An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security

Waseem Iqbal, Haider Abbas, Mahmoud Daneshmand, Bilal Rauf, and Yawar Abbas Bangash

***Abstract*—Internet of Things (IoT) is transforming everyone's life by providing features, such as controlling and monitoring of the connected smart objects. IoT applications range over a broad spectrum of services including smart cities, homes, cars, manufacturing, e-healthcare, smart control system, transportation, wearables, farming, and much more. The adoption of these devices is growing exponentially, that has resulted in generation of a substantial amount of data for processing and analyzing. Thus, besides bringing ease to the human lives, these devices are susceptible to different threats and security challenges, which do not only worry the users for adopting it in sensitive environments, such as e-health, smart home, etc., but also pose hazards for the advancement of IoT in coming days. This article thoroughly reviews the threats, security requirements, challenges, and the attack vectors pertinent to IoT networks. Based on the gap analysis, a novel paradigm that combines a network-based deployment of IoT architecture through software-defined networking (SDN) is proposed. This article presents an overview of the SDN along with a thorough discussion on SDN-based IoT deployment models, i.e., centralized and decentralized. We further elaborated SDN-based IoT security solutions to present a comprehensive overview of the software-defined security (SDSec) technology. Furthermore, based on the literature, core issues are highlighted that are the main hurdles in unifying all IoT stakeholders on one platform and few findings that emphases on a network-based security solution for IoT paradigm. Finally, some future research directions of SDN-based IoT security technologies are discussed.**

***Index Terms*—Internet of Things (IoT) security, software-defined networking (SDN), SDN-IoT, software-defined security (SDSec).**

Manuscript received January 29, 2020; revised March 29, 2020 and May 4, 2020; accepted May 19, 2020. Date of publication May 26, 2020; date of current version October 9, 2020. This work was supported by the Higher Education Commission (HEC), Pakistan, through its initiative of National Center for Cyber Security for the affiliated lab National Cyber Security Auditing and Evaluation Lab under Grant 2(1078)/HEC/M&E/2018/707. *(Corresponding author: Haider Abbas.)*

Waseem Iqbal, Haider Abbas, Bilal Rauf, and Yawar Abbas Bangash are with the Department of Information Security, National University of Sciences and Technology, Islamabad 44000, Pakistan (e-mail: waseem.iqbal@mcs.edu.pk; haider@mcs.edu.pk; bilal-rauf@mcs.edu.pk; yawar@mcs.edu.pk).

Mahmoud Daneshmand is with the School of Engineering and Science, Stevens Institute of Technology, Hoboken, NJ 07030 USA (e-mail: mahmoud.daneshmand@stevens.edu).

Digital Object Identifier 10.1109/JIOT.2020.2997651

I. Introduction

INTERNET and Web expansion into the physical reality was made possible through various aspects that come under the umbrella of the term widely used, i.e., Internet of Things or IoT, which is an evolving topic of economic, social, and technical importance [1]. The growth of advanced enabling technologies, such as cloud computing, data analytics, IP-based networking, ubiquitous computing etc., has brought IoT into reality; otherwise, the trend of controlling devices by combining sensors, computers, and networks has been in use for decades [2]. The word Internet of Things was first introduced by Ashton *et al.* in 1999 [3] while talking of a global network of objects connected to RFID in a supply chain application. Since then, IoT is extended to new application areas and a plethora of new technologies have emerged in the IoT domain, such as industry, agriculture, animal farming, transport, healthcare, smart homes, smart retail, supply chain, smart wearables, smart security, etc. Network of Things or NoT is often used interchangeably with IoT [4].

According to the world's well-known research and advisory firm Gartner, by the end of 2020, 25 billion devices will be connected to the Internet and will have the ability to analyze user data and make smart decisions in an autonomous way [5]. However, making computers/devices/nodes capable of gathering, processing, and decision making without or least input of humans remains the objective of IoT [6]. Building blocks for IoT are not formally defined, but their operation can be defined in terms of sensors, computation, communication, and actuators, which produce data to gain knowledge and make intelligent decisions [7].

It is the data produced by these sensors that have caused the convergence of different fields, such as computer science, software engineering, sensing, networking, artificial intelligence, and communication together. Smarter systems are the products envisioned due to the rapid progress of IoT. Due to the diversity of the IoT environment and exponential progress resultant from the immense research has, indeed, paved the way for lack of a standardized definition and standardization of IoT [2].

More than 85% of organizations in the world will be leveraging IoT devices in different ways according to [8] and about 90% of these enterprises are not certain about their IoT devices security. Likewise, Steinberg [9] stated that many smart home devices can spy inhabitants in their own homes. It is discovered in a study carried out by HP [10] that 70%

of the IoT devices are susceptible to various attacks when connected to the Internet. Furthermore, the newly shifted IoT-based industries, such as power, transportation, chemical, clean water, and sewerage control systems pose elevated security risks [11], [12]. Attacks on industrial systems are a reality and are just not a threat, as more than 60,000 vulnerabilities were found by two Russian security researchers that can gain complete control of compromised systems [13]. Moreover, 25% of enterprise attacks would be due to compromised IoT devices by the end of 2020 [14].

A huge amount of data is produced by these devices such as in the year 2018 (6.2 EB), which is estimated to increase by 478% (30.6 EB) by the end of 2020 [15]. This alarming projected data generation rise of 478% is calling out for intelligent network control and management solution. Many solutions were put forward to resolve existing issues in the IoT paradigm; however, the traditional network is not capable of handling such an enormous number of connected devices and huge data manipulation. The software-defined networking (SDN) is considered as a revolutionary networking technology that supports heterogeneous network, with rapid evolution and dynamism using programmable planes (control and data plane). The SDN and IoT integration can meet the expectation of control and management in diverse scenarios [16], [17].

A. Motivation and Related Work

To the best of our knowledge, until now, many research reviews and survey papers have published IoT security issues and adoption of new networking paradigm, software-defined networking (SDN), for the deployment of IoT networks [18]–[24]. However, the available literature does not provide complete insight into IoT security and leveraging SDN in its true essence to overcome the security issues in the IoT environment. Table I shows a detailed assessment of the existing work till date. It can be analyzed from the table that researchers focus on few elements and do not concentrate on others to provide a complete picture. For example, Khan and Hameed [20] referred to the identification and categorization of limited generic security issues in IoT and outlining possible future research in the area without providing an outline of a complete security model for IoT security. Likewise, Bizanis and Kuipers [21] outlined how SDN and network function virtualization (NFV) can be combined in wireless sensor networks, specifically focusing on 5G. Some generic SDN-NFV-enabled IoT architectures along with use-cases are discussed by the authors without highlighting the security aspects of IoT and provisioning of any software-defined secure model for the purpose. Similarly, the work presented in [22] highlights the gap between academic researchers and commercial vendors who have incorporated machine learning (ML) in SDN for augmenting security in IoT and other networks. Furthermore, the authors also provided few recommendations, which they believe will help solution designers and researchers in building their product, if adopted in the early phase of the design.

Salman *et al.* [23] discussed the security and privacy concerns in IoT emphasizing some open research problems. The article broadly covers some of the generalized threats, including scalability and management complications, heterogeneity and interoperability issues, and handling big data with security and privacy apprehensions. The authors then highlighted the need for convergence of SDN-NFV, fog computing, and 5G-based wireless sensors network for enabling a secure IoT evolution. While, to address the data transfer in a heterogeneous IoT environment, Liu *et al.* [18] presented a middlebox-guard (M-G), which is an SDN-based data transfer security model with the main aim of minimizing network latency and accurately managing data flows between different networks to ensure data transfer security. In a similar attempt of leveraging SDN in an IoT environment for providing security as a service, Conti *et al.* [19] proposed the censor architecture that is a lightweight and mountable remote software attestation scheme for maintaining the integrity of the IoT devices' software being used for specific purpose.

In another effort to identify generic and layerwise threats in IoT, a tremendous effort is put forward by Makhdoom *et al.* [24]. The researcher's main emphasis in the survey article is to concretely define the structure of malware attacks on the IoT ecosystem. In addition, they also presented the attack methodology of various successful malware attacks and highlighted the Distributed Denial-of-Service (DDoS) strategy via IoT botnet. Some open research challenges are also featured in the survey. Though, sufficient research has been conducted on security issues related to IoT; however, by including an overview of technology shift solutions for the deployment of IoT and security efforts through these new network paradigms, such as SDN and NFV, can demonstrate a clear picture of IoT security and its countermeasures through SDN.

B. Contribution of This Article

Based on the extensive study of available literature and to the best of our knowledge, this is the first of its kind effort that reviews the IoT security in depth and highlights SDN-based network security solutions for IoT. To fill the gap highlighted in the current literature as shown in Table I, the main endeavors of this article can be summed up as threefold.

1) The first half presents a comprehensive overview of the characteristics of IoT security. This article advances rationally by presenting a generic IoT architecture followed by IoT protocol stack and corresponding security challenges at various layers of IoT networks. Specific IoT data, communication and end-to-end applications-related specific security threats, and vulnerabilities alongside some generic threats are also explained further. The readers are also acquainted with security requirements and challenges of various IoT application domains.
2) Keeping in view the limitations of the traditional network, we did the gap analysis and emphasized on network-based security solutions for the IoT system. SDN diverse properties, such as scalability, programmability, global visibility, and manageability, can overcome the constraints of the conventional network. We then appraised the readers with SDN in general and elaborated an overview of the architecture to get the complete insight of the new technology. Furthermore, SDN-based deployment models of IoT systems are discussed.

TABLE I
COMPREHENSIVE OVERVIEW OF IOT SECURITY, ITS DEPLOYMENT BASED ON SDN, AND HOW SDN AND ML ARE AUGMENTED TO ADDRESS DIFFERENT THREATS

Research Work	Elaborated Overview of IoT	Generic and Specific Threats to IoT	IoT Application Areas Security Requirements and Challenges	Real World IoT Attacks Examples	Gap Analysis and Way Forward	Intro to Software Defined Networking and Importance for usage in IoT	Deployment of IoT via SDN	Software Defined Security approaches for IoT	Machine Learning for Securing SDN-IoT	Open Research Challenges
F. I. Khan et al.	X	Discussed only five security threats to IoT	X	X	X	X	X	X	X	√
N. Bizan -is et al.	X	X	X	X	Generalized recommendations for leveraging SDN in IoT networks	Introduction to SDN is given in a generic manner and its use for WSN based IoT is highlighted only	√	X	X	Generic
T. N. Nguyen et al.	X	X	X	X	√	X	X	Emphasis on Machine learning based general security models	√	X
O. Salman et al.	X	Broadly covers Identity Management, Authentication, Access	X	X	X	X	Few architectures are discussed	SDN-NFV based 2-3 architectures are discussed only	X	√
Y. Liu et al.	X	Data Transfer Security only	X	X	X	X	X	A Middle Box Guard is introduced to safeguard data transfer	X	X
M. Conti et al.	X	IoT devices remote attestation only	X	X	X	√	X	SDN-cloud based secure IoT architecture CENSOR is proposed for remote SW attestation of IoT devices	X	√
I. Makhd -oom et al.	√	√	√	√	√	Just identified SDN as potential approach for providing security to IoT. I. Makhdoom et al. focused on block chain technology	X	X	X	√

To differentiate this article from other researchers, we presented software-defined security (SDSec)-based IoT models to the best of our knowledge, alongside highlighting the available commercial products as well.

3) Finally, the last effort standpoints by generating a discussion that provides the summary of the IoT security, findings we came across in this article, and emphasizing on the issues that are the main reason for lack of a standardized security framework. At the end, we concluded with open research challenges.

C. Taxonomy of the Article

The remainder of this article is structured as follows. Section II presents a detailed IoT architecture followed by the generic security threats, challenges related to data, communication, and end-applications along with different IoT applications' security requirements and challenges in Section III, whereas Section IV highlights the identified gaps and need for a network-based solution for IoT security. Section V uncovers the SDN paradigm and SDN-based IoT deployments along with SDSec solutions for SDN-IoT. Furthermore, discussion findings, and main issues are identified in the literature available on the IoT security and SDN-based IoT deployments models in Section VI. Section VII highlights the open research challenges, and Section VIII concludes this article as depicted in Fig. 1.

II. IOT ARCHITECTURE

Different IoT applications, such as smart grid, healthcare, transportation system, city, supply chain, farming, retail, wearable, environment, manufacturing, home, security, and

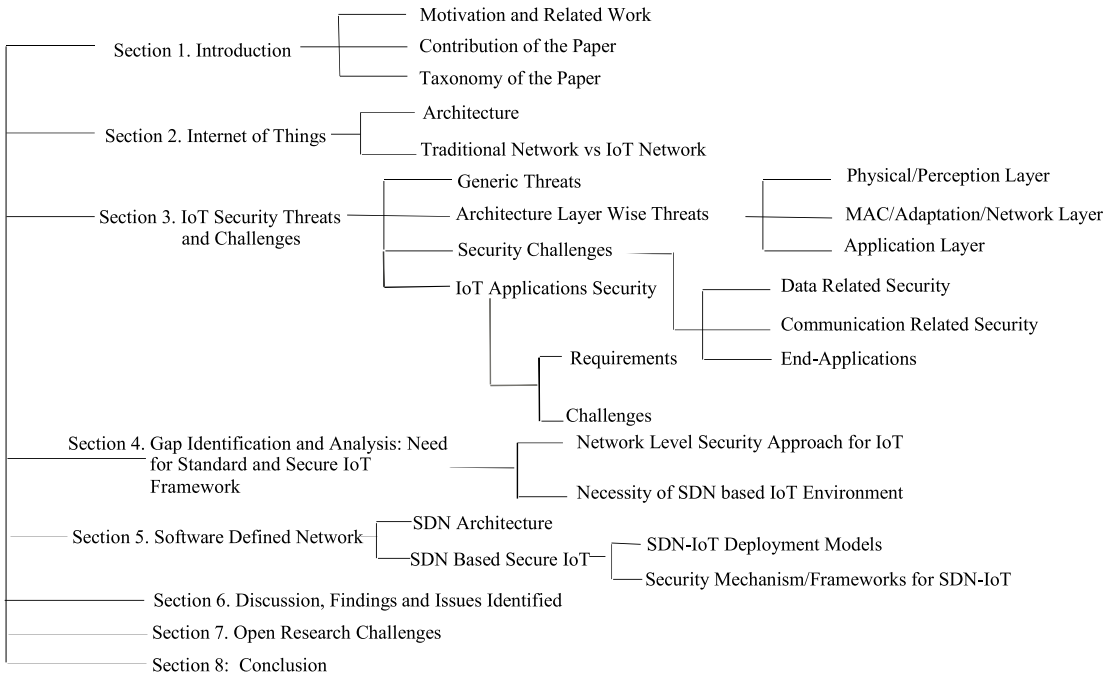


Fig. 1. Organization of this article. A top down approach is used to encompass IoT security, SDN for IoT security, and future work.

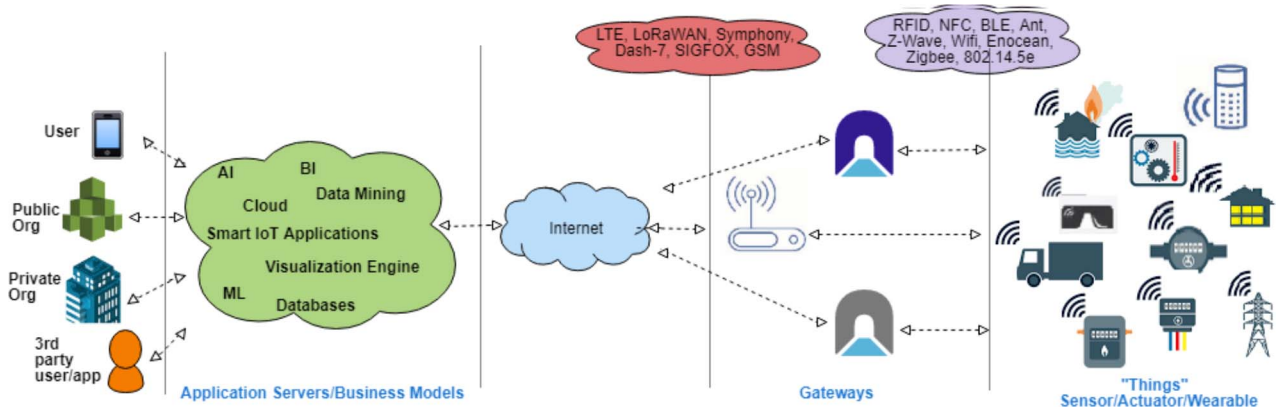


Fig. 2. Generic IoT architecture. The infrastructure layer (from right to left) consists of different sensor nodes, which are further connected to the Internet via the IoT gateway. At the cloud level, different processing is done to address business applications' need, such as BI, data mining, visualization, and other different services.

emergencies are generally referred to as the IoT system. The IoT ecosystem aims at referring all IoT applications as mentioned above. The IoT architecture is composed of various "things" that include sensors, actuators, gateways, protocols, cloud services, network, and application servers which are arranged in different topologies to communicate with each other.

Currently, the world is facing problems, such as manageability, compatibility, and interoperability in IoT solutions, because of the deficiencies in steadiness and standardization [25]. Similarly, the unvarying IoT-layered protocol stack and architectures were observed in [26]–[30]. For example, IoT layers were stated with minor details of basic functionality and protocols by Kumar *et al.* [26]. Likewise, communication protocols at different IoT layers were discussed by Granjal *et al.* [27]. While Al-Fuqaha *et al.* [28] put together key components and technologies that form an IoT system. The major stakeholders have not agreed on a sole IoT reference model due to the nonuniformity and lack of standardization [28]. To trim down this nonuniformity, we present a generic IoT architecture in Fig. 2 and a generalized layered IoT protocol stack is shown in Fig. 3.

