IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures in the Internet of Things

Shapla Khanam[1], (Member, IEEE), Ismail Bin Ahmedy[1,2], Mohd Yamani Idna Idris[1,2], and Mohamed Hisham Jaward[3], Aznul Qalid Bin Md Sabri[4]

[1]Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur 50603, Malaysia.
[2]Centre for Mobile Cloud Computing, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur 50603, Malaysia.
[3]School of Engineering, Monash University Malaysia.
[4]Department of Artificial Intelligence, Faculty of Computer Science & Information Technology, University of Malaya

Corresponding author: Ismail Bin Ahmedy (e-mail: ismailahmedy@um.edu.my) and Shapla Khanam (e-mail: shapla87bd@yahoo.com)

ABSTRACT Internet of Things (IoT) facilitates the integration between objects and different sensors to provide communication among them without human intervention. However, the extensive demand for IoT and its various applications has continued to grow, coupled with the need to achieve foolproof security requirements. IoT produces a vast amount of data under several constraints such as low processor, power, and memory. These constraints, along with the invaluable data produced by IoT devices, make IoT vulnerable to various security attacks. This paper presents an overview of IoT, its well-known system architecture, enabling technologies, and discusses security challenges and goals. Furthermore, we analyze security vulnerabilities and provide state-of-the-art security taxonomy. The taxonomy of the most relevant and current IoT security attacks is presented for application, network, and physical layers. While most other surveys studied one of the areas of security measures, this study considers and reports on the most advanced security countermeasures within the areas of autonomic, encryption, and learning-based approaches. Additionally, we uncover security challenges that may be met by the research community regarding security implementation in heterogeneous IoT environment. Finally, we provide different visions about possible security solutions and future research directions.

INDEX TERMS Attacks, Countermeasures, Encryption, Internet of Things, IoT Architecture, Learning-based Algorithm, Privacy, Security, Secure Communications, Taxonomy

I. INTRODUCTION

Internet of Things (IoT) generally refers to a world of networked smart objects, where every physical "thing" which has a digital element is interconnected. According to [1], IoT is defined as follows.

A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'Things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.

A similar definition is also provided in [2].

IoT enables the interconnectivity of billions of devices to aid computing and communications. Digital entities such as sensors, Radio-Frequency Identification (RFID), internet and localization technology make it possible to transform everyday objects into smart objects which are capable of interpreting and interacting with each other [2]. The embedded sensors in smart objects monitor, sense, and collect different kinds of data about equipment, environment, and human social life [3]. Despite the usefulness of IoT, there is a major concern of security susceptibility. The connections between humans, devices, sensors and services are universal and continuous. No matter how well-designed, intelligently configured, efficiently implemented and properly maintained a security system is, it will have to rely on human intervention and is not immune to security threats. Therefore, human element is required in designing cybersecurity solutions [4]. Although technological developments have further enhanced security solutions and made them fully protected in many cases, there is still an ongoing need for security solutions to evolve and develop in order to overcome new security challenges [5].

Unlike conventional Internet Technology (IT) infrastructure, IoT devices are processor, memory, and power-constrained, and they are usually deployed in hostile, dynamic and heterogeneous environments. In comparison with conventional IT

infrastructures, IoT comprises of potentially numerous types of devices and networks. The main objective of IoT is to offer integration among software, sensors, interoperable communication protocols, network infrastructures, and physical objects [6]. The embedded devices offer a vast number of digital services that support daily human activities. Therefore, we can easily control, operate devices, and share data from long distances in real-time. However, the rapid and large-scale deployment of IoT devices poses a significant security concern. The authentication, authorization, system configuration, verification, access control, information storage and management verification, to name a few, are the main security challenges in the IoT realm. Vital information may leak or be tampered at any time. The security of IoT devices, the information they contain and users' privacy are not guaranteed. In order to encourage wider deployment of IoT, robust security is essential to provide users with a sense of privacy of their personal information [7], [8].

The surveys conducted in [9], [10]–[12], [14] reveal the security breaches and merciless of cyber-threats faced by organizations in the recent years. They reported the security breaches and attacks witnessed by large and small businesses in the United Kingdom. Figure 1 depicts the rate of security breaches experienced by large and small organizations between 2014 and 2019 in the UK. IoT produces a massive amount of data for organizations and businesses, which makes it a target and an alluring venture for adversaries who seek to steal business information for ransom or other intents resulting in financial losses on the part of the organization. Since IoT is becoming a mission-critical element of small, medium, and large organizations and their businesses, security has become an essential component and a requirement of IoT. It is also evident that security solutions of IoT have improved over time [13], yet security threats are also evolving in more far-reaching and destructive ways.

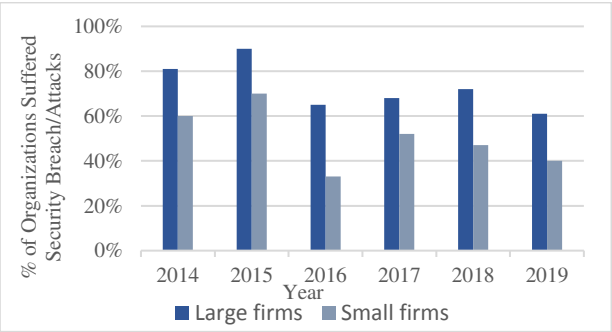

FIGURE 1. The organizations experienced security breaches or attacks in the UK [9]–[11], [14]

Several surveys on IoT security vulnerabilities and challenges have been published between the years of 2012 to 2020 [8], [15], [24], [25], [16]–[23], [26]. However, these surveys have not taken into consideration current attack categories such as multi-dimensional attacks and other security challenges with IoT in terms of their attributes and diversities. Many studies only provided the taxonomy of attacks, whereas others focused only on specific types of security countermeasures for securing IoT. To the best of our knowledge, no other study on IoT security was done to combine learning-based, encryption and autonomic security countermeasures comprehensively.

