 10.1109/TSUSC.2020.2987616.

[28] S. Sen, J. Koo, and S. Bagchi, "TRIFECTA: Security, energy efficiency, and communication capacity comparison for wireless IoT devices," *IEEE Internet Comput.*, vol. 22, no. 1, pp. 74–81, Jan. 2018.

[29] M. Shirvanimoghaddam, K. Shirvanimoghaddam, M. M. Abolhasani, M. Farhangi, V. Z. Barsari, H. Liu, M. Dohler, and M. Naebe, "Towards a green and self-powered Internet of Things using piezoelectric energy harvesting," *IEEE Access*, vol. 7, pp. 94533–94556, 2019.

[30] H. Liao, Z. Zhou, B. Ai, and M. Guizani, "Learning-based energy-efficient channel selection for edge computing-empowered cognitive Machine-to-Machine communications," in *Proc. IEEE 91st Veh. Technol. Conf. (VTC-Spring)*, May 2020, pp. 1–6.

[31] X. Huang, R. Yu, J. Kang, Z. Xia, and Y. Zhang, "Software defined networking for energy harvesting Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1389–1399, Jun. 2018.

[32] X. Liu, A. Liu, T. Wang, K. Ota, M. Dong, Y. Liu, and Z. Cai, "Adaptive data and verified message disjoint security routing for gathering big data in energy harvesting networks," *J. Parallel Distrib. Comput.*, vol. 135, pp. 140–155, Jan. 2020.

[33] Z. Zhou, L. Tan, and G. Xu, "Blockchain and edge computing based vehicle-to-grid energy trading in energy Internet," in *Proc. 2nd IEEE Conf. Energy Internet Energy Syst. Integr. (EI2)*, Oct. 2018, pp. 1–5.

[34] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[35] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015.

[36] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.

[37] M. G. Samaila, M. Neto, D. A. B. Fernandes, M. M. Freire, and P. R. M. Inácio, "Challenges of securing Internet of Things devices: A survey," *Secur. Privacy*, vol. 1, no. 2, p. e20, Mar. 2018.

[38] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, Jul. 2013.

[39] N. Zhang, S. Demetriou, X. Mi, W. Diao, K. Yuan, P. Zong, F. Qian, X. Wang, K. Chen, Y. Tian, C. A. Gunter, K. Zhang, P. Tague, and Y.-H. Lin, "Understanding IoT security through the data crystal ball: Where we are now and where we are going to be," *Cryptogr. Secur., Comput. Sci.*, pp. 1–19, 2017, doi: abs/1703.09809.

[40] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, Jun. 2017.

[41] A. Mosenia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 4, pp. 586–602, Oct. 2017.

[42] *The Internet of Things Reference Model*. Accessed: 2020. [Online]. Available: https://http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf

[43] M. Mahbub, "Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics," *J. Netw. Comput. Appl.*, vol. 168, Oct. 2020, Art. no. 102761.

[44] A. Srivastava, S. Gupta, M. Quamara, P. Chaudhary, and V. J. Aski, "Future IoT-enabled threats and vulnerabilities: State of the art, challenges, and future prospects," *Int. J. Commun. Syst.*, vol. 33, no. 12, p. e4443, Aug. 2020.

[45] R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "Machine learning models for secure data analytics: A taxonomy and threat model," *Comput. Commun.*, vol. 153, pp. 406–440, Mar. 2020.

[46] K. Sheth, K. Patel, H. Shah, S. Tanwar, R. Gupta, and N. Kumar, "A taxonomy of AI techniques for 6G communication networks," *Comput. Commun.*, vol. 161, pp. 279–303, Sep. 2020.

[47] M. Moh and R. Raju, "Using machine learning for protecting the security and privacy of Internet of Things (IoT) systems," *Fog Edge Comput., Princ. Paradigms*, vol. 30, pp. 223–257, 2019.

[48] S. Challa, A. K. Das, V. Odelu, N. Kumar, S. Kumari, M. K. Khan, and A. V. Vasilakos, "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Comput. Electr. Eng.*, vol. 69, pp. 534–554, Jul. 2018.

[49] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2481–2501, Nov. 2014.

[50] M. Ahlmeyer and A. M. Chircu, "Securing the Internet of Things: A review," *Issues Inf. Syst.*, vol. 17, no. 4, pp. 21–28, 2016.

[51] A. Oracevic, S. Dilek, and S. Ozdemir, "Security in Internet of Things: A survey," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, 2017, pp. 1–6.

[52] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, Aug. 2018.

[53] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?" *IEEE Signal Process. Mag.*, vol. 35, no. 5, pp. 41–49, Sep. 2018.

[54] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1686–1721, 3rd Quart., 2020.

[55] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 616–644, 1st Quart., 2020.

[56] S. Li, L. Xu, and S. Zhao, "The Internet of Things: A survey," *Inf. Syst. Frontiers*, vol. 17, no. 2, pp. 243–259, 2015.

[57] S. Tanwar, J. Vora, S. Tyagi, N. Kumar, and M. S. Obaidat, "A systematic review on security issues in vehicular ad hoc network," *Secur. Privacy*, vol. 1, no. 5, p. e39, Sep. 2018.

[58] M. R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco, G. Boggia, and M. Dohler, "Standardized protocol stack for the Internet of (important) Things," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1389–1406, 3rd Quart., 2013.

[59] R. Gupta, S. Tanwar, F. Al-Turjman, P. Italiya, A. Nauman, and S. W. Kim, "Smart contract privacy protection using AI in cyber-physical systems: Tools, techniques and challenges," *IEEE Access*, vol. 8, pp. 24746–24772, 2020.