In an IoT ecosystem, different nodes such as sensors, actuators, and wearable devices are connected to gateways through network communication protocols, such as NFC, BLE, RFID, 802.14.5e, 6LoWPAN, Ant, Z-Wave ZigBee, WiFi, EnOcean, Miwi, DigiMesh, and wireless HART. Furthermore, the gateways are linked to a network or application servers using LoRaWAN, SigFox, LTE, GSM, Dash-7, OFC, etc. The servers are usually placed in the cloud for provisioning of numerous data analytical services for users and public/private organizations, including third-party users and applications. After data aggregation and processing, the raw data are twisted into constructive information in the form

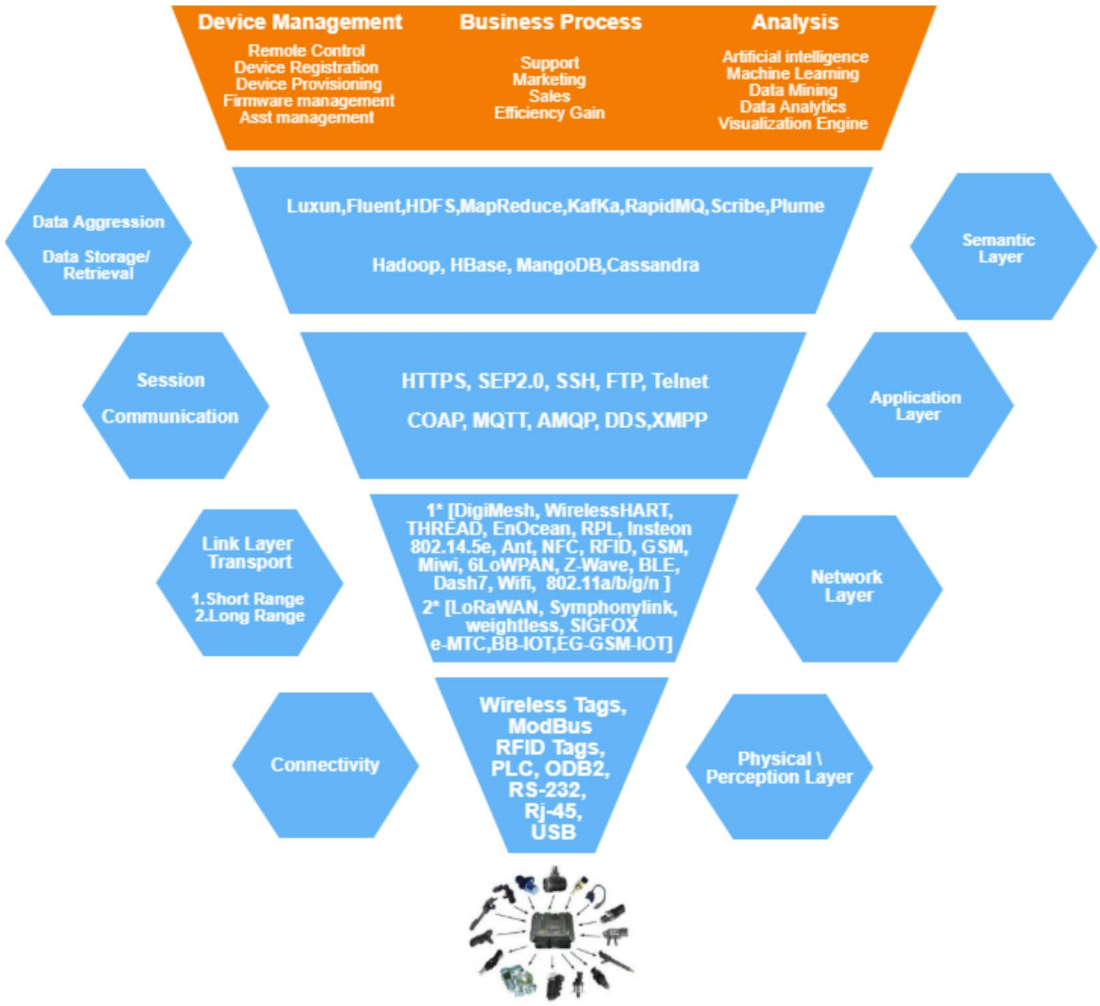


Fig. 3. Generalized layered IoT protocol stack. Different protocols are used in the IoT architecture for different purposes as opposed to traditional networking. In the IoT paradigm, all these protocols address resource constraint behavior, such as limited memory, limited computing, and limited coverage area.

of e-healthcare records and stats, weather/environmental and other updates regarding smart city services, autonomous smart home services, business analytics and support information, industrial automation, smart farming/environment monitoring, and smart gadgets.

In a generic IoT protocol stack, "things," such as sensors and actuators, belong to the first layer that is the physical/perception layer. The main task of this layer is to perceive environmental data and its collection [31]. In addition, modulation/demodulation, encryption/decryption, frequency selection, data transmission, and reception are added tasks of the physical/perception layer. Energy utilization, security, and interoperability are some of the challenges faced by this layer [25]. Receiving data from sensing objects and passing it to the application layer for processing, smart services and analytics are the responsibilities of the second layer, i.e., adaptation/network layer. Network availability, scalability, power utilization, and security are some issues that confront the network layer [25].

Application/service layer is the third layer as shown in Fig. 3. This layer presents smart services to the end users. It also supplies processed and aggregated data to the upper layer that is the semantics layer. Some of the challenges faced by this layer are handing out data received from various sensors, management and storage of data, privacy and security of user data, and compliance with governmental and industrial regulation, such as health insurance portability accountability act (HIPAA) and personal information protection and electronic documents act (PIPEDA). The last layer in the IoT protocol stack is the semantic layer, which is known as the business management layer. All of the IoT system activities are managed by this layer. It uses different technologies to provide services, such as visualization engines, data mining, business intelligence, data analysis, smart decision making, and marketing sales/support. Various uncommon features between IoT and traditional networks are discussed in the following section.

A. Traditional Network Versus IoT Network

The resourcefulness of the end devices is the substantial difference between standard networks and IoT [32]. Resource constraint devices, such as sensor nodes and RFID tags/readers are usually used in IoT systems. These devices mostly operate on low power, limited memory, computing power, and storage area. On the other hand, the traditional network is made

up of overflowing resource devices, such as laptops, computer systems, servers, and smartphones. Therefore, without any limitations of resources, traditional networks can sustain complex and many fold security protocols. Therefore, a balance is required between security and resource computations in IoT systems, which calls for lightweight security algorithms and protocols.

Less secure wireless protocols, such as ZigBee, 802.15.4e, SigFox, LoRa, and 802.11x are used by IoT devices to connect with gateway or Internet, which result in data leakage and privacy issues. Another major difference is that OS and data formats are identical in traditional network devices, whereas, due to different application functionalities and lack of standard OS, the IoT ecosystem faces diverse data formats and contents. It is due to this diversity, that a standard security protocol is yet to be developed that suits all kinds of IoT devices and systems. Conventional networks are protected by perimeter defense design pivoting on software- and hardware-based firewalls, IDS's, and IPS's. The host-based security approach is opted for securing the end nodes by means of anti-virus and security patches. But, the resource constraint behavior of IoT devices refrains from the host-based security approaches [33]. Similarly, due to the lack of physical security, deficiency of host-based defense methods, the slow pace of software updates and security patches, and insufficient access control mechanisms, the traditional perimeter defense methods cannot guard the IoT ecosystem from unauthorized users and insider attacks.

III. IoT Security Threats and Challenges

Nonstandardization of IoT technologies with intensified vulnerabilities will augment more security incidents in IoT systems. The following sections draw attention to some generic threats before discussing layerwise specific threats.

A. Generic Threats

This section highlights some generic threats that are applicable on all IoT systems.

1) *Hardware Vulnerabilities:* Security is not the main consideration of commercially developed IoT products rather they are device functionality centric. Therefore, improvised security features are usually added later on. Hence, hardware vulnerabilities, such as open physical interfaces and boot process vulnerabilities remain in such devices, which can be exploited remotely [34]. While the integrity of the end device, specifically code integrity and authentic data, ensures the consistent and secure operations of IoT systems [35].
2) *Vulnerabilities of Social Engineering:* Human interactions and socializing with IoT devices have greatly impacted the lives of users. The thorough and ubiquitous collection of data makes IoT users vulnerable to social engineering attacks [36]. Hackers can take control of smart devices, such as Google glasses [37], smart TVs, smart refrigerators, Fitbits [38], [39], etc., to keep an eye on users and learning their voices, preferences, and habits.
3) *Legislation Challenges:* The secure use of IoT data cannot be assured by legislation; however, it can compensate for the damage done through the misuse of data. To the best of our knowledge, no standardized legislation and secure data policy are drafted till now. Some efforts have been made by different countries to provide safety to user data, such as general data protection regulation (GDPR) [40] and HIPPA [41]. HIPPA-paralleled security must be provided by IoT device producers and app developers while providing features, such as tapping heart rate, weight, blood pressure, and other health insights.
4) *User Unawareness:* One of the most conventional attack vectors is the user. Employees and end users are susceptible to social engineering, phishing/spear phishing, and fortuitous security breaches due to the lack of security training and awareness. An additional medium of the security breach is the transmission of sensitive data via mobile devices over public networks. With the increase in smartphone users, it is estimated that one third of mobile devices will expose official data [14].
5) *DoS/DDoS Attacks:* Resource exhaustion attacks are carried out on IoT devices due to low memory, computation power, and battery consumption [30], such as jamming of communication channels, malicious utilization of IoT resources in terms of bandwidth, memory, CPU time, disk space, and modifying node configuration. Furthermore, Makhdoom *et al.* [24] stated that DDoS attacks involve 96% of the IoT devices which includes 3% home routers and 1% compromised Linux servers.

B. Architecture Layerwise Threats

Threats and vulnerabilities at different layers of the IoT architecture along with concerned security challenges are summarized in Table II. The following sections focus on the in-depth detail of threats at different layers of the IoT architecture.

1) Physical/Perception Layer: Some of the significant threats at the physical/perception layer are as follows.

1) *Eavesdropping:* Malicious devices such as end nodes are connected to IoT systems for passive sniffing of traffic in order to get some useful information [42].
2) *Battery Drainage Attack:* Continuous authentic requests are sent to carry out a power loss attack on resource constraint IoT devices which prevents the device from entering sleep or energy-saving mode.
3) *Hardware Malfunctioning:* IoT devices are considered as salvation for domains, such as intelligent transport systems (ITS), e-healthcare, smart homes/cities, smart grids, etc. Failure of these devices due to production fault or any cyberattack will lead to a significant impact not only on the system, but also on the lives of users as well [26], [43]. Many smart devices are highlighted by Brewster [44] that are prone to cyberattacks.
4) *Malign Data Injection:* A counterfeit device can be injected in an IoT system that can sniff the wireless

TABLE II
LAYERWISE SECURITY THREATS, VULNERABILITIES, AND CORRESPONDING SECURITY CHALLENGES ARE HIGHLIGHTED ALONG WITH PROTOCOLS BEING USED IN EACH LAYER

Layers	Technology/Protocols	Threat	Susceptibility	IoT Security challenges	Ref
Physical/ Perception	NFC,RFID Tags,ODB2, Rs-232, ModBus, PLC, RJ-45, USB	Eavesdropping	Lack of encryption	Confidentiality	H. Ning et al.
		Battery drainage attacks	No white listing and black listing, No spam control	Resource Constraintness	A. Reziouk et al.
		Hardware failure/exploitation /Device compromise	Casualness by the manufacturers, Developers fault, Unprotected interfaces, No Physical security	Lack of Standard, Physical Security	J. Wurm et al. O. Arias et al. Kumar et al.
		Malign data injection, Cloning of node	Lack of strong access control, No tamper-proofing	Integrity of Device/Data	D. Puthal et al. P. Paganini
		Unauthorized admittance to the devices	Usage of default or hard coded credentials	No standard, Integrity, Confidentiality	Thomas Brewster B.Fowler
MAC/ Adaptation/ Network	NFC, RFID, BLE, Ant, Insteon,MiMAC, WirelessHART, Wifi802.11, 3GPP (NB-IoT, eMTC, EC-GSM), LoRaWAN, Symphony Link, Weightless, SIGFOX, DASH7, Ant+, EnOcean, ZWave, ZigBee, DigiMesh	DoS attacks (collision attack, channel congestion attack, battery exhaustion attack)	Flaw in communication protocols	Availability, Heterogeneity	A. Reziouk et al. T. Borgohain et al. R. M. Savola et al.
		Eavesdropping, MITM attack	Lack of strong authentication mechanism and data security	Confidentiality/ Source integrity	D. Puthal et al.
		Storage attacks	No duplication of data storage, Centralized storage, Malware threats such as crypt locker and ransom ware	Resource Constraintness	Kumar et al.
Application	MQIT, AMQP, DDS, XMPP, PTP, Https, SEP 2.0, SSH, FTP, Telnet, COAP,	Malign codes	No application/web security, Lack of authentication and authorization mechanism	Authentication, Authorization, Integrity	A.R. Sadeghi et al.
		Escalated privileges and data tampering, SQL injection, Disclosure of private data	Weak authentication and authorization mechanism	Access control, Data Authentication, Confidentiality	Dave
		Cross Site Scripting attack	Web vulnerabilities		acunetix
Semantic	HDFS, MapReduce, Kakfa, Rapid MQ, Scribe, Luxun	Theft of Identity and compromise of user privacy	No data and application security	Identity, Leak of Private Data, Confidentiality	K. Hamlen et al.

traffic, insert bogus messages, or can downpour the wireless channel with fake messages, to make the system unavailable for normal users [45].

5) *Node Cloning:* Because of no standardization, node cloning, i.e., forging and duplication of devices, can be easily done in an IoT ecosystem [46]. It can be done in the production and operational phase. An insider attacker can swap the legitimate device with fabricated during the production phase and can also clone the device during the operational phase. Mining of security parameters and firmware overwriting can further be performed after the node cloning attack [47].
6) *Gaining Unauthorized Access to the Device:* One of the main security vulnerability trending nowadays is the usage of default passwords and built-in credentials by the producers. For example, iBaby M3S wireless monitor is available in the market with an encoded "admin" user name and a password [44]. Likewise, insecure APIs are left intentionally by the developers for remote access [48]. Such an attack was carried out on the Summer Baby Zoom WiFi camera by Fowler [49] that used encoded credentials of admin, admin.

2) MAC/Adaptation/Network Layer: Collision attack and channel congestion attack are DoS attack types carried out at this level [50], [51]. Other attacks include escalating frame counter value and spoofing of acknowledgment frames (battery exhaustion attack) [30], [52], abusing CSMA by communicating on various channels [30], [51], and rogue PANId conflict initiation. The network layer is susceptible to many attacks as it connects different private LANs. Few noteworthy

threats are eavesdropping [45], MITM, spoofing [50], message alteration attacks [45], gaining unauthorized access [26], replication of nodes [53], and injection of fake devices [54]. Furthermore, storage attack is also a potential threat to the availability of the data [26]. In addition, nodes, servers, and gateways are bombarded with fake messages to launch DoS attacks [55], [56].

3) Application Layer: Application developers, around the world, focus on the effectiveness and reliable service delivery of the product rather than focusing on security. Therefore, applications can be compromised and legitimate users are denied of authorized services, without much effort. Some main threats to the application layer are as follows.

1) *Malicious Code:* Vulnerabilities of the IoT devices are the main target of malwares that compromise the nodes with ease. The forfeited devices are further exploited as useful nodes in the form of bots to carry out the attack on other end devices/network applications [26].
2) *Weak Application Security:* Brute force/dictionary attack, the unnecessary revelation of data, escalated privileges, and data tampering can be the consequences of weak authentication and authorization mechanism. Furthermore, the IoT systems accessed via websites are vulnerable according to the OWASP application security risk ranking [57], [58]. Few major application risks are discussed in the following sections. IoT applications and databases are vulnerable to SQL injections. Belkin smart home product was exploited by Staff [59]. Malicious code can be injected in a paired WeMo Android app that can acquire full control, i.e., root-level control of connected home automation systems. Once the attacker is inside the IoT application system, the attacker can run IoT devices abnormally, e.g., keeping the lamp on for a longer period of time. Similarly, MITM attack or eavesdropping can be done to sniff the transmitted messages between the user and the Philips smart bulb [60]. Like Web-based applications, IoT systems are also susceptible to cross-site scripting (XSS) attack. Staff [59] successfully carried out an XSS attack on Belkin smart home products. This vulnerability gave an attacker the leverage to run JavaScript code in the victim's browser [61].

C. Security Challenges

There are many security challenges of IoT; however, we can summarize them in three broad categories, namely, IoT data, communication, and end applications-related security. After discussing generic and layerwise IoT threats, the following sections briefly explain the challenges of the aforementioned categories.

1) Data-Related Security: IoT applications receive a massive amount of data generated by end nodes, which can be of a personal or confidential nature. Such data are valuable gain for attackers and commercial competitors. Furthermore, the trustworthiness of the IoT services, such as personal, manufacturer, and societal rely greatly on the genuineness of the data that has an undeviating effect on its output. Apropos, for promising results from IoT services and applications, the data generated by IoT end nodes must be authentic and confidential.