This paper presents different IoT application domains and their security threats, attacks and vulnerabilities. It also presents recent advances in IoT, including its architecture, enabling technologies and protocols. We highlight security challenges, goals and methods of security attack, and identify why IoT security differs from conventional IT security. We provide an extensive taxonomy of security attacks based on a three-layered (application, network and physical layers) IoT architecture. The objective of this survey is to explore, address and bring together the advanced security countermeasures including learning-based algorithms such as Machine Learning (ML) and Deep Learning (DL) techniques; autonomic approaches; and cryptographic or encryption methods. We give some insights into the suitability of implementing them in IoT. We aim to provide a user manual of those security aspects for a heterogeneous IoT environment by discussing the comparisons of existing solutions holistically. We further provide relevant insights and future research directions in order to guide researchers in their quest to address IoT security issues. The contributions of this paper are summarized as follows.

- The study presents insights into IoT architectures and enabling technologies.
- The survey discusses a systematic summary of the IoT security challenges and goals.
- The paper provides a taxonomy of security attacks for three-layered IoT architecture.
- It provides comprehensive and advanced security countermeasures, including learning-based, autonomic and cryptographic/encryption techniques towards securing IoT systems.
- Finally, it provides insightful comparisons of existing countermeasures, discusses their applicability for different security attacks and provides future research directions.

A. RELATED WORKS

There are several review studies on the security of IoT. Some of these studies focused on security challenges, whereas others focused on security solutions based on different techniques and methodologies. The survey by Hassija et al. [27] provided several IoT security challenges and further discussed fog, edge computing, block-chain and machine learning technologies as the various means of scaling up IoT security. Another survey [28] focused on physical layer security, protocols and handover defenses for mobile-IoT. The authors compared the existing security measures for mobile-IoT applications. A systematic review study [29] investigated hardware and software-based security measures for IoT mobile computing devices. In [30], the authors highlighted several authentication methods for IoT and discussed various security verification mechanisms. They also provided future directions for research on authentication mechanisms.

Chen et al. [31] reviewed existing security solutions for global positioning and location-based IoT. The study also presented security aspects of localization of IoT from policy, regulation and legal points of view. They went further to

provide relevant insights to a secured location-based IoT. The authors in [32] addressed security threats and vulnerabilities of network layers of IoT. Their work focused on existing machine learning-based intrusion detection system and analyzed them in terms of detection techniques and validation mechanisms. The study [33] examined insider IoT threats based on various data sources such as IoT deployment environments, IoT architectures. The authors compared different data sources from different IoT layers and investigated the limitations on potential utilization of the data sources and methodologies. Current security challenges on IoT technologies of commercial IoT environments have been reported in [34]. They addressed confidentiality, anonymity, resilience and self-organization attributes of security aspects for IoT.

The authors in [35] reported on the features and challenges of security in distributed IoT. In [36], the authors reviewed only the malware category of attacks, their analysis and detection techniques. The authors in [37] highlighted the key future prerequisites for providing security in a smart home. Furthermore, some studies focused on either the autonomic, learning-based or cryptographic security countermeasures. The authors in [38], classified existing self-secure mitigation techniques for security attacks into different IoT layers. They also identified some information security goals in the field of IoT, which were grouped under five categories: i) confidentiality; ii) integrity; iii) availability; iv) privacy, and; v) authenticity.

The studies [26], [39]–[41] reviewed encryption mechanisms that provide security for IoT. While the study [26] provided a comparative study on symmetric cryptography, the authors in [39] analyzed and presented two main categories of encryption algorithms, namely symmetric and asymmetric, to establish secure communication. They highlighted both server-based and decentralized encryption protocol options for IoT. The authors in [42] compared different encryption primitives and proposed a suitable scheme using parameters that best fit user requirements. Some researchers surveyed recent developments in learning-based intrusion detection system for IoT. For instance, the studies [43], [44] reviewed machine and deep learning-based security solutions for IoT and identified the limitations of each method. The authors in [44] also provided future research challenges and directions. Table I recaps the key contribution of existing surveys on IoT security and provides a comparison with our survey together with exclusion/inclusion parameters.

The existing surveys and reviews on IoT security focused on security challenges and discussed measures, which only focused on a specific type of methodology. Other studies focused on security challenges concerning mobile-IoT, location-based or commercial IoT. Others yet focused on a specific type of security countermeasures such as either learning-based or cryptographic-based measures. However, the existing studies have not taken into consideration current IoT attack categories such as multi-layer attacks, security measures of IoT in terms of its characteristics and diversities. There is a need to undertake a holistic investigation of autonomic, learning-based and encryption-based IoT security countermeasures. To the best of our knowledge, the current study is the only survey that aims at providing a comprehensive and up-to-date analysis of security countermeasures within the current trends in cryptographic or encryption methods, learning-based strategies and autonomic approaches. The paper also aims to provide useful insights and opens a research gateway for future researchers who are interested in IoT security challenges and solutions.