[60] X. Liu, K. Ravichandran, and E. Sánchez-Sinencio, "A switched capacitor energy harvester based on a single-cycle criterion for MPPT to eliminate storage capacitor," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 65, no. 2, pp. 793–803, Feb. 2018.

[61] H. Shao, C.-Y. Tsui, and W.-H. Ki, "The design of a micro power management system for applications using photovoltaic cells with the maximum output power control," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 17, no. 8, pp. 1138–1142, Aug. 2009.

[62] Y.-C. Shih and B. P. Otis, "An inductorless DC–DC converter for energy harvesting with a 1.2-μW bandgap-referenced output controller," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 58, no. 12, pp. 832–836, Dec. 2011.

[63] B. P. Baddipadiga and M. Ferdowsi, "A high-voltage-gain DC-DC converter based on modified dickson charge pump voltage multiplier," *IEEE Trans. Power Electron.*, vol. 32, no. 10, pp. 7707–7715, Oct. 2017.

[64] B. Ji, B. Xing, K. Song, C. Li, H. Wen, and L. Yang, "The efficient BackFi transmission design in ambient backscatter communication systems for IoT," *IEEE Access*, vol. 7, pp. 31397–31408, 2019.

[65] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and B. Sadoun, "HaBiTs: Blockchain-based telesurgery framework for healthcare 4.0," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Aug. 2019, pp. 1–5.

[66] J. Hathaliya, P. Sharma, S. Tanwar, and R. Gupta, "Blockchain-based remote patient monitoring in healthcare 4.0," in *Proc. IEEE 9th Int. Conf. Adv. Comput. (IACC)*, Dec. 2019, pp. 87–91.

[67] M. Hypponen and L. Nyman, "The Internet of (vulnerable) Things: On Hypponen's law, security engineering, and IoT legislation," *Technol. Innov. Manage. Rev.*, vol. 7, no. 4, pp. 5–11, Apr. 2017.

[68] *IEEE Internet Technology Policy Community White Paper Internet of Things (IoT) Security*. Accessed: 2020. [Online]. Available: https://www.academia.edu/32053241/Internet_Of_Things_Iot_Security_Best_Practices._IEEE_Community-led_White_Paper

[69] *The CEO's Guide to Data Security: Protect Your Data Through Innovation*. Accessed: 2020. [Online]. Available: https://www.business.att.com/content/dam/attbusiness/reports/vol5-datasecurity.pdf

[70] J. Y. Keller and D. Sauter, "Monitoring of stealthy attack in networked control systems," in *Proc. Conf. Control Fault-Tolerant Syst. (SysTol)*, Oct. 2013, pp. 462–467.

[71] *German Steel Mill Cyber Attack*. Accessed: 2020. [Online]. Available: https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

[72] S. Dhanda, B. Singh, and P. Jindal, "Lightweight cryptography: A solution to secure IoT," *Wireless Pers. Commun.*, vol. 112, pp. 1947–1980, Jan. 2020.

[73] Á. L. V. Caraguay, A. B. Peral, L. I. B. López, and L. J. G. Villalba, "SDN: Evolution and opportunities in the development IoT applications," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 5, May 2014, Art. no. 735142.

[74] A. Gaur, B. Scotney, G. Parr, and S. McClean, "Smart city architecture and its applications based on IoT," *Procedia Comput. Sci.*, vol. 52, pp. 1089–1094, Jan. 2015.