1) *Confidentiality:* Due to the resource limitations of IoT nodes, generic encryption algorithms cannot be used. Thus, there is a trivial need of lightweight cryptographic ciphers that can provide optimal confidentiality in resource-constrained nodes [62], [63]. Recently, many lightweight cryptographic ciphers have been proposed, e.g., SEA [64], LBlock [65], PRESENT [66], mCrypton [67], and KATAN/KTANTAN [68]. Some researchers worked on the hardware implementation of standardized block ciphers, e.g., [69]. There is a trade-off between cost, performance, and security in different application areas of IoT [68]. For example, the security level may be low for RFID tags in electronic tickets but the demand for low power and latency is high [70]. Based on the mentioned parameters, the implementation of 52 different block ciphers was evaluated by Hatzivasilis *et al.* [71]. The classification of these ciphers was done for different embedded end nodes. Authors identified that due to the uncomplicated nature of the majority of lightweight cryptographic ciphers, they are susceptible to the side-channel analysis (SCA) attack. Fault and time base side-channel attacks on IoT-based RSA, AES, and ECC were researched by Lo'ai and Somani [72] and proposed countermeasures for it. In another effort by Zhang *et al.* [73] proposed a generic framework to investigate and assess algebraic fault attacks on lightweight cryptographic ciphers. Many studies came forward to use physical features for key generation, and in this effort, Majzoobi *et al.* [74] proposed a unique method, physical unclonable functions (PUFs) to generate keys for identification purposes. The secret is not stored in memory in fact, it is derived by PUFs using physical characteristics of ICs. It is generated without using costly hardwares [75].
2) *Authenticity:* The authenticity of the end nodes can be compromised by physical attacks, such as hijacking, replacement, node copying, etc. The authenticity of the data output as well as the integrity of the end nodes need to be verified. Hence, there must be some lightweight attestation methods designed for IoT end nodes. Software, hardware, and hybrid-based static attestation are three main techniques highlighted in the literature. The side-channel information is used in software-based attestation techniques to endorse the authenticity of end nodes without using specialized hardware. It is further split into two main classes, i.e., memory and time-based attestation. Time-based attestation techniques include SWATT [76], Pioneer [77], and SCUBA [78], whereas memory-based attestation techniques include [79] and [80]. Both software and hardware designs are used to shield against potential adversaries in a multihop network between prover and verifier, keeping the hardware changes to minimal [81]. Hybrid attestation techniques cannot guard against physical interruption with devoted secure hardware. Some of the hybrid attestation techniques are

SMART [82], SPM [83], SANCUS [84], TrustLite [85], and TyTAN [86]. Due to compromised keys, both hybrid and software-based methods cannot guard against physical attacks, as prover can be mimicked/cloned [81]. Physical attacks can be guarded only in hardware attestation. Hardware-based attestation techniques rely on purpose-built functions, such as TPM or SGX, which cannot be used in resource-constrained end devices. For this purpose, IoT uses special lightweight hardware characteristics, i.e., PUFs [87], [88]. SEDA [89] was the first proposed swarm attestation technique. Another swarm attestation proposal was put forward by SANA [90]. In the IoT environment, end nodes sometimes connect and leave the swarm dynamically like in *ad hoc* vehicular networks thus, making it harder to attest a swarm device. All the staticattestation methods stated above validate the authenticity of binaries rather than their execution [81]. C-FLAT [91] and LO-FAT [92] offered accurate attestation by manipulating attesting run time for the execution path of a program in IoT embedded end nodes.

3) Communication-Related Security:

1) *Authentication and Access Control:* Devices/users in the IoT environment and their communication exchanges require security features, such as authentication and access control [93]. However, authorization of devices requires authentication beforehand [94]. Due to the varied IoT ecosystem, diverse end nodes/sensors, varied network architecture, and above all limiting resource nature of IoT devices, lightweight access control and authentication processes need to be devised. Mutual authentication is necessary for IoT devices, due to the nonexistence of a trusted third party in a decentralized IoT environment. Both data collectors and data holders need to verify each other before collecting and handing over data in a heterogeneous environment of IoT [95], [96]. Su *et al.* [97] highlighted the privacy and security issues of RFID authentication between tags and readers. Some researchers emphasized that unlinkability and anonymity need to be deliberated for IoT application areas, such as smart healthcare, grids, and the Internet of Vehicles (IoV). Dynamic IoT devices that need a frequent change of locations call for new lightweight cross-domain authentication protocols.

3) Security for End Applications: A huge amount of data is pulled together by IoT gateways from end nodes, which is transported over different networks and operated by various IoT systems. Forensics, legal or social challenges, and privacy issues are few issues bound with data generation and transfer and usage phases. Below is a brief explanation of each issue.

1) *Privacy Concern:* User private/personal data, such as heartbeats and fingerprints, several environmental aspects sensed by end nodes can be used to deduce user preferences and tracking [98], [99]. A user can be a receiver of services and data and at the same time can be an object for data collection by different smart nodes [100], [101]. Unlike the Internet, where users actively set their privacy at risk (e.g., asking different queries for services), IoT user data are sensed and transported with their consent and knowledge [51], [52]. Apthorpe *et al.* [102] revealed that any network spectator or even ISP can deduce sensitive private residence behavior of a user by probing smart home traffic from commercially existing smart devices, which provide even encryption [103], [104]. Furthermore, another problem of overprivileged smart apps authorization also results in privacy issues [105], [106]. Astonishingly, in the e-healthcare sector, medical records and healthcare information in the black market are of higher value than credit card data [107]. Researchers have proposed pseudonym management of data [108], [109], anonymous authentication [110], [111], and access control for privacy preserving in e-healthcare data [112]. In another research [113], Rottondi *et al.* have highlighted that household behavior can be revealed in smart grids through the collection of fine-grained data by smart meters [114]. In smart grids, gateways and control centers use homomorphic encryption that utilizes the same key for ciphertexts without the need for data decryption [114]. Fan *et al.* [115], Shen *et al.* [116], and Rahman *et al.* [117] have worked on privacy sustaining aggregation techniques as user load curves per household can be used to infer individual utilization behavior or daily living habits [118]. Hence, it is imperative that the anonymity of a user must be guaranteed in the smart grid environment and inference of user's behavior and location must not be revealed from sensed data. Technologies, such as data mining and ML, which dynamically add up a business context to raw data, cause another threat to user's privacy. Keeping this in mind, extra efforts are required for user's privacy via ML and data mining techniques [53], [54].
2) *Forensics Challenges:* When IoT infrastructure is the target or used to carry out an attack, it will call for forensic investigations in the IoT ecosystem. Data sensed and made communal by IoT application will introduce opportunities and challenges for forensic investigation. Due to the resource constraints of memory, evidence needs to be shifted to cloud or local centers before overwriting in IoT devices. Therefore, researchers have recognized IoT forensic as a mixture of cloud, network, and device-level forensics [119]. Main forensic challenges in the IoT paradigm are: a) resource-limited characteristic of devices; b) heterogeneous characteristic of devices; and c) the growth in numbers and types of devices [120], [121]. A general digital forensic investigation framework DFIF-IoT [122] was presented to homogenize digital investigation procedures. To simplify the procedure of evidence compilation, analysis and preservation were proposed by FAIoT [120]. The combination of 1-2-3 zones and the next best thing (NBT) model was presented by Oriwoh *et al.* [123]. When investigating and correlating the composed evidence, which may have individual personal information, privacy is another important element that needs to be addressed in the forensic investigation of IoT. Privacy-aware

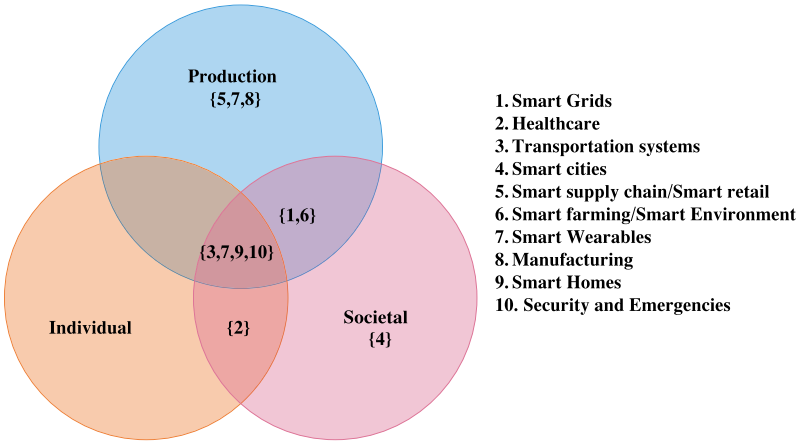


Fig. 4. Convergence of IoT systems.

TABLE III
SUMMARY OF IOT APPLICATIONS CORE SECURITY REQUIREMENTS, WHERE (✓) REPRESENTS THE REQUIREMENT THAT ARE OF UTMOST IMPORTANCE AND (X) SHOWS THE TRIVIAL REQUIREMENTS

IoT APPLICATIONS	Availability	Confidentiality	Integrity	Non -Repudiation	Privacy	Authentication
Smart Grids	✓	✓	✓	✓	✓	X
Healthcare	X	✓	✓	X	✓	✓
Transportation Systems	✓	X	X	✓	✓	✓
Smart Cities	✓	✓	✓	X	X	✓
Smart Manufacturing	✓	✓	✓	X	X	✓
Smart Homes	✓	✓	✓	X	X	✓
Smart Wearables	X	✓	✓	X	✓	✓
Smart Farming	✓	X	X	X	X	✓
Smart Supply Chain	✓	✓	✓	X	✓	✓
Smart Security Systems	✓	✓	✓	X	✓	✓

IoT forensic (ProFIT) is an effort in proposing a privacy-enabled forensic model for IoT [124]. In the ProFIT model, evidence can be gathered with the help of nearby end devices which adds in reconstructing the crime scene context to a much accurate level. To the best of our knowledge, we can deduce from the literature studied that IoT forensics is still evolving and most of the researchers are stretching the existing traditional methods for IoT forensics. Even though to some extent traditional forensic tools can be used in the IoT environment, still a complete framework for IoT forensics is lacking.

3) *Social or Legal Challenges:* Below are the two main issues raised due to IoT adaptation in recent years.
   a) *Liability Dispute:* New legal responsibility arguments are raised due to the introduction of smart/intelligent services provided by IoT. A smart vehicle is one such example, which is progressively put into operation. Every time an accident is met due to smart/automated vehicle, it calls for updated legislation for its usage. To support automated vehicles, Australian National Transport Commission has outlined fresh Australian driving law [125].
   b) *Data Commodification:* The pooling and treatment of bulk of data, make it a commodity creating another problem of ownership of data, which in turn arises few questions, e.g., how managing the data as a product be standardized? who is the proprietor/owner of the data? and is the trading of data possible? Legal responsibilities and concerns are invoked due to these questions. Authorization and revocation of authorization for data collection must be the right of data owners. Data owners/holders can share the portion of data which can be shared with the IoT ecosystem by applications through granular authorization based on context.

D. IoT Applications Security

IoT has enhanced the quality of lives in many fields, such as smart grids, healthcare, transportation system, cities, supply chain, farming, retail, wearables, environment, manufacturing, homes, security, emergencies, etc. Although there could be much more application of IoT, we have categorized them in ten application domains, endeavoring to create an optimal balance between generality and concreteness. These domains are such varied that they can mask all requirements of user groups.

Furthermore, it can be observed that these ten application systems are distinct yet overlapping from the users' point of view, and for this purpose, we have further categorized them into three groups, namely, individuals, societal, and production as shown in Fig. 4. Furthermore, two security challenges are

TABLE IV
SUMMARY OF IOT APPLICATIONS SECURITY CHALLENGES. (✓) REPRESENTS THE CHALLENGES WHICH NEEDS DUE ATTENTION FROM ACADEMIA AND INDUSTRY FROM PRELIMINARY DESIGN STAGES OF SMART DEVICES TO END PRODUCTS, WHEREAS (X) SHOWS THAT THE CHALLENGE IS SIGNIFICANT BUT CAN BE GIVEN LESS ATTENTION DUE TO SPECIFIC IOT SYSTEM

IoT Applications	Heterogeneity	Scalability	Information Vulnerabilities	Data Sensitivity	Privacy	Resources limitations	Mobility	Physical Attacks	Lack of Standardization	Safety challenges
Smart Grids	√	√	√	√	√	X	X	X	X	X
Healthcare	√	X	X	X	X	√	√	X	X	X
Transportation Systems	√	X	X	X	X	X	√	X	X	X
Smart Cities	√	√	X	√	X	X	X	X	X	X
Smart Manufacturing	X	√	X	X	X	√	X	√	√	√
Smart Homes	√	X	√	√	X	X	X	X	X	X
Smart Wearables	√	√	√	√	X	√	X	√	X	√
Smart Farming	√	√	X	√	X	√	X	X	√	X
Smart Supply Chain	√	√	√	√	X	√	X	X	√	X
Smart Security Systems	√	√	X	√	X	√	X	√	√	X

highlighted, which are common for all IoT application areas. The two common security challenges are: 1) vulnerabilities of social engineering and 2) legislation challenges.

Below, we have abstracted the most crucial security requirements (*availability, confidentiality, integrity, nonrepudiation, privacy, and authentication*) and challenges (*heterogeneity, scalability, information vulnerabilities, data sensitivity, privacy, resources limitations, mobility, physical attacks, lack of standardization, and safety challenges*) for the ten IoT application domains stated above. Summary of the security requirements and challenges are depicted in Tables III and IV, respectively.

IV. GAP IDENTIFICATION AND ANALYSIS: NEED FOR STANDARD AND SECURE IOT FRAMEWORK

In the future, the technological era will witness a massive increase in the number of connected devices. The cybercriminals will always mark them as the first choice of attack due to the weak embedded security mechanism and the absence of a standardized architecture. Such devices can be used as bots by attackers to launch the DDoS attack and spread spywares. It is apparent from the modern cyberattacks carried out on these connected devices that current security standards and protocols for IoT have failed in providing security to IoT devices [24].

Current communication protocols have some built-in security features to secure communication at different layers of the IoT protocol stack as shown in Fig. 5. However, different device attacks, such as code modification and malwares cannot be secured with these communication protocols [27], [30]. In reality, taking into account the huge number of IoT connected devices and their threats as discussed in Section III, there is a need for a comprehensive security framework and standardization of IoT.

Apropos an adaptive, novel, and worthy security system is required to tackle the current situation, which should be proactive in nature providing baseline security to end users, network, applications, data, and devices. Therefore, to detect the present-day threats, envisage future security incidents, and to quickly respond to the attack, there is a need for crisp guidelines providing ground for the development of a secure adaptive IoT framework. In this regard, the best practices of organizations, such as Cisco, TCG, IBM Watson IoT and AT&T, and TCG can be reviewed and consulted for a unified framework of IoT security.

A. Network-Level Security Approach for IoT

IoT producers are launching the products with innovations and ease of use to grab the market share without paying due attention to the security. Due to this dilemma and the limited resources of IoT devices, the conventional host-based protections, such as anti-virus, IDS, IPS, etc., cannot be used for smart devices. Therefore, a network-level security architecture is proposed by Yu *et al.* [33] to secure smart devices. The secure system is based on an SDN controller called IoT SENTINEL, a security gateway that is efficient enough in identifying different types of devices connected to a network. Furthermore, the system eliminates potential vulnerabilities by applying mitigation measures. A vulnerability database module is also placed in the IoT SENTINEL controller. ML techniques are adapted for flagging a device as benign or malign. Device type identification along with vulnerability databases' input are fed to the ML module, which can infer

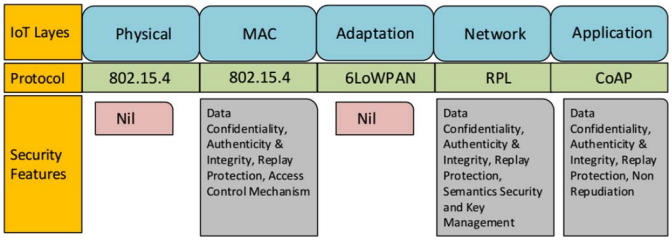


Fig. 5. Security features offered by IoT communication protocols.

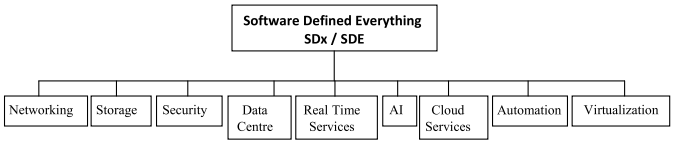


Fig. 6. Classification of software-defined everything.

devices that are vulnerable in a network. Due to the global visibility of the network, such solutions are viable for the smart ecosystem, which can take decision at the network level.

B. Necessity of the SDN-Based IoT Environment

The increased use of mobile/smart devices, server virtualization, and the introduction of cloud services have provoked the networking industry to reconsider the traditional network architectures.

Due to certain traditional networking limitations, such as closed equipment, protocol standardization, few people who could innovate, expensive operation of networks, and buggy software in the equipment, it is impossible to meet current market requirements with such limited traditional network architectures [126], where the network cannot change dynamically according to the network conditions.

These shortcomings lead to the idea of having an OS for the network, which should have a standardized control interface that speaks directly to the hardware [127], [128]. To tackle with the control and management challenges in the conventional networks/platforms, software-defined systems (SDSys) are proposed, which conceal the complexities of traditional networking from the end users, i.e., separating the data plane from the control plane [129]. The SDN is considered a revolutionary network technology in supporting heterogeneous networking with rapid evolution and dynamism using programmable planes (control and data plane). The SDN and IoT integration can meet the expectation of control and management issues in diverse scenarios [16], [17].