TABLE I
RELATED SURVEYS ON IOT SECURITY

Year	Author	Contribution	multi-layer attacks	Learning methods	Autonomic approaches	Encryption methods	Methods of attack	Layer-based taxonomy
2015	Ashraf et al., [38]	Classifies and discusses self-secure techniques for IoT	×	×	✓	×	×	✓
2015	Nguyen et al., [39]	Analyzes and reports categories of encryption algorithm	×	×	×	✓	×	×
2017	Mushtaq et al., [42]	Compares different encryption primitives	×	×	×	✓	×	×
2017	Chen et al., [31]	Reports and discusses security solutions for location-based IoT	×	×	×	✓	✓	✓
2018	Al-Garadi et al., [43]	Discusses ML/DL solutions for IoT	×	✓	×	×	✓	✓
2019	Chaabouni et al., [32]	Addresses security issues and discusses ML-based solutions in network layer of IoT	×	✓	×	×	×	✓
2019	Hassija et al., [27]	Presents security solutions using fog, edge computing, block-chain and ML approaches for IoT	×	✓	×	×	×	×
2019	Hussain et al., [44]	Provides and analyzes learning-based security measures for IoT	×	✓	×	✓	×	×
2020	Sharma et al., [28]	Presents solutions for security, privacy, and trust for Mobile-IoT	×	×	×	×	×	×
2019	Nandy et al., [30]	Highlights several authentication methods for IoT	×	×	×	✓	×	×
2019	Chaabouni et al., [32]	Addresses security issues in network layer and discusses ML-based solutions	×	✓	×	×	×	✓
2020	Kim et al., [33]	Compares data sources from different IoT layers	×	×	×	×	×	✓
	Our Survey	Provides layer-based attack taxonomy and discusses three areas of security countermeasure	✓	✓	✓	✓	✓	✓

B. ORGANIZATION

The remainder of this paper is organized as follows. Section II provides an overview, architecture, enabling technologies and some state-of-the-art applications for IoT. Section III provides the IoT security challenges, security goals and types of security attacks. Section IV provides layer-based attack taxonomy for IoT. Section V offers state-of-the-art security countermeasures including learning-based methods, autonomic approaches and encryption techniques. Section VI provides discussion, and future research directions and Section VII concludes the study.

II. OVERVIEW, ARCHITECTURE, ENABLING TECHNOLOGY AND APPLICATION DOMAINS IN IoT

Despite the wide-ranging opportunities, IoT avails stakeholders and businesses, there are yet significant IoT security concerns that must be addressed. IoT applications generate a vast amount of data for individuals and organizations, which are prone to security attacks. Since low-power IoT devices are commonly deployed in hostile physical environments, more robust security approaches must be implemented in addition to conventional IT security approaches. This section provides an overview of IoT, introduces its architecture, enabling technologies, protocols and some state-of-the-art application domains.

A. OVERVIEW

IoT enables the interconnectivity of several heterogeneous devices and networks using different communication technologies. According to [45], [46], communication may occur between machine-to-machine (M2M) or thing-to-thing (T2T), human-to-thing (H2T) or human-to-human (H2H) through different means of connectivity. IoT aims to provide smart and advanced services to its users through information networks formed by consistent integration of physical objects (e.g., personal computers, smartphones, wearable devices, washing machines, fridge, lights, microwave oven, and medicines). The objects are interconnected or connected to the internet or humans and are capable of transmitting real-time information about patients, property, traffic, and electricity [47]. These smart objects are also capable of delivering the collected lightweight data around the globe. Devices equipped with actuators can extract data, process them and boost the communication efficiency among smart objects.

IoT is distributed and heterogeneous, and therefore, the issues related to security need to be given considerable attention. However, IoT is different from conventional IT in several contexts, including security. IoT also differs in terms of technology and deployment. IoT devices are connected under the constraints of low power and lossy networks (LLNs), which are weak in energy, memory and processing capabilities. Unlike typical IT infrastructure, IoT is globally connected through compressed Internet Protocol Version 6 (IPv6) [62] .

Figure 2 presents security attack scenarios of some key IoT applications. IoT applications are deployed in almost every aspect of our daily lives, including homes, hospitals and industries. Multiple sensors in an application area (e.g., smart home, smart hospital, smart industry and smart transportation) communicate with each other and transmit vital information. Considering a scenario where a driver uses a global positioning system (GPS) to navigate a destination in order to catch up with an urgent meeting; the car's GPS device will usually be connected to multiple devices and utilizes different networks, which are exposed to cyber-attacks. An attacker can potentially bypass the firewall and may launch a denial-of-service (DoS) attack, making the navigation service unavailable or send a wrong signal that misleads the driver. In another scenario based on the same figure, remote operation of the smart home appliances exposes private data to an attacker, or the smart lock of the home could be broken to gain access to home appliances.

In another scenario based on Figure 2, patients get treatment and medication at home or by the healthcare service provider from a remote hospital. However, the patient's sensitive information may be at risk of being stolen or manipulated by the invader who bypasses the hospital firewall, sitting either at the local network or on the cloud internet. The highlighted scenarios present issues that are related to hacking, terrorism, and sabotage, which could potentially affect large-scale intelligent IoT infrastructures such as electricity, hospitals, offices, industries and buildings.

B. ARCHITECTURE

Given the continuous development and expansion, IoT requires a universal and adaptable architecture that suits its heterogeneity and the diverse scope of its application. Currently, there is no universally adopted architecture. Several researchers have proposed many different architectures for IoT [48]–[50]. The three-layered architecture outlines the critical concept of IoT. Figure 3 presents a typical architecture of IoT, which is divided into three basic layers together with their functionalities. The layers are presented and discussed next.