[75] S. R. Moosavi, T. N. Gia, A.-M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, and H. Tenhunen, "SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways," *Procedia Comput. Sci.*, vol. 52, pp. 452–459, Jan. 2015.
[76] R. T. Tiburski, L. A. Amaral, E. De Matos, and F. Hessel, "The importance of a standard securit y archit ecture for SOA-based iot middleware," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 20–26, Dec. 2015.
[77] M. Vucinic, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, "OSCAR: Object security architecture for the Internet of Things," *Ad Hoc Netw.*, vol. 32, pp. 3–16, Sep. 2015.
[78] Y. Jararweh, M. Al-Ayyoub, A. Darabseh, E. Benkhelifa, M. Vouk, and A. Rindos, "SDIoT: A software defined based Internet of Things framework," *J. Ambient Intell. Hum. Comput.*, vol. 6, no. 4, pp. 453–461, Jun. 2015.
[79] S. Chakrabarty and D. W. Engels, "A secure IoT architecture for smart cities," in *Proc. 13th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2016, pp. 812–813.
[80] A. Dawoud, S. Shahristani, and C. Raun, "Deep learning and software-defined networks: Towards secure IoT architecture," *Internet Things*, vols. 3–4, pp. 82–89, Oct. 2018.
[81] N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "A multi-tenant cloud-based DC nano grid for self-sustained smart buildings in smart cities," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 14–21, Mar. 2017.
[82] R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "Tactile Internet and its applications in 5G era: A comprehensive review," *Int. J. Commun. Syst.*, vol. 32, no. 14, p. e3981, Sep. 2019.
[83] S. Doss, A. Nayyar, G. Suseendran, S. Tanwar, A. Khanna, L. H. Son, and P. H. Thong, "APD-JFAD: Accurate prevention and detection of jelly fish attack in MANET," *IEEE Access*, vol. 6, pp. 56954–56965, 2018.
[84] A. N. Kim, F. Hekland, S. Petersen, and P. Doyle, "When HART goes wireless: Understanding and implementing the WirelessHART standard," in *Proc. IEEE Int. Conf. Emerg. Technol. Factory Autom.*, Sep. 2008, pp. 899–907.
[85] Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. Mccann, and K. Leung, "A survey on the IETF protocol suite for the Internet of Things: Standards, challenges, and opportunities," *IEEE Wireless Commun.*, vol. 20, no. 6, pp. 91–98, Dec. 2013.
[86] S. Kandula, D. Katabi, S. Sinha, and A. Berger, "Dynamic load balancing without packet reordering," *SIGCOMM Comput. Commun. Rev.*, vol. 37, p. 51–62, Mar. 2007.
[87] C. M. Vigorito, D. Ganesan, and A. G. Barto, "Adaptive control of duty cycling in energy-harvesting wireless sensor networks," in *Proc. 4th Annu. IEEE Commun. Soc. Conf. Sensor, Mesh Ad Hoc Commun. Netw.*, Jun. 2007, pp. 21–30.
[88] C. Bormann, A. P. Castellani, and Z. Shelby, "CoAP: An application protocol for billions of tiny Internet nodes," *IEEE Internet Comput.*, vol. 16, no. 2, pp. 62–67, Mar. 2012.
[89] *Arduino—Home*. Accessed: 2020. [Online]. Available: https://www.arduino.cc/
[90] *Projects | IoT Development Made Simple—IoT.eclipse.org*. Accessed: 2020. [Online]. Available: https://iot.eclipse.org/projects/
[91] *Beagleboard.org—Community Supported Open Hardware Computers for Making*. Accessed: 2020. [Online]. Available: http://beagleboard.org/
[92] *Devicehive—Open Source IoT Data Platform With the Wide Range of Integration Options*. Accessed: 2020. [Online]. Available: https://devicehive.com/
[93] *Eclipse Smarthome—A Flexible Framework for the Smart Home*. Accessed: 2020. [Online]. Available: https://www.eclipse.org/smarthome/
[94] A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, R. M. Parizi, and K.-K.-R. Choo, "Fog data analytics: A taxonomy and process model," *J. Netw. Comput. Appl.*, vol. 128, pp. 90–104, Feb. 2019.
[95] J. Vora, S. Kaneriya, S. Tanwar, S. Tyagi, N. Kumar, and M. S. Obaidat, "TILAA: Tactile Internet-based ambient assistant living in fog environment," *Future Gener. Comput. Syst.*, vol. 98, pp. 635–649, Sep. 2019.
[96] *Crawdad*. Accessed: 2020. [Online]. Available: https://crawdad.org/
[97] *Linked Sensor Data (kno.e.sis)—Datasets—The Datahub*. Accessed: 2020. [Online]. Available: https://old.datahub.io/dataset/knoesis-linked-sensor-data
[98] *National Land Numerical Information*. Accessed: 2020. [Online]. Available: http://nlftp.mlit.go.jp/ksj-e/index.html
[99] *Internet of People, Things and Computers–Network Protocols and Technologies Lab–NPTLAB*. Accessed: 2020. [Online]. Available: http://nptlab.di.unimi.it/
[100] *UCI Machine Learning Repository*. Accessed: 2020. [Online]. Available: https://archive.ics.uci.edu/ml/index.php
[101] *Intel Lab Data*. Accessed: 2020. [Online]. Available: http://db.csail.mit.edu/labdata/labdata.html
[102] *Professional IoT Solutions—IOMOTE*. Accessed: 2020. [Online]. Available: https://www.iomote.com/
[103] N. Kumar, M. Kumar, and R. B. Patel, "Capacity and interference aware link scheduling with channel assignment in wireless mesh networks," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 30–38, Jan. 2011.
[104] *NB-IoT Wireless Sensors—IOMOTE*. Accessed: 2020. [Online]. Available: https://www.iomote.com/xsense/
[105] *Arduino—Arduinoethernetshield*. Accessed: 2020. [Online]. Available: https://www.arduino.cc/en/Guide/ArduinoEthernetShield
[106] *OpenIoT–Open Source Cloud Solution for the Internet of Things*. Accessed: 2020. [Online]. Available: http://www.openiot.eu/
[107] S. Tanwar, "Verification and validation techniques for streaming big data analytics in Internet of Things environment," *IET Netw.*, vol. 8, no. 2, pp. 92–100, Nov. 2018.
[108] *Contiki: The Open Source Operating System for the Internet of Things*. Accessed: 2020. [Online]. Available: http://www.contiki-os.org/
[109] *Contiki OS: The Open Source OS for IoT—IoTBYHVM—Bits & Bytes of IoT*. Accessed: 2020. [Online]. Available: https://iotbyhvm.ooo/contiki-the-open-source-os-for-iot/
[110] *Teach, Learn, and Make With Raspberry PI–Raspberry PI*. Accessed: 2020. [Online]. Available: https://www.raspberrypi.org/
[111] *Download Raspbian for Raspberry PI*. Accessed: 2020. [Online]. Available: https://www.raspberrypi.org/downloads/raspbian/
[112] *The Thing System—Hello, World!* Accessed: 2020. [Online]. Available: http://thethingsystem.com/
[113] *2020 Unit 42 IoT Threat Report*. Accessed: 2020. [Online]. Available: https://unit42.paloaltonetworks.com/iot-threat-report-2020/
[114] Y. Cherdantseva and J. Hilton, "A reference model of information assurance security," in *Proc. Int. Conf. Availability, Rel. Secur.*, 2013, pp. 546–555.
[115] P. Mehta, R. Gupta, and S. Tanwar, "Blockchain envisioned UAV networks: Challenges, solutions, and comparisons," *Comput. Commun.*, vol. 151, pp. 518–538, Feb. 2020.
[116] A. Kumari, S. Tanwar, S. Tyagi, and N. Kumar, "Fog computing for healthcare 4.0 environment: Opportunities and challenges," *Comput. Electr. Eng.*, vol. 72, pp. 1–13, Nov. 2018.
[117] F.-X. Standaert, *Introduction to Side-Channel Attacks*. Boston, MA, USA: Springer, 2010, pp. 27–42.
[118] V. Sachidananda, S. Siboni, A. Shabtai, J. Toh, S. Bhairav, and Y. Elovici, "Let the cat out of the bag: A holistic approach towards security analysis of the Internet of Things," in *Proc. 3rd ACM Int. Workshop IoT Privacy, Trust, Secur. (IoTPTS)*, New York, NY, USA, 2017, pp. 3–10.
[119] A. Kumari, R. Gupta, S. Tanwar, and N. Kumar, "A taxonomy of blockchain-enabled softwarization for secure UAV network," *Comput. Commun.*, vol. 161, pp. 304–323, Sep. 2020.
[120] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the Internet of Things," *IEEE Secur. Privacy*, vol. 13, no. 1, pp. 14–21, Jan. 2015.
[121] *Owasp IoT Top 10 Vulnerabilities*. Accessed: 2020. [Online]. Available: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10
[122] D. Ramesh and D. K. Rao, "Vampire attack: Draining life from wireless ad–hoc sensor networks," *Int. J. Comput. Appl.*, vol. 144, no. 9, pp. 1–4, 2014.
[123] S. Banerjee, V. Odelu, A. K. Das, S. Chattopadhyay, N. Kumar, Y. Park, and S. Tanwar, "Design of an anonymity-preserving group formation based authentication protocol in global mobility networks," *IEEE Access*, vol. 6, pp. 20673–20693, 2018.
[124] A. Rajan, J. Jithish, and S. Sankaran, "Sybil attack in IOT: Modelling and defenses," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Sep. 2017, pp. 2323–2327.
[125] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the RPL-based Internet of Things," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 8, Aug. 2013, Art. no. 794326.
[126] S. Venkatraman, M. Alazab, and R. Vinayakumar, "A hybrid deep learning image-based analysis for effective malware detection," *J. Inf. Secur. Appl.*, vol. 47, pp. 377–389, Aug. 2019.