V. Software-Defined Security Solutions

A number of domains, such as networking (SDN), security (SDSec), data centers (SDD), storage (SDStor), etc., have merged in the rapidly growing SDSys technology as shown in Fig. 6. These are all components of a wide trending technology that is called software-defined everything also known as SDx/SDE.

Manageability, dynamism, cost effectiveness, and adaptability are few major properties of SDN that make it highly suitable for the high bandwidth and dynamic nature of

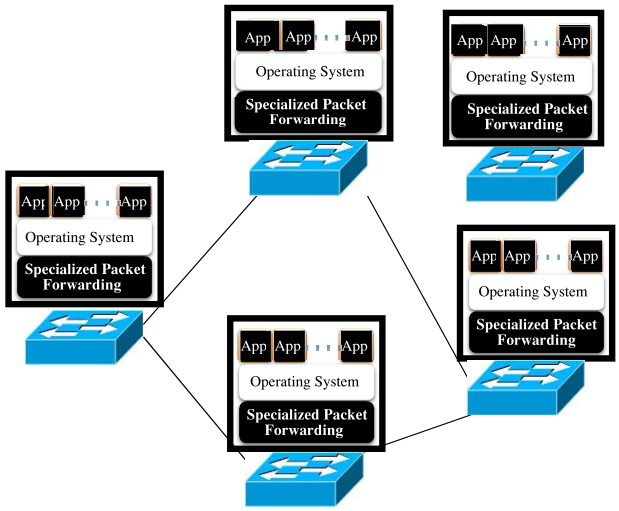


Fig. 7. Closed network. Devices with million lines of source code for different networking features/OS and billions of gates for specialized packet forwarding hardware. It is difficult to modify proprietary code or add innovations.

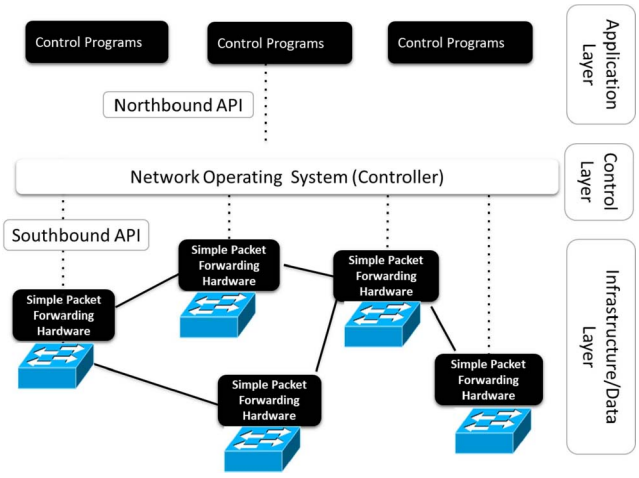


Fig. 8. The intelligence is abstracted from networking devices and placed in a remote programmable controller that has the control of devices forwarding decisions. The SDN architecture is depicted three layers and two communication interfaces.

today's applications [126], [130]. This architecture enables abstraction of the underlying infrastructure for network services/application and the network control to be directly programmable by decoupling the network control and forwarding functions.

A logical view of the SDN architecture is depicted in the Fig. 8, where it is highlighted that the control plane from physical devices as shown in Fig. 7, is shifted to programmable controllers. In software-based controllers, the network intelligence is (logically) centralized, which upholds a global view of the network. This results in presenting the network as a single, logical switch to the applications and policy engines [131], [132].

Network design and operations are made simpler with SDN single logical point that enables enterprises and carriers to acquire vendor-independent control over the entire network. Networking devices are also made simplified with SDN as

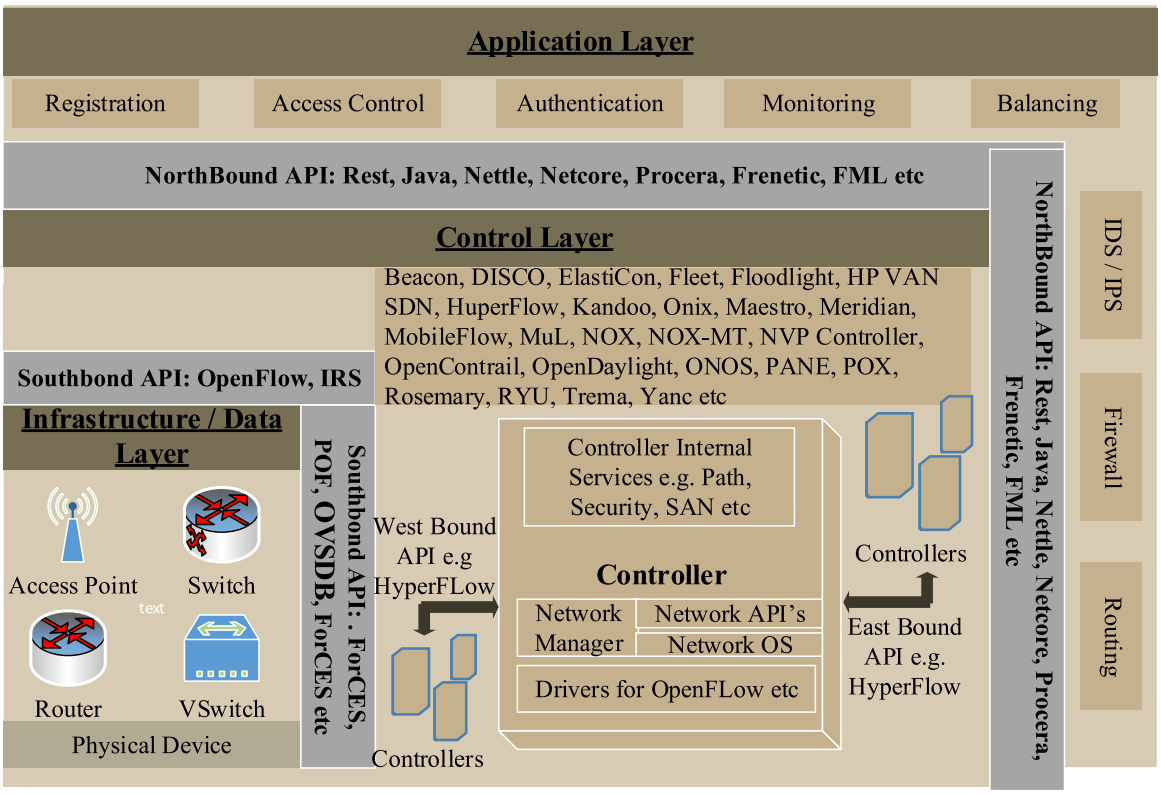


Fig. 9. SDN protocol stack. At different levels, the SDN provides different sets of protocols. Security services, such as IDS, IPS, and DPI can be performed on the go without dedicated appliances as was in traditional networking.

they do not need to be familiar with and process thousands of protocol standards but simply allow instructions from the SDN controllers. The following section briefly highlights the SDN architecture.

A. SDN Architecture

We present a generalized SDN architecture and a consolidated layered SDN protocol stack as shown in Fig. 9. There are three layers in the SDN controller, i.e., infrastructure layer, control layer, and application layer. These layers are interconnected by two communication channels, i.e., southbound interface (SBI) and northbound interface (NBI), whereas east and southbound interfaces are used for connecting different controllers.

The infrastructure layer manages the devices, such as routers, switches, vswitches, and access points connected to it. Through open interfaces such as Openflow [56], these devices are managed as they have no built-in control/software and act just as forwarding elements. The controller computes and allocates flow rules that are stored in the flow table inside these devices. Packets are forwarded to concerned destinations based on the flow rules in the flow table [132].

The application layer accommodates all third-party applications written for a specific purpose and operates on a higher level than the controller. Underlying devices in the infrastructure layer are connected to the application via the controller. The NBI bridges the communication between controllers and applications and *vice versa* [130]. Some of the most frequently adopted third-party applications are routing, access control, network virtualization, application security, network monitoring, IDS/IPS, traffic engineering, etc.

As depicted in Fig. 9, the control layer makes up the core modules that are network manager, network APIs, network operating system (NOS), drivers, and internal services. These major functionalities should be in any simple/basic controller [133]. Installation of flow rules onto the underlying devices is the responsibility of the controller. Through the OpenFlow protocol [56], [132], the forwarding devices communicate with the controller. Whereas, REST API is most widely used for communication between the controller and the third-party applications.

Many controllers are available, but the most famous controllers are RYU [134], ONOS [135], Open Daylight [136], Floodlight [137], NOX [138], and POX [139]. Karakus and Durresi [140] highlighted multiple-topology approaches to deploy controller(s) in the SDN, i.e., centralized controller designs, distributed controller designs, hierarchical controller designs, and hybrid designs. The SDN controller in a control plane is interacted by four different interfaces, which are explained as follows.

Soutbound Interface: It assists in controlling the network behavior through flow entries on the devices. Many SBI APIs exist, such as OpenFlow, IRS, ForCES, POF [141], and Open vSwitch Database (OVSDB) [142]. However, the OpenFlow protocol is the most widely used interface due to its open architecture. The open networking foundation (ONF) considers it the *de facto* standard for the SDN architecture [132].

TABLE V
SUMMARY OF SDN-BASED IoT DEPLOYMENT MODELS DEPICTING CENTRALIZED ARCHITECTURES, ITS IMPLEMENTATION, AND PURPOSE

Centralized Models				
Ref	**Year**	**Proposed Model**	**Implementation**	**IoT Application Area**
Z. Qin et al.	2014	Flow scheduling algorithm is designed for heterogeneous networks to vigorously attain distinguished quality	Qualnet simulation platform	Heterogeneous wireless networking environment
J. Li et al.	2015	A general model of SDN/NFV based IoT architectures is presented with emphasis on highlighting the characteristics of these technologies	Proof of concept	General purpose
Y. Jararweh et al.	2015	Introduced SDN and SDStor modules to cater data management related traditional IoT system challenges	Proof of concept	General purpose
M. Ojo et al.	2016	Introduced NVF coupled with SDN to overcome scalability, elasticity and dynamism properties of heterogeneous IoT networks	Proof of concept	General purpose
I. Bedhief et al.	2016	Dockers are used to manage different smart devices in heterogeneous environment	Mininet simulation of small network with 4 devices	Generic
M. Tortonesi et al.	2016	SPF, an SDN middleware model, is presented for processing the raw data collected from IoT devices on the edge node	Prototype/Simulation in mininet only	Urban area small network
Y. Li et al.	2016	Authors proposed that new services can be offered promptly with their architecture. Multi services support in different domains with different scenarios is presented where smart devices and data can be reprocessed	Campus network deployment	Heterogeneous wireless environment
W. Cerroni et al.	2017	A reference architecture motivated by the ETSI MANO framework is proposed. An intent-based north bound interface for end-to-end service orchestration across multiple technical domains is presented	Mininet simulation only	Smart homes, office
D. Sinh et al.	2018	An architecture is proposed for IoT wherein SDN/NFV orchestrates the complete network via SDN controller	Simulation in mininet only	Small WSN like: home, office etc
Y. Wang et al.	2018	IoT communication application is proposed that merge SDN with publish/subscribe paradigm, with an aim to ease smart applications/ services	Deployed in Heating Control and Information Service System. Simulated in Mininet	Smart homes, office

TABLE VI
SUMMARY OF SDN-BASED IoT DEPLOYMENT MODELS DEPICTING DECENTRALIZED ARCHITECTURES, ITS IMPLEMENTATION, AND WORKING ENVIRONMENT

Decentralized Models				
Ref	**Year**	**Proposed Model**	**Implementation**	**IoT Application Area**
O. Flauzac et al.	2015	Multiple controllers are used to connect different IoT domains using SDN architecture in equal interaction mode	Proof of concept	Smart Home/ campus network
F. Olivier et al.	2015	A SDN-based new network architecture with multiple controllers is presented for Ad-hoc networks and IoT	Proof of concept	Ad Hoc Network
D. Wu et al.	2017	Leveraging SDN/NVF to deploy urban scale heterogeneous IoT by dividing it into different geographic divisions	OMNeT++ simulation	Urban area

Northbound Interface: The communication channel between the application layer and the controller is NBI. Applications communicate with the controller to access network control for managing services and gathering information, such as state and services from the network [140]. REST API is adopted by the majority of controllers [143]. Java API, Frenetic [144], NetKAT [145], NetCore [146], and Pyretic [147] are few other protocols that are used as NBIs.

B. SDN-Based Secure IoT Frameworks

This section presents a detailed description of the various security mechanism/framework for the SDN-based IoT deployment. However, before moving further, it is essential to highlight various IoT deployments leveraging the SDN architecture in order to acquaint the readers with different deployment models and the future scope of IoT by adopting this new technological paradigm. The following sections discuss the SDN-IoT deployment models followed by SDSec-based solutions for IoT.

1) SDN-IoT Deployment Models: To the best of our knowledge, we have presented a consolidated overview of the models put forth by the academicians till now. Tables V and VI present the summary of deployment models of the SDN-based IoT. In SDN, IoT systems can be implemented in one of the two ways, i.e., centralized and decentralized controller architecture as depicted in Fig. 10. The following sections discuss the IoT deployments in both architectures.

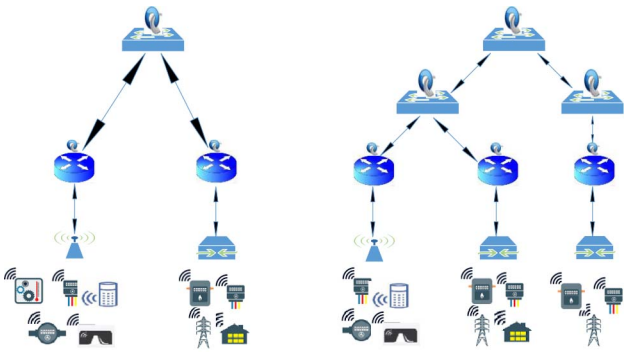


Fig. 10. SDN-IoT implementation techniques. (a) Centralized controller. (b) Decentralized controller. The centralized controller provides easy maintenance but encounters a single point of failure. The decentralized approach addresses the single point of failure; however, it faces the problem of consistency.

Centralized Controller Architecture: SDN is an evolving paradigm and yet is not utilized to the fullest, therefore many proofs of concepts are presented to augment the need for SDN-based IoT deployment. Li *et al.* [148] presented

an overview of the IoT, SDN, and NVF architectures and proposed a generalized model of SDN-IoT leveraging NVF. To make the IoT management process simple and to cater to the generated data challenges in the traditional IoT architecture, such as forward, store, and security, a software-based integration of the SD network, SD storage, and SD security is proposed by Jararweh *et al.* [149]. Similarly, Ojo *et al.* [150] proposed a basic and all-purpose SDN-IoT architecture together with NFV application with explicit options on how and where to embrace SDN and NFV technologies to overcome the challenges of the IoT.

Qin *et al.* [151] designed a software-defined methodology for the IoT ecosystem to vigorously attain distinguished quality levels of different tasks in heterogeneous scenarios. Furthermore, Bedhief *et al.* [152] presented an SDN-Docker-based architecture catering to the heterogeneity at the network and device level. It provides an easy and fast mode to deploy the IoT application because it virtualizes the OS without the overhead and also extends portability features. Furthermore, Tortonesi *et al.* [153] introduced the sieve, process, and forward (SPF) model that expands the reference architecture of ONF by swapping the information processing and dissemination plane with the SDN data plane. Programmable information processors are positioned at the IoT edge and through the proposed SPF model, IoT applications and services are defined and managed.

Likewise, Sinh *et al.* [154] proposed a combination of SDN/NFV technologies for IoT deployment and proposed a mechanism to meet the obligations of deploying IoT services from different providers via slicing end-to-end network fragments. Furthermore, their mechanism can recover an IoT service when it is down. Cerroni *et al.* [155] projected a reference architecture that is basically motivated by the ETSI MANO framework. An intent-based northbound interface for end-to-end service orchestration across multiple technical domains is presented. IoT systems are connected by SDN to the relevant cloud-based services.

Li *et al.* [156] offered SDN-based IoT architecture, in which gateways, devices, and generated data can be programmed by service operators and application developers. Furthermore, interoperability and data provisioning features are also supported at different levels. An amalgamated communication middleware solution SDNPS (an SDN-based publish/subscribe system) for IoT services is proposed by Wang *et al.* [157]. They have merged SDN with publish/subscribe (topic oriented) middleware, which can assist customers of varied smart services to access network along with relieving hassle for service providers and application developers to administer and enhance IoT applications.

Decentralized Controller Architecture: Flauzac *et al.* [158] proposed distributed controller-based SDN network architectures that can be adopted in *ad hoc* and IoT network. The new architecture works in equal interaction with multiple SDN controllers. It is also scalable with several SDN domains that can be or without network infrastructure, where the controller is accountable for that domain. A border controller is introduced to bridge the communications between domains. Olivier *et al.* [159] deliberated the SDN-based architectural design for access control and global traffic observation for *ad hoc* networks and discussed their performance consequences.

Wu *et al.* [160] introduced UbiFlow, a ubiquitous flow control and mobility management software-defined IoT system, for multinetworks. The UbiFlow works on multiple controllers to distribute urban-scale SDN into geographic divisions. To maintain network consistency and scalability, a distributed hashing overlay structure is put forward. A new IoT architecture is presented by Tomovic *et al.* [161], which merges the advantages of two evolving technologies: 1) SDN and 2) fog computing. The SDN augments resource management and traffic control implementation of complex mechanisms, whereas fog computing supports network edge-level data management and analysis, therefore delivering provision for applications with low and foreseeable latency.