1) APPLICATION LAYER

This layer consists of an array of smart IoT application solutions [21], [49], [51]. The IoT market has enormous potentials that attract the development of smart applications in almost every aspect. Many IoT applications have already been deployed in certain domains such as smart buildings, including homes and offices, smart cities, and wearable bands for health monitoring, smart traffic systems, environment monitoring, smart alarm system, and smart personal assistant. IoT application layer is the highest layer within the IoT architecture, which provides an interface between objects and networks. It offers a variety of functionalities such as data formation, presentation, monitoring of device conditions, notifications, alert, controlling device functions, management and processing of data, device performance optimization and autonomous operations, providing quality-of-service to end-users [52], [53]. A typical application layer includes a service support platform, middleware, computing and communication software [54]. A survey [55] presented facilities for practical applications of IoT. The main goal of the IoT application layer is to provide different application services to the end-users. Data Confidentiality, Integrity, and Availability (CIA) should be guaranteed at this layer by securing applications from unauthorized access,

ensuring software/logs integrity and keeping the application services available at any time. During the processing of sensitive data, issues such as illegal access and malicious modification of data may arise [56]. This layer could also be susceptible to a number of security attacks such as Spoofing, Message Forging, Virus and Worms among others.

2) NETWORK LAYER

This IoT layer is comprised of software, protocols, and technologies that enable object-to-object and object-to-internet connectivity [52]. It is mainly formed using either local area network such as wireless and wired network, personal area network (e.g., ZigBee), near field communication (NFC), Bluetooth and wide area networks such as GSM, LTE, 5G, and cloud computing [49], [51], [57]. The variations of the IoT communication model have been outlined in [58], as M2M communications, machine-to-gateway model, machine-to-cloud communications, and back-end data-sharing model. The main function of this layer is to transmit gathered data in the form of a digital signal, which is collected from the physical layer of corresponding platforms via a connected network. This layer is vulnerable to a number of security threats and attacks [20]. Common attacks in this layer include Denial-of-Service (DoS), Sinkhole, Hello Flood, Blackhole, to name a few. It is essential for the network layer to have communication security for secure data transmission over a public network [59], [60].

3) PHYSICAL LAYER

The bottom layer of IoT architecture is known as the physical layer. In IoT, this layer is also referred to as the perception layer [20], [49], [50]. It includes physical world objects and virtual entities. The main task of this layer is to collect data from the environment through various sensors. IoT devices are embedded with electrical and mechanical hardware components such as sensors, antennas, actuators, processors [52]. Smartphones, RFID technology [21], [51], wearable devices are capable of processing, identifying, connecting, communicating and storing data. In the perception layer, the sensors or RFID convert the collected raw data of the physical objects to the readable digital signals. IoT objects sense and gathers data from the physical world such as temperature, humidity, proximity, to name but a few. However, this layer of IoT is prone to a lot of security attacks such as Jamming, Tampering and Collusion [20].

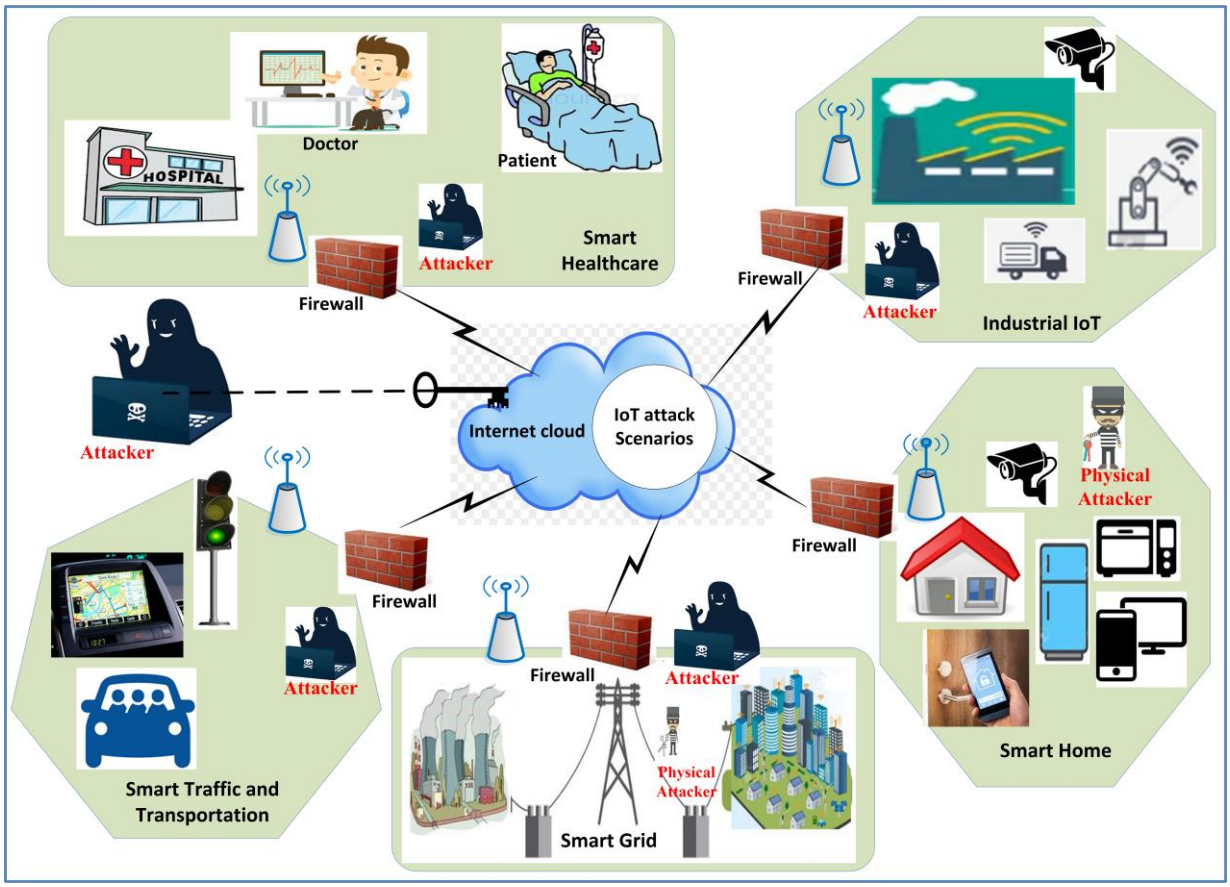

FIGURE 2. IoT Security Attack Scenarios in Different Application Areas.