[127] R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "Tactile-Internet-based telesurgery system for healthcare 4.0: An architecture, research challenges, and future directions," *IEEE Netw.*, vol. 33, no. 6, pp. 22–29, Nov. 2019.

[128] *Smart Nest Thermostat: A Smart Spy in Your Home*. Accessed: 2020. [Online]. Available: https://blackhat.com/docs/us-14/materials/us-14-Jin-Smart-Nest-Thermostat-A-Smart-Spy-In-Your-Home-WP.pdf

[129] Z. Basnight, J. Butts, J. Lopez, and T. Dube, "Firmware modification attacks on programmable logic controllers," *Int. J. Crit. Infrastructure Protection*, vol. 6, no. 2, pp. 76–84, Jun. 2013.

[130] O. Arias, J. Wurm, K. Hoang, and Y. Jin, "Privacy and security in Internet of Things and wearable devices," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 1, no. 2, pp. 99–109, Apr. 2015.

[131] A. Tekeoglu and A. S. Tosun, "A testbed for security and privacy analysis of IoT devices," in *Proc. IEEE 13th Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS)*, Oct. 2016, pp. 343–348.

[132] B. Reaves and T. Morris, "An open virtual testbed for industrial control system security research," *Int. J. Inf. Secur.*, vol. 11, no. 4, pp. 215–229, Aug. 2012.

[133] A. Furfaro, L. Argento, A. Parise, and A. Piccolo, "Using virtual environments for the assessment of cybersecurity issues in IoT scenarios," *Simul. Model. Pract. Theory*, vol. 73, pp. 43–54, 2017. Smart Cities and Internet of Things.

[134] S. Siboni, V. Sachidananda, Y. Meidan, M. Bohadana, Y. Mathov, S. Bhairav, A. Shabtai, and Y. Elovici, "Security testbed for Internet-of-Things devices," *IEEE Trans. Rel.*, vol. 68, no. 1, pp. 23–44, Mar. 2019.

[135] S. Siboni, A. Shabtai, N. O. Tippenhauer, J. Lee, and Y. Elovici, "Advanced security testbed framework for wearable IoT devices," *ACM Trans. Internet Technol.*, vol. 16, no. 4, pp. 1–25, Dec. 2016.

[136] V. Sachidananda, J. Toh, S. Siboni, A. Shabtai, and Y. Elovici, "POSTER: Towards exposing Internet of Things: A roadmap," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, Oct. 2016, pp. 1820–1822.

[137] C. Burin des Roziers, G. Chelius, T. Ducrocq, E. Fleury, A. Fraboulet, A. Gallais, N. Mitton, T. Noél, and J. Vandaele, "Using senslab as a first class scientific tool for large scale wireless sensor network experiments," in *NETWORKING*, J. Domingo-Pascual, P. Manzoni, S. Palazzo, A. Pont, and C. Scoglio, Eds. Berlin, Germany: Springer, 2011, pp. 147–159.

[138] L. Sanchez, L. Muñoz, J. A. Galache, P. Sotres, J. R. Santana, V. Gutierrez, R. Ramdhany, A. Gluhak, S. Krco, E. Theodoridis, and D. Pfisterer, "SmartSantander: IoT experimentation over a smart city testbed," *Comput. Netw.*, vol. 61, pp. 217–238, Mar. 2014.

[139] R. Tommy, G. Sundeep, and H. Jose, "Automatic detection and correction of vulnerabilities using machine learning," in *Proc. Int. Conf. Current Trends Comput., Electr., Electron. Commun. (CTCEEC)*, Sep. 2017, pp. 1062–1065.