2) SDSec Mechanisms/Frameworks for SDN-IoT: In this section, we present the SDSec solutions for enabling secure IoT systems. Although, this domain is still in its infancy, however, there are few research efforts, which are elaborated in the following sections.

Dos/DDos Solutions: To counter the Dos attack, one of the very first effort is proposed by Al-Ayyoub *et al.* [162] that incorporates (trust, zone-ID, permissions, and scope) parameters in the host and all security techniques are delegated to the SDSec controller to check an incoming packet against the defined parameters. Such a solution is viable for small-scale networks, however, it can be a bottleneck for large-scale networks as all intelligence is abstracted from the underlying layer and summed up in one controller. Bull *et al.* [163] introduced the idea of a flexible flow-based security mechanism using SDN gateway for monitoring the traffic, which is initiated and directed to IoT devices. This gateway can detect anomalous behavior and perform an appropriate response, such as blocking, forwarding, or applying QoS.

Bhunia and Gurusamy [164] proposed an IoT security framework leveraging SDN as a gateway called SoftThings. The main objective is to monitor IoT traffic at the edge of the network despite the core network for detection and mitigation of anomalous behavior. ML techniques are used to detect abnormality in the traffic. SLICOTS is a mechanism proposed by Mohammadi *et al.* [165], for countering the TCP SYN flooding attack in SDN. The SLICOTS module resides in the controller and leverages the dynamic programmable feature of SDN to monitor TCP connection requests and detect and prevent TCP SYN attacks.

Bawany and Shamsi [166] introduced the SEAL framework that adopts SDN key features to improve the security and resilience of an IoT system. The SEAL framework has three modules that can effectively detect and mitigate DDoS attacks on application servers and network resources. It promises reliability, scalability, and fault tolerance in the smart city applications. In addition to the estimated-weighted moving average scheme is used to achieve adaptability. A summary of Dos/DDoS security solutions is depicted in Table VII.

Data and Communication Security Solutions: Chakrabarty *et al.* [167] introduced Black SDN to secure the SDN-based IoT network communication from traffic

TABLE VII
SUMMARY OF DOS/DDOS SECURITY SOLUTION FOR IOT: MECHANISM, IMPLEMENTATION TECHNIQUE, AND LIMITATIONS

DoS/DDoS Security Solution					
Ref	**Year**	**SDSec Solution**	**Mechanism**	**Implementation**	**Limitations**
M. Al-Ayyoub et al.	2015	SDSecurity	Security policies are embedded in controller to check in-coming packets against defined parameters to detect anomaly	Mininet simulation only, no real world implementation	Suitable for small network. Bottleneck for large networks
P. Bull et al.	2016	Flow Based Security	A secure flexible method for IoT devices is proposed through SDN gateway to counter flooding attacks using flow rules	No real IoT scenario defined. Mininet simulation only	Static rules are used, not suitable for adaptive environments
Y. Jararweh et al.	2017	SoftThings	Machine Learning approach is used at the SDN gateway to detect and mitigate abnormal traffic behavior at the gateway/network level	Mininet Simulation only using basic ML technique	Limited to TCP and ICMP packets only. Limited number of packets are addressed for simulation
R. Mohammadi et al.	2017	SLICOTS	SLICOTS: A lightweight module for defense against SYN flooding attacks, residing at the network edge	No real world scenario is considered, only mininet simulation	Limited to TCP SYN attack only, large number of packets can cause controller overload
N. Z. Bawany et al.	2019	SEAL	SEAL framework is designed with three different modules to meet application wise precise security criteria for detection of DDoS attacks using EWMA filters	Mininet simulation only	Traffic generated for result analysis is in controlled environment

analysis and inference attacks. Authors have suggested using an SDN controller as a middlebox for encrypting the header, metadata, and payload at the network layer of the IEEE 802.15.4 LR-WPAN. The Black SDN aims at protecting IEEE 802.15.4 traffic by introducing symmetric encryption along with a complicated routing algorithm, thus, trading off the efficiency of the network.

Flauzac *et al.* [158] presented a secure networking architecture for *ad hoc* and IoT networks, utilizing SDN with multiple controllers in equal interaction mode. It is scalable with manifold SDN domains, where every domain controller is accountable for its domain. Furthermore, border controllers are introduced to regulate the communications between domains. The border controller works in distributed interaction to assure domain independence in case of failure. The whole network security is augmented with the concept of a grid of security implanted in the individual controller to counter attacks.

Similar to simplify the IoT data management process, Jararweh *et al.* [149] proposed to integrate SDN, SDStor, and SDSec in one control model to achieve security. Gonzalez *et al.* [168] presented a cluster network of 500 devices using SDN augmenting network virtualization and OpenFlow technologies. The proposed system handles the communication between clusters through a cluster head with predefined rules, based on IP headers managed by an SDN controller. Gonzalez *et al.* [169] presented a new mechanism based on SDN architectures utilizing ARP requests to regulate and secure *ad hoc* network information exchanges. Preinstalled flows are used for routing the communication between controllers and devices.

Middlebox-guard (M-G) is presented by Liu *et al.* [18], which is an SDN-based data transfer security model that trims down network latency and manages data flows to ensure the network run securely. The proposed data flow management protocol determines the correct route by checking the status of a packet. Furthermore, to safeguard middlebox from turning into a hotspot, M-G proposes an offline integer linear program (ILP) algorithm to handle switch capacity limitations. Moreover, a lightweight scheme for remote attestation of the software is put forward by Conti *et al.* [19] named as CENSOR. It ensures the integrity of the software that is being run by IoT devices to attain secure application services for achieving specific goals in the network. A summary of data and communication security solutions is depicted in Table VIII.

Privacy Solutions: Smart IoT devices are exposed to confidentiality and data privacy issues due to insecure Web applications and APIs such as in the case of Philips Hue Smart Bulb [60]. The data exchange is via HTTP in plain text and an attacker can eavesdrop on the insecure transmitted data between the user and bulb. Furthermore, the attacker can mark himself as a legitimate user in the list extracted from the Ethernet bridge as shown in Fig. 11. To counter such attack, Sivaraman *et al.* [60] proposed an external third-party module known as security management provider (SMP) that enables network-level security solutions utilizing SDN architecture, unlike the traditional solution, which focuses on enhancing device embedded security. The SPM can recognize and quarantine device-level threats at the network level. SPM offers security as a service to smart-home devices.

Gheisari *et al.* [170] proposed a mechanism, IoT-SDNPP, for preserving privacy in smart cities. It divides the smart devices into two distinct classes via clustering techniques. If the device is with privacy tag up, the controller sends a

TABLE VIII
SUMMARY OF DATA AND COMMUNICATION SECURITY SOLUTIONS FOR IOT: MECHANISM, IMPLEMENTATION TECHNIQUE, AND LIMITATIONS

Data and Communication Security Solutions					
Ref	**Year**	**SDSec Solution**	**Mechanism**	**Implementation**	**Limitations**
Chakrabarty et al.	2015	Black SDN	Introduction of symmetric encryption to secure 802.15.4 IoT devices communication, meta data and payload at the link and network layers	Simulated on Black Network	Degraded network performance with the introduction of encryption, suitbable for small networks
Flauzac et al.	2015	Border Controller	Border controller are presented to secure Ad-hoc and IoT networks, using SDN with multiple controllers in equal interaction mode	No implementation or simulation, just proof of concept	Computational overhead is introduced, may cause performance bottleneck
D. Sinh et al.	2015	SDIoT	Combining SDN, SDStor, and SDSec into one controller to yield better results	Only proof of concept without implementation or simulation	Complex scheme presented for large networks. Performance bottleneck for single controller
C. Gonzalez et al.	2016	SDN-IoT Cluster	Controlling clusters by leveraging SDN cluster head communication with predefined rules based on IP headers	Simulation is being carried out on mininet	Fixed cluster communication mechanism with static rules defined via IP headers only
C. Gonzalez et al.	2016	SDNCH	A routing protocol that can manage routing in Ad-hoc networks using ARP requests in SDN clustered network with pre-installed flows	Simulation is being carried out on mininet	Fixed communication based on ARP request pre-installed rules
Y. Li et al.	2018	Middle Box Guard (M-G)	SDN-IoT based middle box (M-G) is introduced to manage data flows by inspecting packet status for security and stability	Mininet simulator is used only, no real world implementation	Complex algorithms are used for packet inspection causing performance bottleneck
M. Conti et al.	2019	CENSOR	SDN assisted cloud-enabled secure IoT network architecture is proposed for software attestation and communication security	Mininet simulator is used only, no real world implementation	Cloud/Fog/SDN enabled complex security solution is proposed without catering real world smart system traffic

message to a smart device for encrypting all messages through a specified encryption algorithm, else if the smart device is not privacy enabled, it does not use any encryption. No real-world implementation or simulation is performed by the authors.

Likewise, to augment privacy in smart cities, another approach is put forwarded by Gheisari *et al.* [171]. Here, the SDN controller takes the decision grounding on the IoT devices, data sensitivity level, and attributes of the routes for categorization of devices as normal or privacy preserving. Furthermore, the privacy-aware devices split their sensitive data and route it through the VPN mechanism. A summary of privacy solutions is depicted in Table IX.

Anomaly Detection Solutions: Vilalta *et al.* [172] proposed an SDN-enabled secure architecture for IoT devices. The mechanism encompasses an algorithm to detect anomaly detection based on statistical analysis. For this purpose, ADRENALINE and IOTWORLD testbeds are used for simulating IoT network, running on SDN/NFV edge node. The proposed mechanism targets to defuse identified attack patterns by preinstalled flow entries in the flow table. Similarly,

TABLE IX
SUMMARY OF PRIVACY SOLUTIONS FOR IoT: MECHANISM, IMPLEMENTATION TECHNIQUE, AND LIMITATIONS

Privacy Solutions					
Ref	**Year**	**SDSec Solution**	**Mechanism**	**Implementation**	**Limitations**
Sivaraman et al.	2015	SMP	Designing a security solution (SPM) that develops, customizes, and delivers extra security to IoT smart home users at the network level	Implementation on Campus Network and Home Network using real world testbed	Limited to Hue Bulb and Nest smoke alarm, more smart devices may be introduced to check the efficacy of the solution
Gheisari et al.	2018	IoT-SDNPP	The authors presented IoT-SDNPP, where privacy is conserved in the smart city, IoT device by varying the privacy behavior dynamically	Visual studio.Net CSharp version 2018 is used. No	No real world simulation or implementation is carried out, furthermore mechanism is not explained
M. Gheisari et al.	2019	Context-aware privacy	Context-aware privacy preserving smart cities mechanism is presented by authors to differentiate sensitive and non-sensitive data based on the smart devices.	Simulations are carried out using mininet wifi with six devices	This mechanism may work for small network but is not suitable for large networks

TABLE X
SUMMARY OF ANOMALY DETECTION SOLUTIONS FOR IoT: MECHANISM, IMPLEMENTATION TECHNIQUE, AND LIMITATIONS

Anomaly Detection Solutions					
Ref	**Year**	**SDSec Solution**	**Mechanism**	**Implementation**	**Limitations**
R. Vilalta et al.	2016	Secure SDN-IoT	SDN/NFV edge node, SDN controller and an E2E security application modules are orchestrated to detect and mitigate anomalies by pre-installed flow entries in the flow table	IoTWorld Testbed and the ADRENALINE testbed is used to carry out experiments	Proposed solution is suitable for small scale SDN-IoT, may cause performance bottleneck in large networks
Miettinen et al.	2017	IoT SENTINEL	IoT SENTINEL is proposed to identify vulnerable devices by device type identification and information from the vulnerable databases	Simulations are carried out using mininet along with real world tests	Software updates are not considered in the identification of vulnerable devices, only vulnerable databases are considered
Sharma et al.	2019	SHSec	A SDN based middleware architecture is presented to assess network performance and viability using link failures. The proposed model is evaluated on various metric parameters. It protects against threats and mitigate network security attacks	No real world experimental testbed, simulations are performed on mininet simulator	Results are generated using controllerd environment which resulted in high accuracy and sensitivity. Real traffic needs to be included for validation of results

IOT SENTINEL is proposed by Miettinen *et al.* [173] to efficiently identify different types of IoT devices automatically by device model and software version. It also neutralizes the communication of vulnerable devices from further propagation in the network. Vulnerable devices are identified by device type identification and information from vulnerable databases.

Sharma *et al.* [174] presented an SHSec-SDN-based architecture that can effectively and concisely manage and secure the smart home IoT. SHSec acts as a middleware to provide interoperability to varied resource-constrained devices. It protects against threats to mitigate network security attacks. A summary of anomaly detection solutions is depicted in Table X.

General Security Solutions: The identification and authentication schemes are proposed by Salman *et al.* [175] for heterogeneous IoT networks based on the SDN architecture. Different technologies reliant device identities are brought into a shared identity working on virtual IPv6 addresses, for authenticating devices and gateways. Khan and Hameed [176] have highlighted security management challenges in IoT, and to deliver security services, an SDN-based management framework is proposed by researchers. The proposed mechanism

TABLE XI
SUMMARY OF GENERAL SECURITY SOLUTIONS FOR IOT: MECHANISM, IMPLEMENTATION TECHNIQUE, AND LIMITATIONS

General Security Solutions					
Ref	**Year**	**SDSec Solution**	**Mechanism**	**Implementation**	**Limitations**
Salman et al.	2016	Identity Management	An identity-based authentication scheme for heterogeneous IoT networks using SDN is designed, that is validated by AVISPA and SPAN tool	Simulation is performed in mininet whereas SPAN and AVISPA tools are used for validation	Complex solution for low processing nodes, causing procssing over head
Khan et al.	2017	SDN-IoT	Designed a framework for provisioning of trust, key management, privacy, authentication and security attack mitigation services to IoT systems	No implementation or simulation, just proof of concept	Overall overhead and resource consumption are not considered
Farris et al.	2017	SDN-NFV based IoT	SDN-NFV based security service orchestration have been proposed to provide security to IoT	No implementation or simulation, just proof of concept	Scalability is not kept as consideration of the smart systems
Budakoti et al.	2018	Middleware IoT for SDN	A lightweight IoT Middleware solution is presented which augment interoperability between varied devices like sensor, nodes, and mobile phones that transfer data on different networks using various protocols	Real world testbed is created using laptop and different sensors	Suitable for small scale SDN-IoT systems, scalability is not considered

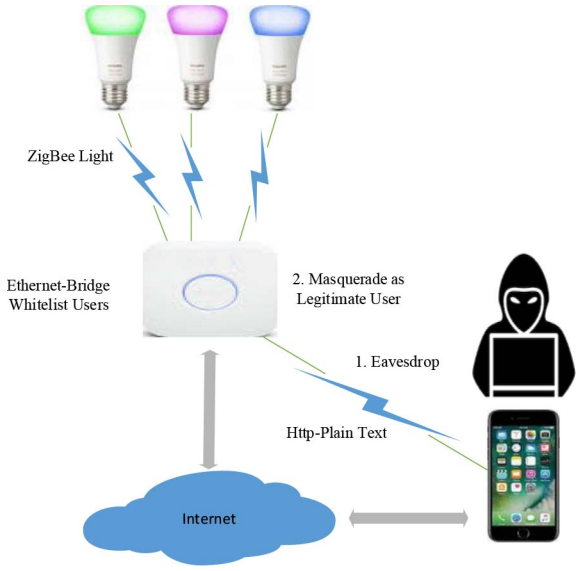


Fig. 11. Smart Philip bulb attack pattern. This scenarios explain how an attacker can eavesdrop the insecure small IoT home network.

consists of a centralized controller with trust, key management, privacy, authentication, and security attack mitigation module.

Farris *et al.* [177] presented a new framework that can effectively combine security features supported by NFV and SDN to augment IoT implementation scenarios. An orchestration module is designed to assist different communication technologies for achieving the desired objectives by applying predefined policies and provide a reactive response to unexpected behavior. Furthermore, two case studies have been examined to evaluate and adopt the proposed framework. Budakoti *et al.* [178] presented a lightweight IoT middleware solution, which can augment interoperability between varied devices, such as sensors, nodes, and mobile phones that transfer data on different networks using various protocols. The middleware solution is deployed on the IoT gateway, i.e., on the edge node which can foster well-organized data analysis for real time, critical applications. A summary of general security solutions is depicted in Table XI.

Furthermore, adding on to the efforts of researchers and academicians working on enhancing security via SDN, it is worth mentioning that the SDSec inputs from the industry as well. Although the pace of vendor-specific commercially available tools is not up to the mark as expected, but still there are few commercially developed security applications that are designed to integrate with SDN controllers. CatBird [179] is one of the first commercially available tools that provides dynamic security based on policies. Furthermore, security and compliance policies are configured to achieve secure network controls. vARMOUR DSS deception [180] is yet another commercially available product that is a simple, scalable, and secure cyber deception solution. It allows organizations to integrate the proactive approach into their defense-in-depth strategies by luring attackers to step outside the realm of legitimate traffic so that they can be easily recognized and properly tackled.