C. ENABLING PROTOCOLS AND TECHNOLOGIES

Numerous protocols interoperate, and thus, an appropriate communication system architecture should be used to ensure interoperation. Nevertheless, there are still issues with interoperability among diverse network technologies. Authors in [61] state that the standardization of the latest progress is the only way to the future development of IoT. Evolving new IoT-based

protocols and technologies will play a vital role in the coming years. The protocols used in conventional internet for data sharing are not compliant options for low power IoT constraint. Therefore, there have been some standardized protocols for IoT to connect smart things and end-user applications. IoT protocol stack, enabling elements are presented in Figure 3. This figure also demonstrates the functionalities of the protocols for each layer of IoT.

The Constrained Application Protocol (CoAP) is a widely used ultralight standard for application layer of IoT. On the other hand, CoAPs are the secure version of CoAP. CoAPs utilizes Datagram Transport Layer Security (DTLS) to protect data between two applications [48], [52], [62], [63]. Message Queuing Telemetry Transport, MQTT for Sensor Networks (MQTT-SN), Data Distribution Services (DDS), Extensible Messaging and Presence Protocol (XMPP), Advanced Message Queuing Protocol (AMQP) are some other application layer protocols for IoT [52], [63]. A Quick Constrained Application Protocol Internet Connection (QUIC) is an IoT transport layer protocol used in experimental phases [64]. QUIC was designed by Google to offer security protection, flow control over User Datagram Protocol (UDP) and to avoid congestion as well as reducing transport latency by using congestion control mechanisms similar to TCP. IPv6 is one of the key internet layer protocols for IoT [62], [65]. IPv6 offers end-to-end IP datagram transmission for the packet-switched network through multiple IP networks. IPv6 over Low Power Wireless Personal Area Network (6LoWPAN) is low power and low-cost communication network, which makes IoT devices to be connected to the internet through IPv6. Routing Protocol for Low Power and Lossy Networks (RPL) is a standardized IPv6 protocol for the constrained IoT networks [62]. RPL is the IPv6 routing protocol standardized for IoT [15], [36].

IoT is envisioned to integrate different wireless technologies. Bluetooth Low Energy (BLE), Z-Wave, EPCglobal are some of the IoT physical layer protocols. RFID and NFC [66]–[69] are ultralight technologies for short-range communication for IoT. IEEE 802.15.4 is the Low-Rate Wireless Personal Area Networks (LR-WPANs) [69] utilized for IoT due to security, authentication, encryption, reliable communication, high message throughput, and to accommodate a huge number of nodes [70]. Bluetooth operates in the 2.4 GHz frequency and is one of the key technologies for short-range communication. IEEE 802.11 is another physical layer specification for Wireless Fidelity (WiFi) or (WLAN). The energy consumption is higher in WiFi than that of Bluetooth and ZigBee [61]. Cellular technologies such as 2G (GSM), 2.5G (GPRS), 3G (UMTS/WCDMA, HSPA), 4G LTE, 5G can also be used for IoT communication. As all the protocols for IoT are designed for resource-constrained devices and networks, these protocols could be susceptible to security attacks to a large degree. The constrained devices are vulnerable to attacks from inside the 6LoWPAN and internet. Therefore, lightweight security solutions are to be developed for these constrained devices and networks [71].