[140] T. M. Mitchell, J. G. Carbonell, and R. S. Michalski, *Machine Learning: A Guide to Current Research*, vol. 12. Berlin, Germany: Springer, 1986.

[141] D. Barber, *Machine Learning*. Cambridge, U.K.: Cambridge Univ. Press, 2012, pp. 303–304.

[142] M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1996–2018, 4th Quart., 2014.

[143] L. Xiao, Y. Li, X. Huang, and X. Du, "Cloud-based malware detection game for mobile devices with offloading," *IEEE Trans. Mobile Comput.*, vol. 16, no. 10, pp. 2742–2750, Oct. 2017.

[144] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. Ping Liu, "A system for Denial-of-Service attack detection based on multivariate correlation analysis," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 447–456, Feb. 2014.

[145] Y. Gwon, S. Dastangoo, C. Fossa, and H. T. Kung, "Competing mobile network game: Embracing antijamming and jamming strategies with reinforcement learning," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2013, pp. 28–36.

[146] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-layer spoofing detection with reinforcement learning in wireless networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10037–10047, Dec. 2016.

[147] F. A. Narudin, A. Feizollah, N. B. Anuar, and A. Gani, "Evaluation of machine learning classifiers for mobile malware detection," *Soft Comput.*, vol. 20, no. 1, pp. 343–357, Jan. 2016.

[148] A. Azmoodeh, A. Dehghantanha, and K.-K.-R. Choo, "Robust malware detection for Internet of (battlefield) Things devices using deep eigenspace learning," *IEEE Trans. Sustain. Comput.*, vol. 4, no. 1, pp. 88–95, Jan. 2019.

[149] N. Kumar, N. Chilamkurti, and S. Misra, "Bayesian coalition game for the Internet of Things: An ambient intelligence-based evaluation," *IEEE Commun. Mag.*, vol. 53, no. 1, pp. 48–55, Jan. 2015.

[150] H. Hashemi, A. Azmoodeh, A. Hamzeh, and S. Hashemi, "Graph embedding as a new approach for unknown malware detection," *J. Comput. Virol. Hacking Techn.*, vol. 13, no. 3, pp. 153–166, Aug. 2017.

[151] I. Santos, F. Brezo, X. Ugarte-Pedrero, and P. G. Bringas, "Opcode sequences as representation of executables for data-mining-based unknown malware detection," *Inf. Sci.*, vol. 231, pp. 64–82, May 2013.

[152] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet Things*, vol. 7, Sep. 2019, Art. no. 100059.

[153] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, and K.-K.-R. Choo, "A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks," *IEEE Trans. Emerg. Topics Comput.*, vol. 7, no. 2, pp. 314–323, Apr. 2019.

[154] N. Moustafa, B. Turnbull, and K.-K.-R. Choo, "An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4815–4830, Jun. 2019.

[155] I. Kotenko, I. Saenko, and A. Branitskiy, "Framework for mobile Internet of Things security monitoring based on big data processing and machine learning," *IEEE Access*, vol. 6, pp. 72714–72723, 2018.

[156] P. Punithavathi, S. Geetha, M. Karuppiah, S. H. Islam, M. M. Hassan, and K.-K.-R. Choo, "A lightweight machine learning-based authentication framework for smart IoT devices," *Inf. Sci.*, vol. 484, pp. 255–268, May 2019.

[157] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Future Gener. Comput. Syst.*, vol. 82, pp. 761–768, May 2018.

[158] G. D'angelo, F. Palmieri, M. Ficco, and S. Rampone, "An uncertainty-managing batch relevance-based approach to network anomaly detection," *Appl. Soft Comput.*, vol. 36, pp. 408–418, Nov. 2015.

[159] P. M. Kumar and U. Devi Gandhi, "A novel three-tier Internet of Things architecture with machine learning algorithm for early detection of heart diseases," *Comput. Electr. Eng.*, vol. 65, pp. 222–235, Jan. 2018.

[160] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, "N-baiot—Network-based detection of iot botnet attacks using deep autoencoders," *IEEE Pervas. Comput.*, vol. 17, no. 3, pp. 12–22, Jul./Sep. 2018.

[161] B. Chatterjee, D. Das, S. Maity, and S. Sen, "RF-PUF: Enhancing IoT security through authentication of wireless nodes using *in-situ* machine learning," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 388–398, Feb. 2019.

[162] S. Tyagi, S. Tanwar, S. K. Gupta, N. Kumar, and J. J. P. C. Rodrigues, "A lifetime extended multi-levels heterogeneous routing protocol for wireless sensor networks," *Telecommun. Syst.*, vol. 59, no. 1, pp. 43–62, May 2015.

[163] R. Maes, *Physically Unclonable Functions: Constructions, Properties and Applications*. Berlin, Germany: Springer, 2013.

[164] J. Chauhan, S. Seneviratne, Y. Hu, A. Misra, A. Seneviratne, and Y. Lee, "Breathing-based authentication on resource-constrained iot devices using recurrent neural networks," *Computer*, vol. 51, no. 5, pp. 60–67, 2018.

[165] K. Patel, D. Mehta, C. Mistry, R. Gupta, S. Tanwar, N. Kumar, and M. Alazab, "Facial sentiment analysis using AI techniques: State-of-the-art, taxonomies, and challenges," *IEEE Access*, vol. 8, pp. 90495–90519, 2020.

[166] S. K, L. S. K., A. Khanna, S. Tanwar, J. J. P. C. Rodrigues, and N. R. Roy, "Alzheimer detection using group grey wolf optimization based features with convolutional classifier," *Comput. Electr. Eng.*, vol. 77, pp. 230–243, Jul. 2019.