VMware vShield data security [181] is another effort by the commercial realm that defends important data in the virtual and cloud infrastructure. Furthermore, it can track any attack generation. OneControl [182] by NetCitadel is a security solution that generates security alerts with context and provides organizations with a single integrated view of security events in order to enable analysis, ranking, and threat response. DefenseFlow [163] is created by Radware-Opendaylight project that is an SDN-based DDoS mitigation

TABLE XII
LIST OF COMMERCIALLY AVAILABLE SDSEC SOLUTION. THESE SOLUTIONS CAN BE INCORPORATED IN A CLOUD AND DATA-CENTER NETWORKS

Ref	Vendor	Application Area	Solution	Remarks
[183]	Catbird formerly called vSecurity	Hybrid and Private Cloud using SDN	Multi firewalls and hyper visors integration solution	Supports Microsoft, VMware vCloud and Cisco Virtual Security Gateway (VSG)
[184]	VArmour	SDN based Data Centers	VArmour DSS Deception	Protects distributed data located across several servers in an efficient manner to allow the enterpriseto adapt with the new business changes in the world
[185]	Vshield Data Security	SDN	Virtual Security Framework	Allows customers to build policy based groups and establish logical boundaries between them
[186]	NetCitadel	SDN	OneControl	Eliminated manual configuration and response actions to when an event or change occurs
[167]	Radware-OpenDaylight Controller	SDN	DefenseFlow	DefenseFlow is SDN based DDoS abating software and hardware package that permits all gadgets of the network to become part of the DDoS mitigation process

package. It joins all network gadgets to become a part of the DDoS mitigation process. Mainly it performs two tasks, i.e., the protected traffic is monitored and then forwarding the attack generated traffic to abating centers. A summary of the vendor-specific SDSec solutions is depicted in Table XII.

VI. DISCUSSION, FINDINGS, AND ISSUES IDENTIFIED

1) This section discusses some of the findings and issues identified to depict the overall summary of the IoT security situation and way forward. To accomplish a specific malign objective, diverse vulnerabilities and different attack vectors are exploited at various layers of IoT, such as physical, MAC/Network, and application layer as shown in Table II. For example, in IoT devices hardware, some open interfaces are left open by manufacturers for a specific use. However, the attacker exploits this vulnerability and gain unauthorized access into these devices for manipulating the normal operation of the devices [35]. Likewise, the availability of the network services and the network itself is targeted from a jamming perspective. Apropos, different mechanisms are required for anti-jamming protection, which are completely different from mechanisms providing security against eavesdropping. Hence, unique security mechanisms are required depending on various IoT application areas and their corresponding threat vectors.
2) Due to compromised IoT devices, DDoS is the most widely carried out attack [33]. Therefore, keeping in mind the resource constraints of the IoT devices, a proper network mechanism needs to be placed at the entry and exit point of the IoT network.
3) The security requirement of different IoT applications is not fulfilled by security protocols, of the numerous IoT technologies available. However, specific security requirements are provided by all technologies. Extra security mechanism can be provided to a specific application area if the provided security is not enough. Nevertheless, it demands extra cost for additional hardware computation and bandwidth, etc.
4) A single parameter cannot relate the security features of two different technologies.
5) It is important to examine different IoT applications and their related threats in order to provide complete and effective privacy and security solutions. Smart buildings and smart homes are tough similar, but have different environments. For a specific threat, there must be a tailor-made solution, specifically the one comprising physical layer security and traditional cryptography. The objective is to deliver a cost-effective solution while additionally considering the low energy constraints of the different solutions as it may be operated by a battery [24].
6) While designing IoT products, security is usually not the key concern. Product producers are keen to deliver devices with minimal price, low-power greediness, wide coverage, high bit rate, and easy configurations.
7) Due to the resource constraints, the installation of standard IT security protocols is not possible in smart devices. However, if different features offered as optional are removed, certain standard security protocols can be customized.
8) Because of the promising features of centralized access and collected information from the network due to the global view, SDN can configure the devices and regulate the network with dynamism. Therefore, for IoT networks, it is considered to be an appropriate choice of network deployment. In addition, services, such as data gathering, security, analysis, decision making, and configuration of remedial mechanisms turn out to be quicker and simpler by the amalgamation of SDN and IoT.
9) An expandable distributed system with millions of IoT devices can be easily managed by the SDN technology. Multiple SDN controllers, which may be distributed physically, are responsible for controlling the number of subnetworks with IoT devices. As all the controllers are logically connected in a centralized manner, therefore application developers (controller) have the leverage of controlling all smart devices via a single controller.

10) The hardware and data format are abstracted from the underlying IoT applications hardware through the data plane of SDN. This provides enhanced resource utilization for different IoT applications and numerous operators who can utilize the reusability of the current IoT networks for the development of future IoT services. Furthermore, it has magnified desperately the desirable horizontal market which delivers IoT services that are autonomous of a particular application area. Apropos, the SDN is a much-envisioned concept for the future generation IoT architectures.
11) An SDN controller is exploited to efficiently apply security policies on some or all of the networking devices simultaneously. Modifying security policies in the SDN need either adding up security services at the control plane or only updating the security applications, instead of physically modifying the underlying network firmware or hardware.
12) As discussed in Sections III (threats to IoT) and VI-B (SDSec mechanisms/frameworks for SDN-IoT), respectively, it can be inferred that significant research and development are being done both by academia and the commercial sectors to diminish IoT threats. All of these threats are related to the security triad, i.e., threat to secrecy, integrity, and accessibility of data. Consequently, Tables VII–XI show that various academic and research community security solutions proposed to provide defensive, detective, reactive, and remedial measures. For example, device security-related issues, such as device identity [173], [175], tamper proofing [19], and registration and management [158] have been addressed by various researchers. Likewise, data management [18], [149], [168], anomaly detection [172], [176], privacy-preserving techniques [60], [173], DoS/DDoS mitigation techniques [162]–[164], [166], and secure gateways [19], [158], [167] have also been diligently undertaken. Similarly, Table XII highlights some commercial off-the-shelf (COTS) products for SDN-based secure IoT.

VII. Open Research Challenges

1) *Fundamental Security Standard:* There are security, conformity, and interoperability issues in the IoT currently due to no devices standardization, heterogeneous IoT applications, and varied IoT products [183]. The majority of the IoT devices are being produced without any fundamental security standard [25]. However, there is a dire need for cohesive security steps, keeping in view the present threats of IoT devices. These steps include but are not limited to mandatory user authentication and authorization, encrypting data during transmission and at rest, and device security for preventing tampering and application security. Nevertheless, the resource constraints of several IoT devices, such as sensors, microcontroller devices, CCTV, childcare products such as baby cam, and lighting systems for homes along with the computation and memory rich obligations of conventional cryptographic encryption and authentication mechanisms, there is a need for fostering lightweight cryptographic protocols for IoT devices. Minimal manufacturing cost and low energy consumption in terms of application-specific functionalities are also believed to be the restraining factors in fostering a generic solution for all IoT devices. Respectively, to compel bare minimum security standards in IoT devices, there is a desperate need for international standards body for IoT.
2) *Authentication and Access Control:* One of the main security requirements of IoT is authentication. In order to access the IoT application or/and services, the user must be authenticated beforehand. Although, substantial work is done to provide authentication and access control mechanisms in IoT [176], [177]; however, the adaptive nature of IoT networks demands further attention to it. Characteristically, several platforms use data exchange for accessing IoT services and applications. The data are obtained from the IoT devices in a raw form and forwarded to a decision-making process for meaningful information. Depending on the fundamental IoT architecture, these processes may differ, but the data flow remains the same in IoT systems. Therefore, when an IoT device is accessed by any user or application, it must be validated/authenticated to the IoT network and be assured that it has the essential access rights for retrieving the data, else the access must be denied. Similar to traditional networks, access control holds ample significance in IoT networks. Moreover, subject to the data sensitivity of some IoT services and applications, it is imperative to revoke and grant access to certain users. Hence, an adaptive authentication and access control mechanism is needed for IoT systems.
3) *Software Code Integrity:* Various IoT end device integrity ensuring solution exists. Hardware-based techniques are the most reliable solutions that require a safe/secure environment for the execution of the whole attestation process. Producing hardware-based secure IoT products is not a practical approach, because of the low cost and alternative high-scale deployment. Therefore, as an alternative, it is must to discover secure software-based techniques that can be easily configured in low-power IoT devices with the elasticity of timely up gradation. The next generation of networks will probably be equipped with the mammoth number of heterogeneous devices. Consequently, to correctly detect and then adjust any malign software alteration with efficacy, a swarm attestation technique is a challenging task for the huge heterogeneous network [89].
4) *Machine Learning for IoT Security:* ML algorithms build behavioral models using mathematical expression techniques on enormous data sets. Without explicitly programming, ML can empower smart devices to learn. Based on new input data, these models serve as a source

for future predictions. ML is used in scenarios when either human skills do not exist or are unable to leverage their expertise, e.g., speech recognition, etc. In addition, it is also utilized in adaptive nature scenarios, such as routing algorithms in networks or observing the software code integrity of an application. Tough in several areas, ML techniques are known for performing well, however, these are machines and there is always a chance of true negative and false positives [184]. Hence, management and alteration of the model are required when ML techniques predict inaccurately. On the other hand, deep learning (DL) is a new type of ML in which the model itself can govern the accuracy of prediction. IoT systems with contextual and adapted assistance, DL models are best fit for classification and prediction due to the self-service nature. ML and DL can provide promising results for IoT networks in several ways, e.g., a huge amount of data is produced by IoT systems, which can be utilized by ML and DL techniques to enable IoT systems a better and smart decision. Few ML-based security-oriented real-world applications are: a) software and applications malicious code identification and b) behavior analysis-based detecting of DDoS attacks. In traditional networks, ML and DL have been greatly utilized in security solutions, such as IDS, IPS, privacy, etc. Hence, DL techniques can also be utilized for IoT security solution along with SDN-like network-based technology [185].

5) *Problems in Practical Deployment of SDN-IoT:* The IoT network is growing at an exponential speed as compared with the traditional networks [158]. Therefore, an agile and flexible network-based technology is required for next-generation IoT such as SDN. But there are following few problems in the deployment of SND-based IoT that needs to be addressed from the initial planning and design phase.
   a) OpenFlow is constantly evolving, resulting in the multiple flow tables and addition of new matching fields, such as MPLS and IPv6, thus creating more flexibility vis-a-vis complicating the forwarding plane.
   b) The SDN-based IoT is usually the centralized controller architecture and the data from the forwarding devices are constantly being forwarded to the controller, thus resulting in delays in pushing flow tables and may even result in packet loss.
   c) The IoT devices and traditional network nodes are increasing mammoths in number, hence shifting the single controller regime to multiple distributed controllers is needed. The interaction and coordination between these distributed controllers is a serious issue in practice.

VIII. Conclusion

This article focuses on highlighting the generic and well-known attacks and threats pertinent to different layers of the IoT architecture. These threats span from eavesdropping of the transmitted messages, identity theft, and unauthorized access to malicious software code injection, etc. We illustrated a real-world successful attack carried out on smart homes. This article also presented security requirements and challenges of different IoT application areas. Furthermore, based on the gap analysis to counter heterogeneity and security issues of IoT, it is highlighted that a network-based deployment and security solution, such as SDN is needed for the IoT paradigm. Moreover, IoT deployments using SDN and SDN-IoT-based security models are also discussed in detail to better understand the work done by the academicians and researchers. To acquaint the readers, we then presented discussion, findings, and issues, which are actually causing a standstill in the vast deployment of IoT and SDN-based IoT architectures. Finally, IoT security and SDN-IoT deployment models centric open research challenges are discussed.

With respect to today's threat landscape, the innate security given by the conventional communication protocols does not ensure against code modification, node/device compromise attack, and overwhelming malware attacks. It is also evident from the modern cyberattacks carried out on IoT devices that current security standards and protocols for IoT have failed in providing security to IoT devices. Hence, an adaptive, novel, and worthy IoT security system is required to tackle the current security landscape, which should be proactive in nature providing baseline security to end users, networks, applications, data, and devices.

Therefore, the ML technology with its inherent adaptive nature and promising results is suggested as a tool bundled with SDN to address the privacy and security concerns of IoT. ML can solve various security issues in traditional networks due to its trained behavioral model based on strong mathematical expressions and the SDN can provide network-level security services to the IoT as a third-party application. Apropos, we intend to foster a security solution for IoT systems in the future, based on SDN and ML approaches with the goal to defend IoT systems against most of the security attacks.

References

[1] S. Kraijak and P. Tuwanut, "A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends," in *Proc. WiCOM*, 2015, p. 6.

[2] K. Rose, S. Eldridge, and L. Chapin, "The Internet of Things: An overview," in *Proc. Internet Soc. (ISOC)*, 2015, p. 80.

[3] K. Ashton *et al.*, "That Internet of Things thing," *RFID J.*, vol. 22, no. 7, pp. 97–114, 2009.

[4] J. Voas, B. Agresti, and P. A. Laplante, "A closer look at IoT's things," *IT Prof.*, vol. 20, no. 3, pp. 11–14, May 2018.

[5] Gartner, Inc. (1999). *Worlds Well Known Trusted Advisor in It*. [Online]. Available: https://www.gartner.com/en

[6] J. Mocnej, A. Pekar, W. K. Seah, and I. Zolotova, *Network Traffic Characteristics of the IoT Application Use Cases*, Victoria Univ. Wellington, Wellington, New Zealand, Jun. 2017.

[7] J. Voas, "Primitives and elements of Internet of Things (IoT) trustworthiness," Nat. Inst. Stand. Technol., Gaithersburg, MA, USA, Rep., 2016.

[8] A. Meola, *How the Internet of Things Will Affect Security & Privacy*, Bus. Insider, New York, NY, USA, 2016.

[9] J. Steinberg, *These Devices May Be Spying on You (Even in Your Own Home)*, Forbes, Jersey City, NJ, USA, May 2014.

[10] H. Fortify, "Internet of Things security study: Smartwatches," 2015.

[11] T. Hahn *et al.*, "IBM point of view: Internet of Things security," IBM, Armonk, NY, USA, White Paper, Apr. 2015.

[12] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," *Digit. Commun. Netw.*, vol. 4, no. 2, pp. 118–137, 2018.

[13] D. Storm, "Hackers exploit SCADA holes to take full control of critical infrastructure," *Computerworld*, vol. 15, 2014.

[14] AT&TCybersecurityInsights. (2016). *The CEOS Guide to Data Security Protect Your Data Through Innovation*. [Online]. Available: https://www.business.att.com/cybersecurity/docs/vol5-datasecurity.pdf

[15] *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020 White Paper*, Cisco, San Jose, CA, USA, 2016.

[16] S. K. Tayyaba, M. A. Shah, O. A. Khan, and A. W. Ahmed, "Software defined network SDN based Internet of Things IoT a road ahead," in *Proc. ACM Int. Conf. Future Netw. Distrib. Syst.*, 2017, p. 15.

[17] 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.–Dec. 2016.

[18] Y. Liu, Y. Kuang, Y. Xiao, and G. Xu, "SDN-based data transfer security for Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 257–268, Feb. 2018.

[19] M. Conti, P. Kaliyar, and C. Lal, "CENSOR: Cloud-enabled secure IoT architecture over SDN paradigm," *Concurrency Comput. Pract. Exp.*, vol. 31, no. 8, 2019, Art. no. e4978.

[20] F. I. Khan and S. Hameed, "Understanding security requirements and challenges in Internet of Things (IoTs): A review," 2018. [Online]. Available: arXiv:1808.10529.

[21] N. Bizanis and F. A. Kuipers, "SDN and virtualization solutions for the Internet of Things: A survey," *IEEE Access*, vol. 4, pp. 5591–5606, 2016.

[22] T. N. Nguyen, "The challenges in SDN/ML based network security: A survey," 2018. [Online]. Available: arXiv:1804.03539.

[23] O. Salman, I. Elhajj, A. Chehab, and A. Kayssi, "IoT survey: An SDN and fog computing perspective," *Comput. Netw.*, vol. 143, pp. 221–246, Oct. 2018.

[24] 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.

[25] A. Banafa. (2016). "IoT standardization and implementation challenges," *IEEE Internet of Things Newsletter*.

[26] S. A. Kumar, T. Vealey, and H. Srivastava, "Security in Internet of Things challenges solutions and future directions," in *Proc. IEEE 49th Hawaii Int. Conf. Syst. Sci. (HICSS)*, 2016, pp. 5772–5781.

[27] 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.

[28] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[29] M. Khari *et al.*, "Internet of Things: Proposed security aspects for digitizing the world," in *Proc. 3rd Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, 2016, pp. 2165–2170.

[30] A. Reziouk, E. Laurent, and J.-C. Demay, "Practical security overview of IEEE 802.15.4," in *Proc. IEEE Int. Conf. Eng. MIS (ICEMIS)*, 2016, pp. 1–9.

[31] D. Uckelmann, M. Harrison, and F. Michahelles, "An architectural approach towards the future Internet of Things," in *Architecting the Internet of Things*. Heidelberg, Germany: Springer, 2011, pp. 1–24.

[32] 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, 2014.

[33] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things," in *Proc. 14th ACM Workshop Hot Topics Netw.*, 2015, p. 5.

[34] G. Hernandez, O. Arias, D. Buentello, and Y. Jin, "Smart nest thermostat: A smart spy in your home," in *Proc. Black Hat USA*, 2014, pp. 1–8.

[35] S. Zonouz, J. Rrushi, and S. McLaughlin, "Detecting industrial control malware using automated PLC code analytics," *IEEE Security Privacy*, vol. 12, no. 6, pp. 40–47, Nov./Dec. 2014.

[36] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in *Proc. IEEE Int. Conf. I-SMAC IoT Soc. Mobile Anal. Cloud (I-SMAC)*, 2017, pp. 32–37.

[37] B. Javed, M. W. Iqbal, and H. Abbas, "Internet of Things (IoT) design considerations for developers and manufacturers," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2017, pp. 834–839.