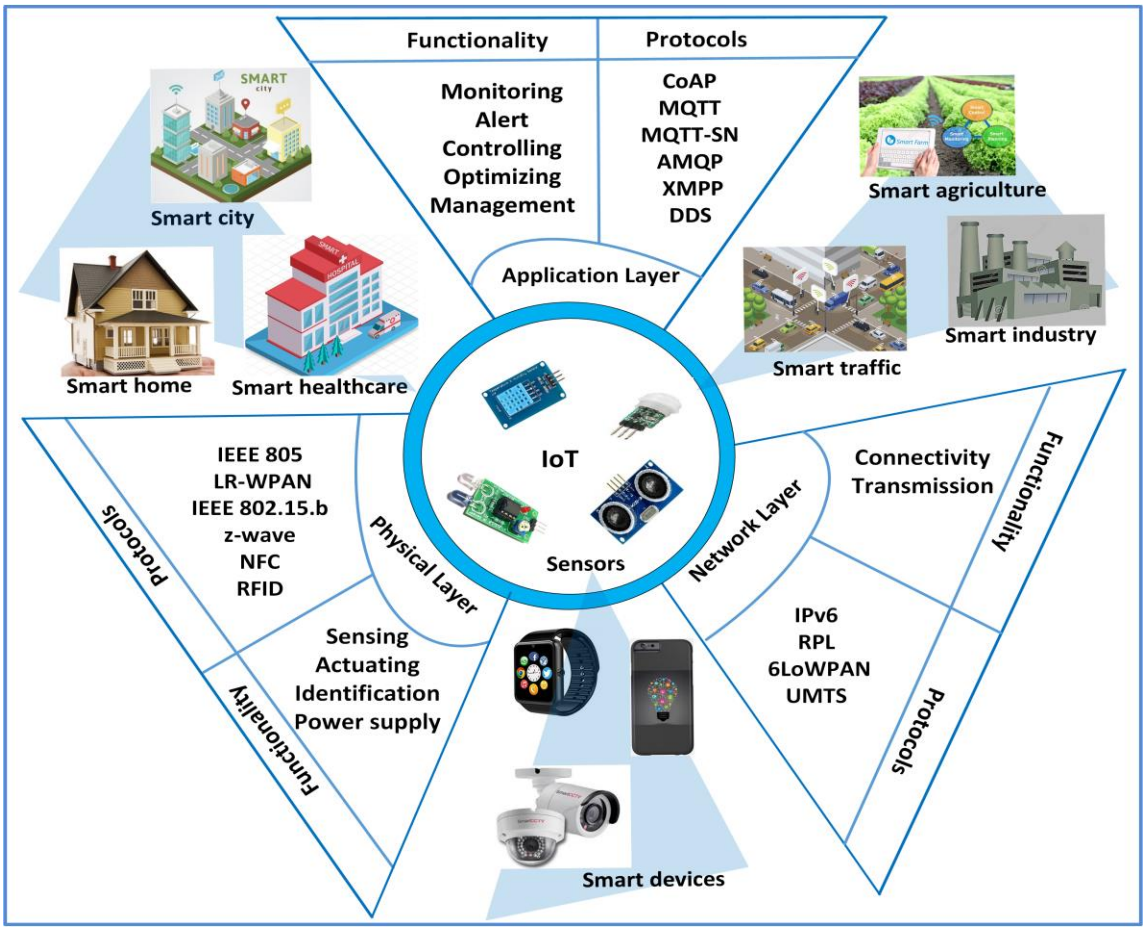

FIGURE 3. An overview of IoT, architecture, functionalities, enabling technologies, and applications.

D. IoT APPLICATION DOMAINS

IoT applications have become an integral part of our everyday lives. These applications are growing rapidly. IoT applications suffer from a number of security threats, privacy and trust issues, which vary from application to application, environment and industry. Effective security solutions should be enforced on different IoT domains based on the nature of applications and functionalities to ensure secure communication and let people enjoy the complete benefit of IoT without compromising their privacy. This section presents some recent application domains and discusses their respective security issues, trust and privacy.

- **Smart Home:** Some of the modern homes are equipped with smart and automated appliances, such as smart lighting, refrigerator, washer, air-condition, electric meter, alarm system and CCTV. For ensuring safety and security, these homes are powered by smart cameras, sensors, smart locks and alarm systems. These smart appliances can be operated through the internet from long distances. The usage of such smart technologies provide a high level of comfort in smart homes and enhance overall security, trust and privacy while reducing overall expenditure [72], [73]. To ensure security and to protect smart houses from theft or intrusion, criteria such as confidentiality, auto-immunity, and reliability must be met [72]. IoT devices installed in smart homes should be password-protected, and user login must be confidential.
- **Industrial IoT:** The cyber-physical system is the basis of industrial IoT, which is capable of real-time monitoring, diagnosing and controlling physical process and production remotely. IoT-equipped smart industries and factories optimize production processes, enable the manufacture of smart products and provide knowledge-based smart services by utilizing resources with the help of the data gathered by the IoT system. The smart products are usually powered by RFID for digital identity that also can collect and store data [74]. However, the industrial IoT and its products attached with the digital entity are vulnerable to many security issues such as trust, privacy and confidentiality. They also introduce challenges such as standardization of production system, social and legal aspects. The diverse industrial IoT devices demand highly scalable addressing system, security solutions and data privacy. Due to resource limitations, the industrial IoT architecture demands low-cost, low-powered infrastructures, yet fully integrated with robust security solutions.
- **Smart City:** The concept of a smart city comes from the integration of different IoT applications in various sectors. In a smart city, the integration of multiple services supports its stakeholders in a distributed and dependable manner [75]. However, providing privacy and trust among the stakeholders in the smart city applications remains an important issue. There are security issues related to hacking, terrorism, physical damage which could destroy the infrastructure of smart city applications in areas such as electricity supply, healthcare, corporate offices, factories and traffic systems [76].
- **IoT Healthcare System:** It is one of the most prominent and fascinating application areas of IoT [77]. The smart hospital-based treatment or remote healthcare services have gained popularity in recent years. IoT medical services such as distant health monitoring, elderly care, chronic healthcare and fitness programs are some of the potentially rising applications [78]. However, a patient's private and sensitive information may be at risk to be stolen or manipulated. Patient's personal information is confidential, and thus, it is important to secure them from exposure to any unauthorized access. If the medical report of a patient is leaked and altered, the doctor may end up treating the patient erroneously, which can be lethal and life threatening for the patients. Patient's data privacy and authentication are of immense importance; therefore, medical applications of IoT should be highly secured [79].
- **Smart Traffic System:** The use of RFIDs and various sensors make urban driving pleasant and traffic management more efficient. Smart traffic applications of IoT give people a sense of 'living in the future'. An IoT-enabled traffic system provides route information such as a number of cars in a certain route or lane; parking information such as availability and directions to the parking space; public transport information such as the number of occupants and availability of seats on a bus or train. Ultrasonic sensors are already in use in urban vehicles for safe driving [80]. However, the automation of the system may bring security and trust issues for passengers [81]. As smart cars, buses, trains among others are connected to the internet, the passengers' data become exposed to the risk of being compromised.
- **Smart Grid:** The smart electrical supply system is known as smart grid, which is mainly a network of electric transmission lines, transmitters, substations to distribute electricity across homes and businesses from the power plant in the most efficient way. Smart meters, sustainable energy resources, smart machines and efficient energy properties are some of the power functions of a smart grid [72], [82]. The use of IoT in an electric grid makes the energy distribution and management much more efficient through two-way communication and reduces the impact on climate [83]. Technological improvements in smart electric grid systems increase their security vulnerabilities and threats. Authentication, confidentiality, trust, integrity, and availability represent the key areas of concerns that

should be addressed when dealing with a smart power grid.