[167] U. Jayasinghe, G. M. Lee, T.-W. Um, and Q. Shi, "Machine learning based trust computational model for IoT services," *IEEE Trans. Sustain. Comput.*, vol. 4, no. 1, pp. 39–52, Jan. 2019.

[168] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1644–1652, Sep. 2017.

[169] B. Li, S. Gangadhar, S. Cheng, and P. K. Verma, "Predicting user comfort level using machine learning for smart grid environments," in *Proc. ISGT*, Jan. 2011, pp. 1–6.

[170] T. Remani, E. A. Jasmin, and T. P. I. Ahamed, "Residential load scheduling with renewable generation in the smart grid: A reinforcement learning approach," *IEEE Syst. J.*, vol. 13, no. 3, pp. 3283–3294, Sep. 2019.

[171] S. Ryu, J. Noh, and H. Kim, "Deep neural network based demand side short term load forecasting," *Energies*, vol. 10, no. 1, p. 3, Dec. 2016.
[172] A. Kumari, D. Vekaria, R. Gupta, and S. Tanwar, "Redills: Deep learning-based secure data analytic framework for smart grid systems," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2020, pp. 1–6.
[173] S. Rathore and J. H. Park, "Semi-supervised learning based distributed attack detection framework for IoT," *Appl. Soft Comput.*, vol. 72, pp. 79–89, Nov. 2018.
[174] W. Li, W. Meng, Z. Tan, and Y. Xiang, "Design of multi-view based email classification for IoT systems via semi-supervised learning," *J. Netw. Comput. Appl.*, vol. 128, pp. 56–63, Feb. 2019.
[175] L. K. Shar, L. C. Briand, and H. B. K. Tan, "Web application vulnerability prediction using hybrid program analysis and machine learning," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 6, pp. 688–707, Nov. 2015.
[176] A. Lahmadi, C. Brandin, and O. Festor, "A testing framework for discovering vulnerabilities in 6LoWPAN networks," in *Proc. IEEE 8th Int. Conf. Distrib. Comput. Sensor Syst.*, May 2012, pp. 335–340.
[177] B. Cui, S. Liang, S. Chen, B. Zhao, and X. Liang, "A novel fuzzing method for ZigBee based on finite state machine," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 1, Jan. 2014, Art. no. 762891.
[178] J. Men, G. Xu, Z. Han, Z. Sun, X. Zhou, W. Lian, and X. Cheng, "Finding sands in the eyes: Vulnerabilities discovery in IoT with EUFuzzer on human machine interface," *IEEE Access*, vol. 7, pp. 103751–103759, 2019.
[179] Y. Jia, Y. Xiao, J. Yu, X. Cheng, Z. Liang, and Z. Wan, "A novel graph-based mechanism for identifying traffic vulnerabilities in smart home IoT," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2018, pp. 1493–1501.
[180] G. George and S. M. Thampi, "A graph-based security framework for securing industrial IoT networks from vulnerability exploitations," *IEEE Access*, vol. 6, pp. 43586–43601, 2018.
[181] F. Farivar, M. S. Haghighi, A. Jolfaei, and M. Alazab, "Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 4, pp. 2716–2725, Apr. 2020.
[182] U. D. Gandhi, P. M. Kumar, R. Varatharajan, G. Manogaran, R. Sundarasekar, and S. Kadu, "HIoTPOT: Surveillance on IoT devices against recent threats," *Wireless Pers. Commun.*, vol. 103, no. 2, pp. 1179–1194, Nov. 2018.
[183] Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, "IoTPOT: A novel honeypot for revealing current IoT threats," *J. Inf. Process.*, vol. 24, no. 3, pp. 522–533, 2016.
[184] E. Vasilomanolakis, S. Srinivasa, C. G. Cordero, and M. Muhlhauser, "Multi-stage attack detection and signature generation with ICS honeypots," in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp. (NOMS)*, Apr. 2016, pp. 1227–1232.
[185] D. Buza, F. Juhász, G. Miru, M. Félegyházi, and T. Holczer, "CryPLH: Protecting smart energy systems from targeted attacks with a PLC honeypot," in *Proc. Int. Workshop Smart Grid Secur.*, Feb. 2014, pp. 181–192.
[186] S. Litchfield, D. Formby, J. Rogers, S. Meliopoulos, and R. Beyah, "Rethinking the honeypot for cyber-physical systems," *IEEE Internet Comput.*, vol. 20, no. 5, pp. 9–17, Sep. 2016.
[187] J. D. Guarnizo, A. Tambe, S. S. Bhunia, M. Ochoa, N. O. Tippenhauer, A. Shabtai, and Y. Elovici, "SIPHON: Towards scalable high-interaction physical honeypots," in *Proc. 3rd ACM Workshop Cyber-Physical Syst. Secur. (CPSS)*, New York, NY, USA, 2017, pp. 57–68.
[188] S. Dowling, M. Schukat, and H. Melvin, "A ZigBee honeypot to assess IoT cyberattack behaviour," in *Proc. 28th Irish Signals Syst. Conf. (ISSC)*, Jun. 2017, pp. 1–6.
[189] *Kippo—SSH Honeypot*. Accessed: 2020. [Online]. Available: https://github.com/desaster/kippo
[190] V. Visoottiviseth, P. Akarasiriwong, S. Chaiyasart, and S. Chotivatunyu, "PENTOS: Penetration testing tool for Internet of Thing devices," in *Proc. IEEE Region 10 Conf. (TENCON)*, Nov. 2017, pp. 2279–2284.
[191] C.-K. Chen, Z.-K. Zhang, S.-H. Lee, and S. Shieh, "Penetration testing in the IoT age," *Computer*, vol. 51, no. 4, pp. 82–85, Apr. 2018.