[38] S. Katz and B. L. Marshall, "Tracked and fit: Fitbits, brain games, and the quantified aging body," *J. Aging Stud.*, vol. 45, pp. 63–68, Jun. 2018.

[39] M. L. Hale, K. Lotfy, R. F. Gamble, C. Walter, and J. Lin, "Developing a platform to evaluate and assess the security of wearable devices," *Digit. Commun. Netw.*, vol. 5, no. 3, pp. 147–159, 2019.

[40] P. Voigt and A. Von dem Bussche, "The EU general data protection regulation (GDPR)," *A Practical Guide*, 1st ed. Cham, Switzerland: Springer Int., 2017.

[41] P. F. Edemekong and M. J. Haydel, "Health insurance portability and accountability act (HIPAA)," in *StatPearls [Internet]*. New York, NY, USA: StatPearls, 2019.

[42] K. Hamlen, M. Kantarcioglu, L. Khan, and B. Thuraisingham, "Security issues for cloud computing," *Int. J. Inf. Security Privacy*, vol. 4, no. 2, pp. 36–48, 2010.

[43] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial IoT devices," in *Proc. 21st Asia South Pac. Design Autom. Conf. (ASP-DAC)*, 2016, pp. 519–524.

[44] T. Brewster. (2015). *Its Depressingly Easy to Spy on Vulnerable Baby Monitors Using Just a Browser*. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2015/09/02/baby-surveillance-with-a-browser/n2508d85b1aa0

[45] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "Threats to networking cloud and edge datacenters in the Internet of Things," *IEEE Cloud Comput.*, vol. 3, no. 3, pp. 64–71, May/Jun. 2016.

[46] B. Balamurugan and D. Biswas, "Security in network layer of IoT: Possible measures to preclude," in *Security Breaches and Threat Prevention in the Internet of Things*. Hoboken, NJ, USA: IGI Glob., 2017, pp. 46–75.

[47] P. Paganini. (2014). *MS Windows NT Kernel Description*. [Online]. Available: https://securityaffairs.co/wordpress/30320/security/microsoft-patch-kerberos-bug.html

[48] 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.–Jun. 2015.

[49] B. Fowler, "Some top baby monitors lack basic security features report finds," 2015.

[50] T. Borgohain, U. Kumar, and S. Sanyal. (2015). *Survey of Security and Privacy Issues of Internet of Things*. [Online]. Available: http://arxiv.org/abs/1501.02211

[51] V. B. Misic, J. Fang, and J. Misic, "MAC layer security of 802.15.4-compliant networks," in *Proc. IEEE Int. Conf. Mobile Adhoc Sensor Syst. Conf.*, 2005, p. 8.

[52] N. Sastry and D. Wagner, "Security considerations for IEEE 802.15.4 networks," in *Proc. 3rd ACM Workshop Wireless Security*, 2004, pp. 32–42.

[53] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "A dynamic prime number based efficient security mechanism for big sensing data streams," *J. Comput. Syst. Sci.*, vol. 83, no. 1, pp. 22–42, 2017.

[54] J. Murphy. (2016). *MS Windows NT Kernel Description*. [Online]. Available: https://developer.ibm.com/iotplatform/2016/09/23/enhanced-security-controls-for-ibm-watson-iot-platform

[55] R. M. Savola, H. Abie, and M. Sihvonen, "Towards metrics driven adaptive security management in eHealth IoT applications," in *Proc. 7th Int. Conf. Body Area Netw.*, 2012, pp. 276–281.

[56] A. Kanuparthi, R. Karri, and S. Addepalli, "Hardware and embedded security in the context of Internet of Things," in *Proc. ACM Workshop Security Privacy Dependability Cyber Veh.*, 2013, pp. 61–64.

[57] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in *Proc. 52nd ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, 2015, pp. 1–6.

[58] Dave. (2017). *Ten Most Critical Web Application Security Risks*. [Online]. Available: https://www.owasp.org

[59] C. Staff. (2016). *SQLI XSS Zero Days Expose BELKIN IoT Devices Android Smartphones*. [Online]. Available: https://www.csoonline.com/article/3138935/sqli-xss-zero-days-expose-belkin-iot-devices-android-smartphones.html

[60] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, "Network level security and privacy control for smart home IoT devices," in *Proc. IEEE 11th Int. Conf. Wireless Mobile Comput. Netw. Commun. (WiMob)*, 2015, pp. 163–167.

[61] Acunetix. (2018). *Cross-Site Scripting (XSS) Attack*. [Online]. Available: https://www.acunetix.com/websitesecurity/cross-site-scripting/

[62] B. J. Mohd, T. Hayajneh, and A. V. Vasilakos, "A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues," *J. Netw. Comput. Appl.*, vol. 58, pp. 73–93, Dec. 2015.

[63] H. Ning, H. Liu, and L. T. Yang, "Cyberentity security in the Internet of Things," *Computer*, vol. 46, no. 4, pp. 46–53, 2013.

[64] S. R. Moosavi *et al.*, "SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways," *Procedia Comput. Sci.*, vol. 52, pp. 452–459, Jun. 2015.

[65] W. Wu and L. Zhang, "LBlock: A lightweight block cipher," in *Proc. Int. Conf. Appl. Cryptography Netw. Security*, 2011, pp. 327–344.

[66] A. Bogdanov *et al.*, "PRESENT: An ultra-lightweight block cipher," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, 2007, pp. 450–466.

[67] C. H. Lim and T. Korkishko, "mCrypton—A lightweight block cipher for security of low-cost RFID tags and sensors," in *Proc. Int. Workshop Inf. Security Appl.*, 2005, pp. 243–258.

[68] C. DeCanniere, O. Dunkelman, and M. Kne, "KATAN and KTANTAN a family of small and efficient hardware-oriented block ciphers," in *Proc. Cryptograph. Hardw. Embedded Syst. (CHES)*, 2009, pp. 272–288.

[69] A. Moradi, A. Poschmann, S. Ling, C. Paar, and H. Wang, "Pushing the limits: A very compact and a threshold implementation of AES," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2011, pp. 69–88.

[70] M. A. Orumiehchiha, J. Pieprzyk, and R. Steinfeld, "Cryptanalysis of WG-7: A lightweight stream cipher," *Cryptography Commun.*, vol. 4, nos. 3–4, pp. 277–285, 2012.

[71] G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou, and C. Manifavas, "A review of lightweight block ciphers," *J. Cryptograph. Eng.*, vol. 8, no. 2, pp. 141–184, 2018.

[72] A. T. Lo'ai and T. F. Somani, "More secure Internet of Things using robust encryption algorithms against side channel attacks," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, 2016, pp. 1–6.

[73] F. Zhang *et al.*, "A framework for the analysis and evaluation of algebraic fault attacks on lightweight block ciphers," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 1039–1054, May 2016.

[74] M. Majzoobi, M. Rostami, F. Koushanfar, D. S. Wallach, and S. Devadas, "Slender PUF protocol: A lightweight, robust, and secure authentication by substring matching," in *Proc. IEEE Symp. Security Privacy Workshops*, 2012, pp. 33–44.

[75] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

[76] A. Seshadri, A. Perrig, L. Van Doorn, and P. Khosla, "SWATT: Software-based attestation for embedded devices," in *Proc. IEEE Symp. Security Privacy*, 2004, pp. 272–282.

[77] A. Seshadri, M. Luk, E. Shi, A. Perrig, L. Van Doorn, and P. Khosla, "Pioneer: Verifying code integrity and enforcing untampered code execution on legacy systems," *ACM SIGOPS Oper. Syst. Rev.*, vol. 39, no. 5, pp. 1–16, 2005.

[78] A. Seshadri, M. Luk, A. Perrig, L. van Doorn, and P. Khosla, "SCUBA: Secure code update by attestation in sensor networks," in *Proc. 5th ACM Workshop Wireless Security*, 2006, pp. 85–94.

[79] Y. Yang, X. Wang, S. Zhu, and G. Cao, "Distributed software-based attestation for node compromise detection in sensor networks," in *Proc. 26th IEEE Int. Symp. Reliable Distrib. Syst. (SRDS)*, 2007, pp. 219–230.

[80] T. AbuHmed, N. Nyamaa, and D. Nyang, "Software-based remote code attestation in wireless sensor network," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, 2009, pp. 1–8.

[81] T. Abera *et al.*, "Things, trouble, trust: On building trust in IoT systems," in *Proc. ACM 53rd Annu. Design Autom. Conf.*, 2016, p. 121.

[82] K. Eldefrawy, G. Tsudik, A. Francillon, and D. Perito, "SMART: Secure and minimal architecture for (establishing dynamic) root of trust," in *Proc. NDSS*, vol. 12, 2012, pp. 1–15.

[83] R. Strackx, F. Piessens, and B. Preneel, "Efficient isolation of trusted subsystems in embedded systems," in *Proc. Int. Conf. Security Privacy Commun. Syst.*, 2010, pp. 344–361.

[84] J. Noorman *et al.*, "SANCUS 2.0: A low-cost security architecture for IoT devices," *ACM Trans. Privacy Security*, vol. 20, no. 3, p. 7, 2017.

[85] P. Koeberl, S. Schulz, A.-R. Sadeghi, and V. Varadharajan, "TrustLite: A security architecture for tiny embedded devices," in *Proc. ACM 9th Eur. Conf. Comput. Syst.*, 2014, p. 10.

[86] F. Brasser, B. El Mahjoub, A.-R. Sadeghi, C. Wachsmann, and P. Koeberl, "TyTAN: Tiny trust anchor for tiny devices," in *Proc. 52nd ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, 2015, pp. 1–6.

[87] A.-R. Sadeghi, S. Schulz, and C. Wachsmann, "Short paper: Lightweight remote attestation using physical functions," in *Proc. WiSec*, 2011, pp. 109–114.

[88] J. Kong, F. Koushanfar, P. K. Pendyala, A.-R. Sadeghi, and C. Wachsmann, "PUFatt: Embedded platform attestation based on novel processor-based PUFs," in *Proc. 51st ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, 2014, pp. 1–6.

[89] N. Asokan *et al.*, "SEDA: Scalable embedded device attestation," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Security*, 2015, pp. 964–975.

[90] M. Ambrosin, M. Conti, A. Ibrahim, G. Neven, A.-R. Sadeghi, and M. Schunter, "SANA: Secure and scalable aggregate network attestation," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 731–742.

[91] T. Abera *et al.*, "C-FLAT: Control-flow attestation for embedded systems software," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 743–754.

[92] G. Dessouky *et al.*, "LO-FAT: Low-overhead control flow attestation in hardware," in *Proc. ACM 54th Annu. Design Autom. Conf.*, 2017, p. 24.

[93] D. Dragomir, L. Gheorghe, S. Costea, and A. Radovici, "A survey on secure communication protocols for IoT systems," in *Proc. IEEE Int. Workshop Secure Internet Things (SIoT)*, 2016, pp. 47–62.

[94] H. Kim and E. A. Lee, "Authentication and authorization for the Internet of Things," *IT Prof.*, vol. 19, no. 5, pp. 27–33, 2017.

[95] A. Alcaide, E. Palomar, J. Montero-Castillo, and A. Ribagorda, "Anonymous authentication for privacy-preserving IoT target-driven applications," *Comput. Security*, vol. 37, pp. 111–123, Sep. 2013.

[96] A. Farahzadi, P. Shams, J. Rezazadeh, and R. Farahbakhsh, "Middleware technologies for cloud of things: A survey," *Digit. Commun. Netw.*, vol. 4, no. 3, pp. 176–188, 2018.

[97] C. Su, B. Santoso, Y. Li, R. H. Deng, and X. Huang, "Universally composable RFID mutual authentication," *IEEE Trans. Depend. Secure Comput.*, vol. 14, no. 1, pp. 83–94, Jan./Feb. 2017.

[98] R. H. Weber, "Internet of Things: Privacy issues revisited," *Comput. Law Security Rev.*, vol. 31, no. 5, pp. 618–627, 2015.

[99] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the Internet of Things: Threats and challenges," *Security Commun. Netw.*, vol. 7, no. 12, pp. 2728–2742, 2014.

[100] J. Lopez, R. Rios, F. Bao, and G. Wang, "Evolving privacy: From sensors to the Internet of Things," *Future Gener. Comput. Syst.*, vol. 75, pp. 46–57, Oct. 2017.

[101] R. Mendes and J. P. Vilela, "Privacy-preserving data mining: Methods, metrics, and applications," *IEEE Access*, vol. 5, pp. 10562–10582, 2017.

[102] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan, and N. Feamster, "Spying on the smart home: Privacy attacks and defenses on encrypted IoT traffic," 2017. [Online]. Available: arXiv:1708.05044.

[103] J. Liu, C. Zhang, and Y. Fang, "EPIC: A differential privacy framework to defend smart homes against Internet traffic analysis," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1206–1217, Apr. 2018.

[104] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A privacy preserving communication protocol for IoT applications in smart homes," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1844–1852, Dec. 2017.

[105] Y. Tian *et al.*, "SmartAuth: User-centered authorization for the Internet of Things," in *Proc. 26th USENIX Security Symp. (USENIX Security)*, 2017, pp. 361–378.

[106] E. Fernandes, A. Rahmati, J. Jung, and A. Prakash, "Security implications of permission models in smart-home application frameworks," *IEEE Security Privacy*, vol. 15, no. 2, pp. 24–30, Mar./Apr. 2017.

[107] M. A. Sahi *et al.*, "Privacy preservation in e-healthcare environments: State of the art and future directions," *IEEE Access*, vol. 6, pp. 464–478, 2017.

[108] B. Riedl, V. Grascher, and T. Neubauer, "A secure e-health architecture based on the appliance of pseudonymization," *J. Softw.*, vol. 3, no. 2, pp. 23–32, 2008.

[109] X. Liu, Y. Li, J. Qu, and Y. Ding, "A lightweight pseudonym authentication and key agreement protocol for multi-medical server architecture in TMIS," *KSII Trans. Internet Inf. Syst.*, vol. 11, no. 2, pp. 924–944, 2017.

[110] X. Li *et al.*, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Comput. Netw.*, vol. 129, pp. 429–443, Dec. 2017.

[111] A. M. Koya and P. Deepthi, "Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network," *Comput. Netw.*, vol. 140, pp. 138–151, Jul. 2018.

[112] K. Seol, Y.-G. Kim, E. Lee, Y.-D. Seo, and D.-K. Baik, "Privacy-preserving attribute-based access control model for XML-based electronic health record system," *IEEE Access*, vol. 6, pp. 9114–9128, 2018.

[113] C. Rottondi, G. Verticale, and A. Capone, "Privacy-preserving smart metering with multiple data consumers," *Comput. Netw.*, vol. 57, no. 7, pp. 1699–1713, 2013.

[114] S. Ge, P. Zeng, R. Lu, and K.-K. R. Choo, "FGDA: Fine-grained data analysis in privacy-preserving smart grid communications," *Peer-to-Peer Netw. Appl.*, vol. 11, no. 5, pp. 966–978, 2018.

[115] C.-I. Fan, S.-Y. Huang, and Y.-L. Lai, "Privacy-enhanced data aggregation scheme against internal attackers in smart grid," *IEEE Trans. Ind. Informat.*, vol. 10, no. 1, pp. 666–675, Feb. 2014.

[116] H. Shen, M. Zhang, and J. Shen, "Efficient privacy-preserving cube-data aggregation scheme for smart grids," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1369–1381, Jun. 2017.

[117] M. A. Rahman, M. H. Manshaei, E. Al-Shaer, and M. Shehab, "Secure and private data aggregation for energy consumption scheduling in smart grids," *IEEE Trans. Depend. Secure Comput.*, vol. 14, no. 2, pp. 221–234, Mar./Apr. 2015.

[118] D. Engel and G. Eibl, "Wavelet-based multiresolution smart meter privacy," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1710–1721, Jul. 2017.

[119] S. Zawoad and R. Hasan, "FAIoT: Towards building a forensics aware ECO system for the Internet of Things," in *Proc. IEEE Int. Conf. Services Comput.*, 2015, pp. 279–284.

[120] L. Caviglione, S. Wendzel, and W. Mazurczyk, "The future of digital forensics: Challenges and the road ahead," *IEEE Security Privacy*, vol. 15, no. 6, pp. 12–17, Nov. 2017.

[121] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 78, pp. 544–546, Jan. 2018.

[122] V. R. Kebande and I. Ray, "A generic digital forensic investigation framework for Internet of Things (IoT)," in *Proc. IEEE 4th Int. Conf. Future Internet Things Cloud (FiCloud)*, 2016, pp. 356–362.

[123] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, "Internet of Things forensics: Challenges and approaches," in *Proc. 9th IEEE Int. Conf. Collaborative Comput. Netw. Appl. Worksharing*, 2013, pp. 608–615.

[124] A. Nieto, R. Rios, and J. Lopez, "IoT-forensics meets privacy: Towards cooperative digital investigations," *Sensors*, vol. 18, no. 2, p. 492, 2018.

[125] *Changing Driving Laws to Support Automated Vehicles*, NTC, Melbourne VIC, Australia, Oct. 2017.

[126] O. N. Fundation, "Software-defined networking: The new norm for networks," vol. 2, ONF, Menlo Park, CA, USA, White Paper, pp. 2–6, 2012.

[127] M. Casado, M. J. Freedman, J. Pettit, J. Luo, N. McKeown, and S. Shenker, "ETHANE: Taking control of the enterprise," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 4, pp. 1–12, 2007.