- **Smart Farming:** Integration of different sensors and RFID technologies make conventional agriculture, animal and fish farming smarter. Various sensors are capable of monitoring temperature, humidity, soil moisture, and microbial contaminants in smart farming [27]. Sensors and RFID attached to the animal's body or fish farm are able to monitor health conditions, keep track of their activities and notify the stakeholder remotely. However, smart farming industries are prone to several security issues. The agricultural products can be damaged, or fishes and animals can be carted away if the security of such applications is not ensured.

III. SECURITY CHALLENGES, GOALS AND METHODS OF ATTACK IN IoT

Using the conventional and existing security approaches directly in the resource-constrained IoT devices is not straightforward. In short, the security approaches, models and architectures of the conventional network are designed based on the users' perspective, which may not always be suitable for M2M communication. The security threats or attacks may be similar for both networks, but the solution techniques and approaches are different in each network [84]. The major security challenges, security goals and the methods of security attacks are presented next.

A. SECURITY CHALLENGES

This section provides the security challenges while implementing security in IoT for application, network and physical layers. Table II briefly summarizes the comparison between IoT and conventional IT security challenges.

1) APPLICATION LAYER CHALLENGES

Heavyweight software or security solutions may not be appropriate for IoT devices. Therefore, it is worth considering the following limitations before implementing security modules in IoT devices.

- **Embedded Software:** Either a lightweight General-Purpose Operating System (GPOS) or Real-Time OS (RTOS) is embedded in low memory IoT devices [85], [86]. These IoT operating systems are equipped with tiny network protocol stacks, which may not come with adequate security modules. Hence, lightweight, robust, and fault-tolerant security modules should be designed for such thin software and protocol stacks [86], [87].
- **Security Patch:** The deployment of IoT devices might be in a remote area. The sensing devices may not receive security patches or software updates without affecting functional safety. A high cost may incur to update a security patch [8]. Mitigating potential security issues would not be possible remotely as IoT OS and protocol stack may not be able to receive and incorporate a new security patch.
- **Device and Data Volume:** A large number of applications generate an enormous volume of data which impact the security and privacy on the data and devices [88]. A report shows that less than 10,000 household devices are capable of generating 150 million discrete data points per day [89].

2) NETWORK LAYER CHALLENGES

IoT network layer provides functionalities such as communication and data routing among different devices across the internet and within 6LoWPAN networks. However, the IoT network layer is prone to different routing attacks due to the following limitations.

- **Topological Changes and Mobility:** IoT devices are mobile in many cases, and mobility is one of the main features of IoT. IoT devices may leave or join a network from anywhere at any time. The conventional security algorithm may not be suitable for such dynamic topological changes.
- **Scalability:** An increasing number of new, dynamic IoT devices are daily springing into existence, and more devices are being connected to the global network. Existing security schemes and their properties are not scalable and suitable for such increasing number of IoT devices.
- **Diverse Communication Medium:** Smart devices connect to private, public, global, and local networks through a range of wired and wireless communication mediums. Such diverse properties of wired and wireless links make it complicated to develop a comprehensive security scheme.
- **Multi-Protocol Networking**: IoT devices might use IP or non-IP or combination of both network protocols at the same time for communication. It is hard to make a conventional security algorithm suitable for IoT devices considering multiple communication protocols.

TABLE II
COMPARISON BETWEEN IT AND IoT SECURITY CHALLENGES

Parameter	IT	IoT
Power, Memory, and Processor	Powerful	Constrained [90]
Environment	User-friendly	Hostile, dynamic and heterogeneous [91]
Diversity	Mostly homogeneous	Heterogeneous [92], [93]
Data volume	Low	Very high [89], [94], [95]
Security Requirement	Lightweight/ Heavyweight	Lightweight [3], [90]
Embedded software	Heavy OS and software	Lightweight GPOS/RTOS [85], [86]
Protocols used	HTTP, TCP	6LoWPAN, CoAP, RPL, DTLS [62]

3) PHYSICAL LAYER CHALLENGES

The IP-connected IoT heterogeneous devices are mostly resource-constrained, which makes it more prone to security threats and attacks. However, the existing heavyweight security solutions are not suitable to implement in IoT devices due to the following characteristics.

- **Processor, Memory, and Power:** The battery-driven IoT devices are energy inefficient, and due to the limited

power, the processor/CPUs have relatively low clock cycle. Hence, devices are not computationally powerful. Heavy cryptographic algorithms cannot be implemented in such devices. Limited RAM and flash memory are embedded in an IoT device. Therefore, memory-efficient security schemes should be ported. The device may run out of memory after booting up the operating system if the heavyweight security schemes designed for the conventional network are implemented in IoT. For example, the classical public-key cryptography algorithms are heavyweight for key management in constrained IoT [59], [97].

- **Packaging:** Some of the IoT applications might demand placements in remote locations, which may remain unattended. An adversary may capture and tamper with the IoT devices. Cryptographic information may then be extracted to modify the programs or to replace the devices with malicious nodes. Therefore, the tamper-resistant packaging of such IoT devices is required to overcome this issue [87].

B. SECURITY GOALS

The security goal/necessity of IoT is discussed in this section. The traditional and common security goals include Confidentiality, Integrity, and Availability (CIA). However, apart from this CIA triad, other requirements such as privacy, lightweight solutions, authenticity, and standardized policies have become very important. Figure 4 shows the security goals for IoT including lightweight security solutions, privacy and CIA triad. To achieve a secure communication for IoT, the following security principles should be considered.