[192] L. Markowsky and G. Markowsky, "Scanning for vulnerable devices in the Internet of Things," in *Proc. IEEE 8th Int. Conf. Intell. Data Acquisition Adv. Comput. Systems: Technol. Appl. (IDAACS)*, Sep. 2015, pp. 463–467.
[193] E. Ko, T. Kim, and H. Kim, "Management platform of threats information in IoT environment," *J. Ambient Intell. Humanized Comput.*, vol. 9, no. 4, pp. 1167–1176, Aug. 2018.
[194] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine learning-based network vulnerability analysis of industrial Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6822–6834, Aug. 2019.
[195] *Dojo By Bullguard-Intelligent Vulnerability Scanner*. Accessed: 2020. [Online]. Available: https://www.bullguard.com/press/press-releases/2018/dojo-by-bullguard-introduces-first-of-its-kind-int.aspx
[196] M. Patton, E. Gross, R. Chinn, S. Forbis, L. Walker, and H. Chen, "Uninvited connections: A study of vulnerable devices on the Internet of Things (IoT)," in *Proc. IEEE Joint Intell. Secur. Informat. Conf.*, Sep. 2014, pp. 232–235.
[197] R. Gupta, A. Kumari, and S. Tanwar, "A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles," *Trans. Emerg. Telecommun. Technol.*, pp. 1–24, Jun. 2020, doi: 10.1002/ett.4009.
[198] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal, "Security and privacy in smart farming: Challenges and opportunities," *IEEE Access*, vol. 8, pp. 34564–34584, 2020.
[199] *Cyber Security in UK Agriculture*. Accessed: 2020. [Online]. Available: https://www.nccgroup.com/uk/our-research/cyber-security-in-uk-agriculture/
[200] O. S. Cupp, D. E. Walker, and J. Hillison, "Agroterrorism in the US: Key security challenge for the 21st century," *Biosecur. Bioterrorism, Biodefense Strategy, Pract., Sci.*, vol. 2, no. 2, pp. 97–105, 2004.
[201] A. Salam, *Internet of Things for Sustainable Community Development: Internet of Things in Agricultural Innovation and Security*. Cham, Switzerland: Springer, 2020, pp. 71–112.
[202] O. Day and T. M. Khoshgoftaar, "A survey on heterogeneous transfer learning," *J. Big Data*, vol. 4, no. 1, p. 29, Dec. 2017.
[203] Y. Jia, Q. A. Chen, S. Wang, A. Rahmati, E. Fernandes, Z. Mao, and A. Prakash, "ContexIoT: Towards providing contextual integrity to appified IoT platforms," in *Proc. NDSS*, Jan. 2017, pp. 1–15.
[204] A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, M. Maasberg, and K.-K.-R. Choo, "Multimedia big data computing and Internet of Things applications: A taxonomy and process model," *J. Netw. Comput. Appl.*, vol. 124, pp. 169–195, Dec. 2018.
[205] E. McKenna, I. Richardson, and M. Thomson, "Smart meter data: Balancing consumer privacy concerns with legitimate applications," *Energy Policy*, vol. 41, pp. 807–814, Feb. 2012.
[206] Y. Michalevsky, A. Schulman, G. A. Veerapandian, D. Boneh, and G. Nakibly, "Powerspy: Location tracking using mobile device power analysis," in *24th USENIX Secur. Symp. (USENIX Security)*, Washington, DC, USA, Aug. 2015, pp. 785–800.
[207] A. Azab, M. Alazab, and M. Aiash, "Machine learning based botnet identification traffic," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Aug. 2016, pp. 1788–1794.
[208] R. Vinayakumar, M. Alazab, S. Srinivasan, Q.-V. Pham, S. K. Padannayil, and K. Simran, "A visualized botnet detection system based deep learning for the Internet of Things networks of smart cities," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4436–4456, Jul. 2020.
[209] A. Banafa, "IoT standardization and implementation challenges," *IEEE Internet Things J.*, 2016. Accessed: 2020. [Online]. Available: https://iot.ieee.org/newsletter/july-2016/iot-standardization-and-implementation-challenges.html
[210] O. Vermesan and P. Friess, *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*. Aalborg, Denmark: River Publishers, 2013.
[211] L. Lerman, S. Medeiros, G. Bontempi, and O. Markowitch, "A machine learning approach against a masked AES," in *Proc. Int. Conf. Smart Card Res. Adv. Appl.*, Nov. 2013, pp. 61–75.
[212] A. Heuser and M. Zohner, "Intelligent machine homicide," in *Proc. Int. Workshop Constructive Side-Channel Anal. Secure Design*, May 2012, pp. 249–264.
[213] S. Greydanus, "Learning the enigma with recurrent neural networks," *Neural Evol. Comput., Comput. Sci.*, pp. 1–7, 2017, doi: 1708.07576.
[214] S. Jialin Pan and Q. Yang, "A survey on transfer learning," *IEEE Trans. Knowl. Data Eng.*, vol. 22, no. 10, pp. 1345–1359, Oct. 2010.

POOJA ANAND is currently a full-time Research Scholar with the Department of Computer Sciences and Information Technology, Central University of Jammu, India, under the supervision of Dr. Yashwant Singh and Dr. Arvind Selwal. Her current research interests are in the areas of operational cybersecurity, including attack detection and characterization, vulnerabilities assessment methodologies, the Internet of Things, and machine learning.