[128] M. Casado *et al.*, "SANE: A protection architecture for enterprise networks." in *Proc. USENIX Security Symp.*, vol. 49, 2006, p. 50.

[129] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "SDN security: A survey," in *Proc. IEEE SDN Future Netw. Services (SDN4FNS)*, 2013, pp. 1–7.

[130] K. Benzekki, A. El Fergougui, and A. E. Elalaoui, "Software-defined networking (SDN): A survey," *Security Commun. Netw.*, vol. 9, no. 18, pp. 5803–5833, 2016.

[131] N. McKeown *et al.*, "OpenFlow enabling innovation in campus networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, 2008.

[132] ONF. (2013). *Open Networking Foundation*. [Online]. Available: https://www.opennetworking.org

[133] I. Alsmadi and D. Xu, "Security of software defined networks: A survey," *Comput. Security*, vol. 53, pp. 79–108, Sep. 2015.

[134] RYU. (2015). *Osrg.githubioryu*. [Online]. Available: https://osrg.github.io/ryu/

[135] ONOS. (2015). *Open Networking Operating System Project*. [Online]. Available: https://onosproject.org

[136] ODL. (2018). *Openday Light Project*. [Online]. Available: https://www.opendaylight.org

[137] FDL. (2019). *Flood Light Project*. [Online]. Available: http://www.projectfloodlight.org/floodlight/

[138] N. Gude *et al.*, "NOX: Towards an operating system for networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 3, pp. 105–110, 2008.

[139] M. McCauley. (2018). *Pox Controller*. [Online]. Available: https://github.com/noxrepo/

[140] M. Karakus and A. Durresi, "A survey: Control plane scalability issues and approaches in software-defined networking (SDN)," *Comput. Netw.*, vol. 112, pp. 279–293, Jan. 2017.

[141] H. Song, "Protocol-oblivious forwarding: Unleash the power of SDN through a future-proof forwarding plane," in *Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw.*, 2013, pp. 127–132.

[142] B. Pfaff and B. Davie, "The open vSwitch database management protocol," IETF, RFC 7047, 2013.

[143] D. Kreutz, F. Ramos, P. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," 2014. [Online]. Available: arXiv:1406.0440.

[144] N. Foster *et al.*, "Frenetic: A network programming language," *ACM SIGPLAN Notices*, vol. 46, no. 9, pp. 279–291, 2011.

[145] C. J. Anderson *et al.*, "NetKat: Semantic foundations for networks," *ACM SIGPLAN Notices*, vol. 49, no. 1, pp. 113–126, 2014.

[146] C. Monsanto, N. Foster, R. Harrison, and D. Walker, "A compiler and run-time system for network programming languages," *ACM SIGPLAN Notices*, vol. 47, no. 1, pp. 217–230, 2012.

[147] J. Reich, C. Monsanto, N. Foster, J. Rexford, and D. Walker, "Modular SDN programming with pyretic," in *Proc. USENIX*, 2013, p. 8.

[148] J. Li, E. Altman, and C. Touati, "A general SDN-based IoT framework with NVF implementation," 2015.

[149] Y. Jararweh, M. Al-Ayyoub, E. Benkhelifa, M. Vouk, and A. Rindos, "SDIoT: A software defined based Internet of Things framework," *J. Ambient Intell. Humanized Comput.*, vol. 6, no. 4, pp. 453–461, 2015.

[150] M. Ojo, D. Adami, and S. Giordano, "A SDN-IoT architecture with NFV implementation," in *Proc. IEEE Globecom Workshops (GC Wkshps),* 2016, pp. 1–6.

[151] Z. Qin, G. Denker, C. Giannelli, P. Bellavista, and N. Venkatasubramanian, "A software defined networking architecture for the Internet-of-Things," in *Proc. IEEE Netw. Oper. Manag. Symp. (NOMS)*, 2014, pp. 1–9.

[152] I. Bedhief, M. Kassar, and T. Aguili, "SDN-based architecture challenging the IoT heterogeneity," in *Proc. 3rd Smart Cloud Netw. Syst. (SCNS)*, 2016, pp. 1–3.

[153] M. Tortonesi, J. Michaelis, A. Morelli, N. Suri, and M. A. Baker, "SPF: An SDN-based middleware solution to mitigate the IoT information explosion," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, 2016, pp. 435–442.

[154] D. Sinh, L.-V. Le, B.-S. P. Lin, and L.-P. Tung, "SDN NFV a new approach of deploying network infrastructure for IoT," in *Proc. IEEE 27th Wireless Opt. Commun. Conf. (WOCC)*, 2018, pp. 1–5.

[155] W. Cerroni *et al.*, "Intent-based management and orchestration of heterogeneous OpenFlow/IoT SDN domains," in *Proc. IEEE Conf. Netw. Softw. (NetSoft)*, 2017, pp. 1–9.

[156] Y. Li, X. Su, J. Riekki, T. Kanter, and R. Rahmani, "A SDN-based architecture for horizontal Internet of Things services," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2016, pp. 1–7.

[157] Y. Wang, Y. Zhang, and J. Chen, "An SDN-based publish/subscribe-enabled communication platform for IoT services," *China Commun.*, vol. 15, no. 1, pp. 95–106, 2018.

[158] O. Flauzac, C. Gonzalez, A. Hachani, and F. Nolot, "SDN based architecture for IoT and improvement of the security," in *Proc. IEEE 29th Int. Conf. Adv. Inf. Netw. Appl. Workshops*, 2015, pp. 688–693.

[159] F. Olivier, G. Carlos, and N. Florent, "New security architecture for IoT network," *Procedia Comput. Sci.*, vol. 52, pp. 1028–1033, Jun. 2015.

[160] D. Wu, D. I. Arkhipov, E. Asmare, Z. Qin, and J. A. McCann, "UbiFlow: Mobility management in urban-scale software defined IoT," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2015, pp. 208–216.

[161] S. Tomovic, K. Yoshigoe, I. Maljevic, and I. Radusinovic, "Software-defined fog network architecture for IoT," *Wireless Pers. Commun.*, vol. 92, no. 1, pp. 181–196, 2017.

[162] M. Al-Ayyoub, Y. Jararweh, E. Benkhelifa, M. A. Vouk, and A. Rindos, "SDSecurity: A software defined security experimental framework," in *Proc. IEEE Int. Conf. Commun. Workshop (ICCW)*, 2015, pp. 1871–1876.
[163] P. Bull, R. Austin, E. Popov, M. Sharma, and R. Watson, "Flow based security for IoT devices using an SDN gateway," in *Proc. IEEE 4th Int. Conf. Future Internet Things Cloud (FiCloud)*, 2016, pp. 157–163.
[164] S. S. Bhunia and M. Gurusamy, "Dynamic attack detection and mitigation in IoT using SDN," in *Proc. IEEE 27th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, 2017, pp. 1–6.
[165] R. Mohammadi, R. Javidan, and M. Conti, "SLICOTs: An SDN based lightweight countermeasure for TCP SYN flooding attacks," *IEEE Trans. Netw. Service Manag.*, vol. 14, no. 2, pp. 487–497, Jun. 2017.
[166] N. Z. Bawany and J. A. Shamsi, "Seal SDN based secure and agile framework for protecting smart city applications from DDoS attacks," *J. Netw. Comput. Appl.*, vol. 145, Nov. 2019, Art. no. 102381.
[167] S. Chakrabarty, D. W. Engels, and S. Thathapudi, "Black SDN for the Internet of Things," in *Proc. IEEE 12th Int. Conf. Mobile Ad Hoc Sensor Syst.*, 2015, pp. 190–198.
[168] C. Gonzalez, S. M. Charfadine, O. Flauzac, and F. Nolot, "SDN-based security framework for the IoT in distributed grid," in *Proc. Int. Multidiscipl. Conf. Comput. Energy Sci. (SpliTech)*, 2016, pp. 1–5.
[169] C. Gonzalez, O. Flauzac, F. Nolot, and A. Jara, "A novel distributed SDN-secured architecture for the IoT," in *Proc. Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, 2016, pp. 244–249.
[170] M. Gheisari, G. Wang, S. Chen, and H. Ghorbani, "IoT-SDNPP a method for privacy-preserving in smart city with software defined networking," in *Proc. Int. Conf. Algorithms Architect. Parallel Process.*, 2018, pp. 303–312.
[171] M. Gheisari, G. Wang, W. Z. Khan, and C. Fernandez-Campusano, "A context-aware privacy-preserving method for IoT-based smart city using software defined networking," *Comput. Security*, vol. 87, Nov. 2019, Art. no. 101470.
[172] R. Vilalta *et al.*, "Improving security in Internet of Things with software defined networking," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2016, pp. 1–6.
[173] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A.-R. Sadeghi, and S. Tarkoma, "IoT sentinel: Automated device-type identification for security enforcement in IoT," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, 2017, pp. 2177–2184.
[174] P. K. Sharma, J. H. Park, Y.-S. Jeong, and J. H. Park, "SHSEC: SDN based secure smart home network architecture for Internet of Things," *Mobile Netw. Appl.*, vol. 24, no. 3, pp. 913–924, 2019.
[175] O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab, and A. Kayssi, "Identity-based authentication scheme for the Internet of Things," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, 2016, pp. 1109–1111.
[176] F. I. Khan and S. Hameed, "Software defined security service provisioning framework for Internet of Things," 2017. [Online]. Available: arXiv:1711.11133.
[177] I. Farris *et al.*, "Towards provisioning of SDN/NFV-based security enablers for integrated protection of IoT systems," in *Proc. IEEE Conf. Stand. Commun. Netw. (CSCN)*, 2017, pp. 169–174.
[178] J. Budakoti, A. S. Gaur, and C.-H. Lung, "IoT gateway middleware for SDN managed IoT," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber Phys. Soc. Comput. (CPSCom) IEEE Smart Data (SmartData)*, 2018, pp. 154–161.
[179] CatBird. (2014). *Private Cloud Security*. [Online]. Available: https://docplayer.net/2298462-Catbird-6-0-private-cloud-security.html
[180] vArmour. (2015). *VArmour DSS Deception Data Sheet*. [Online]. Available: https://www.varmour.com
[181] Vmware. (2010). *The Technology Foundations of VMware vShield*. [Online]. Available: https://www.vmware.com/files/pdf/techpaper/vShield-Tech-Foundations-WP.pdf
[182] "Netcitadels one control platform the key to intelligent, adaptive network security," Netcitadel, Mountain View, CA, USA, White Paper, 2012.
[183] H. Aftab, K. Gilani, J. Lee, L. Nkenyereye, S. Jeong, and J. Song, "Analysis of identifiers in IoT platforms," *Digit. Commun. Netw.*, to be published.
[184] J. Qiu, Q. Wu, G. Ding, Y. Xu, and S. Feng, "A survey of machine learning for big data processing," *EURASIP J. Adv. Signal Process.*, vol. 2016, no. 1, p. 67, 2016.
[185] K. Sha, T. A. Yang, W. Wei, and S. Davari, "A survey of edge computing based designs for IoT security," *Digit. Commun. Netw.*, vol. 131, pp. 189–199, Sep. 2019.

Waseem Iqbal received the bachelor's degree in computer science from the Department of Computer Science, University of Peshawar, Peshawar, Pakistan, in 2008, and the master's degree in information security from the Military College of Signals, National University of Sciences and Technology (NUST), Islamabad, Pakistan, in 2012.

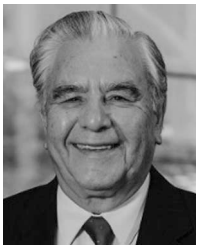
He is an Academician, a Researcher, a Security Professional, and an Industry Consultant. He was inducted as a Lecturer with the Department of Information Security, NUST, in May 2012, where he was promoted as an Assistant Professor in Feb 2015. He is currently enrolled in Ph.D. program and is in research phase. He has authored over 35 scientific research articles in prestigious international journals (ISI-indexed) and conferences. He is a Principal Advisor for more than eight M.S. students and ten UG projects. Eight out of ten UG projects are industry funded projects. He has conducted more than 15 CEH, CHFI, CSCU, and Forensics practical hands on workshops for industry and general public.

Dr. Iqbal was awarded the Overall University Best Teacher Award for the year 2014/15. He achieved the merit-based scholarship throughout his bachelor's degree. His professional services include, but not limited to industry consultation, workshops organizer/resource person, technical program committee member, conference chief organizer, invited speaker, and reviewer for several international conferences.

Haider Abbas received the M.S. degree in engineering and management of information systems and the Ph.D. degree in information security from the KTH Royal Institute of Technology, Stockholm, Sweden, in 2006 and 2010, respectively.

He is a Cyber Security Professional, an Academician, a Researcher, and an Industry Consultant who took professional trainings and certifications from the Massachusetts Institute of Technology, Cambridge, MA, USA; Stockholm University, Stockholm; the Stockholm School of Entrepreneurship, Stockholm; IBM, Armonk, NY, USA; and the EC Council, Albuquerque, NM, USA. He is also an Adjunct Faculty and Doctoral Studies Advisor with the Florida Institute of Technology, Melbourne, FL, USA, and Manchester Metropolitan University, Manchester, U.K.

Dr. Abbas has been awarded the One of the Youngest Fellows of the Institution of Engineering and Technology, U.K., in recognition of his services to the international research community and excellence in professional standing; and a Fellow of the British Computer Society, U.K., and the Institute of Science and Technology, U.K. His professional career consists of activities ranging from research and development and industry consultations (government and private), through multinational research projects, research fellowships, doctoral studies advisory services, international journal editorships, conferences/workshops chair, invited/keynote speaker, technical program committee member, and reviewer for several international journals and conferences.



Mahmoud Daneshmand received the B.S. and M.S. degrees in mathematics from the University of Tehran, Tehran, Iran, and the M.S. and Ph.D. degrees in statistics from the University of California at Berkeley, Berkeley, CA, USA.

He is the Co-Founder and a Professor with the Department of Business Intelligence and Analytics as well as the Data Science Ph.D. Program, and a Professor with the Department of Computer Science, Stevens Institute of Technology, Hoboken, NJ, USA. He has more than 40 years of industry and university experience as the Executive Director, the Assistant Chief Scientist, a Professor, a Researcher, a Distinguished Member of Technical Staff, the Technology Leader, the Founding Chair of Department, and the Dean of School with: Bell Laboratories, Murray Hill, NJ, USA; AT&T Shannon Labs-Research, Atlanta, GA, USA; the University of California at Berkeley; the University of Texas at Austin, Austin, TX, USA; New York University, New York, NY, USA; Sharif University of Technology, Tehran; the University of Tehran; and Stevens Institute of Technology. He is a Data Scientist, expert in big data analytics, artificial intelligence, and machine learning with extensive industry experience including with the Bell Laboratories as well as the Info Lab of the AT&T Shannon Labs-Research. He has published more than 200 journal and conference papers; authored/coauthored three books, and has graduated more than 2000 Ph.D. and M.S. students.

Dr. Daneshmand holds key leadership roles in IEEE Journal Publications, IEEE Major Conferences, Industry—IEEE Partnership, and IEEE Future Direction Initiatives. He is the Co-Founder and the Chair of Steering Committee of the IEEE INTERNET OF THINGS JOURNAL; a Member of Steering Committee of the IEEE TRANSACTION ON BIG DATA; an Advisory Board of the IEEE Blockchain Newsletter; a Guest Editor of several IEEE journal publications; a Guest Editor of ITU Journal Special Issue on Data for Good; the Co-Founder of the IEEE Big Data Initiative; and the Vice Chair of the IEEE Technical Community on Big Data. He has served as the general chair, the keynote chair, the panel chair, the executive program chair, and the technical program chair of many IEEE major conferences. He has given many keynote speeches in major IEEE as well as international conferences.

Bilal Rauf received the M.S. degree in computer science with major in wireless LAN from Umeå University, Umeå, Sweden.

He is working as an Assistant Professor with the Department of Computer Software Engineering, Military College of Signals, NUST, Islamabad, Pakistan. He worked as a Lecturer from February 2008 to March 2012. In April 2012, he was promoted to the rank of an Assistant Professor. He is also CCNA certified. He has three research publications in international conferences to his credit. He is currently involved in teaching undergraduate courses and supervising UG final year projects in the field of computer networks and mobile computing. In addition to teaching, he is also responsible to manage Department's Computer Labs as System Administrator. His research interests are wireless LAN, QoS in wireless LAN, and computer networks.

Yawar Abbas Bangash received the B.S. degree in software engineering from the KPK University of Engineering and Technology, Peshawar, Pakistan, in 2008, the M.S. degree in computer science (information security) from Wuhan University of Technology, Wuhan, China, in 2014, and the Ph.D. degree from Huazhong University of Science and Technology, Wuhan, in 2017.

From 2008 to 2012, he worked with Huawei Organization Pakistan Ltd., Islamabad, Pakistan, Higher Education Commission (HEC) Project PERN2, and Baluchistan Education Foundation on different positions in networking sector. He has published high-quality papers in ISI indexed journals. He also conducted various workshops related to 5G technologies and SDN. In addition, he is supervising ten M.S. students and co-supervising three Ph.D. students. He is currently an Assistant Professor with the Military College of Signals, National University of Sciences and Technology, Islamabad. His research interests are software-defined networking, software-defined storage, wireless sensor networks, formal methods in software engineering, AI, information security, cloud computing, data center networking, IoT, and security in SDN, WSN, and smart IoT.

Dr. Bangash won the HEC Prestigious Scholarship "M.S. leading to Ph.D." for five years in 2012.