YASHWANT SINGH received the bachelor's degree from SLIET Longowal, the master's degree from Punjab Engineering College, Chandigarh, and the Ph.D. degree from Himachal Pradesh University, Shimla. He was with the Jaypee University of Information Technology for 10 Years. He is currently an Associate Professor and the Head of the Department of Computer Science and Information Technology, Central University of Jammu, where he has been a Faculty Member since 2017. He is also a Visiting Professor at Jan Wyzykowski University, Polkowice, Poland. He has collaborated actively with researchers in several other disciplines of computer science, particularly machine learning and electrical engineering. Roughly, he has served on 30 conference and workshop program committees and served as the General Chair for PDGC-2014, ICRIC-2018, ICRIC-2019, and ICRIC-2020. He currently serves as the Coordinator of the Kalam Centre for Science and Technology (KCST), Central University of Jammu, established by DRDO. He has published more than 70 research articles in international journals, international conferences, and book chapters of repute. He has research projects worth INR 15 Crore (Approx.) in his credit. He has guided three Ph.D. and 24 M.Tech. students. He has visited eight countries for his academic visits, i.e., U.K., Germany, Poland, Chez Republic, Hungary, Slovakia, Austria, and Romania. His research interests lie in the area of the Internet of Things, wireless sensor networks, ICS/SCADA cybersecurity, ranging from theory to design to implementation.

ARVIND SELWAL is currently working as the Sr. Assistant Professor with the Department of Computer Science and Information Technology, Central University of Jammu, India. He has more than 14 years experience of teaching UG and PG classes. He has successfully guided 12 M.Tech. and one M.Phil. students. His research interests include machine learning, biometric security, image processing, and advanced database systems. He has contributed more than 20 research articles in reputed international/national journals indexed in Scopus and SCI. He has authored a book on *Fundamentals of Automata Theory and Computation*.

MAMOUN ALAZAB (Senior Member, IEEE) received the Ph.D. degree in computer science from the School of Science, Information Technology and Engineering, Federation University of Australia. He is a Cyber Security Researcher and Practitioner with industry and academic experience. He is currently an Associate Professor with the College of Engineering, IT and Environment, Charles Darwin University, Australia. His research is multidisciplinary that focuses on cybersecurity and digital forensics of computer systems with a focus on cybercrime detection and prevention. He has more than 150 research papers in many international journals and conferences. He is the Founding Chair of the IEEE Northern Territory (NT) Subsection.

SUDEEP TANWAR (Member, IEEE) received the B.Tech. degree from Kurukshetra University, India, in 2002, the M.Tech. degree (Hons.) from Guru Gobind Singh Indraprastha University, New Delhi, India, in 2009, and the Ph.D. degree, in 2016, with a specialization in the wireless sensor network. He is currently an Associate Professor with the Computer Science and Engineering Department, Institute of Technology, Nirma University, Ahmedabad, India. He is currently a Visiting Professor with Jan Wyzykowski University, Polkowice, Poland, and the University of Pitesti, Pitesti, Romania. He has authored or coauthored more than 140 technical research papers published in leading journals and conferences from the IEEE, Elsevier, Springer, Wiley, and so on. Some of his research findings are published in top-cited journals such as the IEEE Transactions on Network Science and Engineering (TNSE), the IEEE Transactions on Vehicular Technology, the IEEE Transactions on Industrial Informatics, the *Computer Communication*, the *Applied Soft Computing*, the *Journal of Network and Computer Application*, the *Pervasive and Mobile Computing*, the *International Journal of Communication System*, *Telecommunication System, Computer and Electrical Engineering*, and the IEEE Systems Journal. He has also published six edited/authored books with International/National Publishers like IET, Springer. He has guided many students leading to M.E./M.Tech. and guiding students leading to Ph.D. His current research interests include wireless sensor networks, fog computing, smart grid, IoT, and blockchain technology. He was invited as the Guest Editors/Editorial Board Members of many International Journals, invited for keynote Speaker in many International Conferences held in Asia, and invited as Program Chair, Publications Chair, Publicity Chair, and Session Chair in many International Conferences held in North America, Europe, Asia, and Africa. He has been awarded the best research paper awards from IEEE GLOBECOM 2018, IEEE ICC 2019, and Springer ICRIC-2019. He is an Associate Editor of the *International Journal of Communication Systems* (IJCS) (Wiley), and *Security and Privacy Journal* (Wiley).

NEERAJ KUMAR (Senior Member, IEEE) received the Ph.D. degree in CSE from Shri Mata Vaishno Devi University, Katra, India. He was a Postdoctoral Research Fellow with Coventry University, Coventry, U.K. He is a Visiting Professor at Coventry University, Coventry, U.K. He is currently a Full Professor with the Department of Computer Science and Engineering, Thapar University, Patiala, India. He has published more than 300 technical research papers in leading journals and conferences from IEEE, Elsevier, Springer, John Wiley, and so on. Some of his research findings are published in top-cited journals such as the IEEE TIE, IEEE TDSC, IEEE TITS, IEEE TCC, IEEE TKDE, IEEE TVT, IEEE TCE, IEEE Netw., IEEE Comm., IEEE WC, IEEE IoTJ, IEEE SJ, FGCS, JNCA, and ComCom. He has guided many Ph.D. and M.E./M.Tech. students. His research is supported by fundings from Tata Consultancy Service, Council of Scientific and Industrial Research (CSIR), and the Department of Science and Technology. He has awarded the best research paper awards from IEEE ICC 2018 and IEEE Systems Journal 2018. He is leading the research group Sustainable Practices for the Internet of Energy and Security (SPINES), where group members are working on the latest cutting edge technologies. He is a TPC member and reviewer of many international conferences across the globe.