1) LIGHTWEIGHT SOLUTIONS

Lightweight security solutions can be introduced as a unique feature since IoT devices are considered computationally less powerful and embedded with limited memory. The lightweight approach must be considered as a security requirement while designing, developing and implementing an encryption or authentication protocols for IoT [18]. For example, RFID tags in e-passport can suffer from un-traceability attacks; hence, lightweight yet robust security solutions must be designed for such ultralight protocols. As the security algorithms or protocols are meant to be run on IoT devices, these must be compatible with the device's limited capabilities.

2) AUTHENTICITY

By addressing the constraints of IoT, it is essential to verify and validate the users involved in communication. A comprehensive review of authentication mechanisms has been presented in [30]. A lightweight authentication mechanism [88] is proposed recently for resource-constrained devices. RFID tags and NFC are few examples of such advanced innovations, which IoT devices may benefit from as an authentication scheme. An NFC based authentication mechanism has been proposed [98] to ensure that energy and processors are not in use at end nodes. Other than these, trust management, data, device, and user authentication are also important.

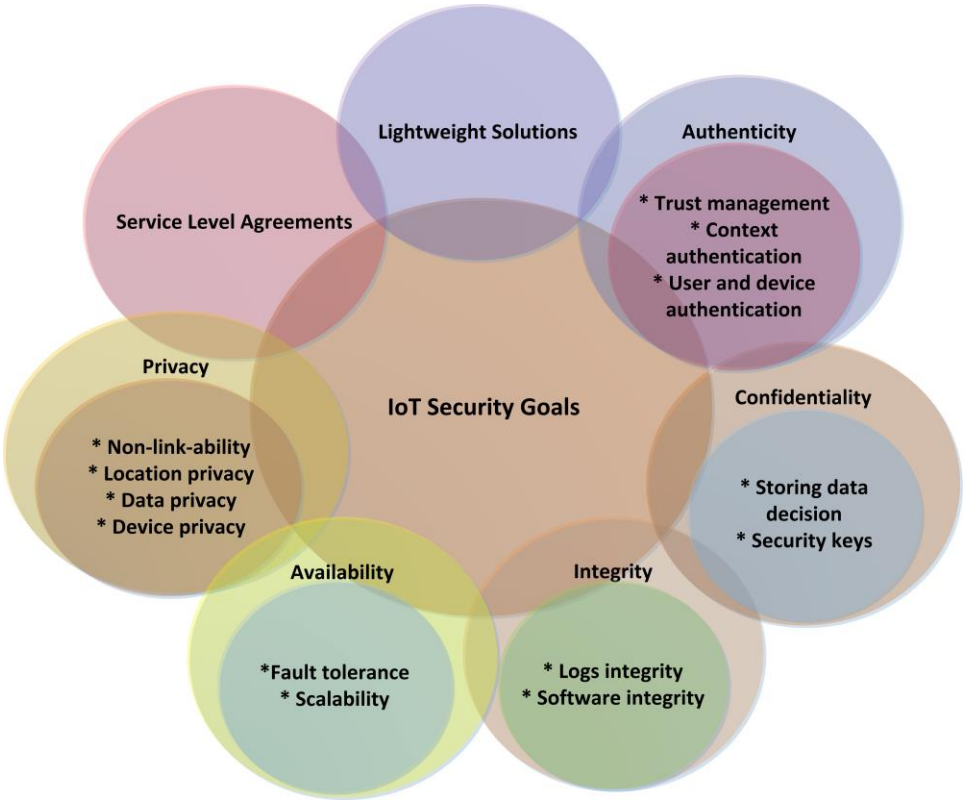

FIGURE 4. Security goals of IoT.

- **Context Authentication:** Obtained sensed data and control information, functional properties, and states of the devices are to be authenticated as a pre-requisite.
- **Trust Management:** Trust management plays an important role as it reduces risk factors and allows customer acceptance. Adaptive routing in the smart grid is entirely trust-based schemes for IoT components which is reported in [99]. Trust management does not only contribute to IoT security, but it also improves the overall network performance [100]. There are different data aggregation algorithms or machine learning approaches available to obtain trustworthy data in IoT [3].
- **User and Device Authentication:** IoT devices and the central unit should autonomously be able to authenticate a user identity that is demanding a certain action. In this process, a single-sign-on mechanism can be applied as once authenticated the users may interact with several devices.

3) CONFIDENTIALITY

Confidentiality is one of the key features for securing IoT. All information must be protected from unauthorized nodes during any transmission. This can be done by using a shared key, where both sender and receiver use this key to encrypt and decrypt data.

- **Storing data:** The autonomic decision should be made to protect confidentiality during storage of vital data locally and in the cloud.
- **Security Keys:** To upgrade the security key is challenging due to the constrained nature of IoT in order to provide confidentiality. Ample research effort is required to overcome the challenges to support the autonomic version of such key management schemes. Symmetric key schemes may support IoT with acceptable overhead [38].

4) INTEGRITY

Data integrity ensures that the information remains unchanged during transmission. A symmetric cryptographic algorithm is typically used to help data under transmission by creating signatures for them. Another approach, namely, Message Integrity Check (MIC), is used to verify the integrity of received data. An autonomic security solution may provide an acceptable level of data integrity for IoT regardless of inadequate resources [38]. The autonomic decision-making integrity components are as follows.

- **Logs integrity:** In case any alteration is observed, the autonomic system must have the ability to reveal the path by generating activity logs. The logs can be stored locally or centrally and for a short or long period of time [38].
- **Software Integrity:** The system must ensure the integrity of the software that devices will run. It also should be able to monitor if any device is captured or pseudo-data is flooded on the network [38].

5) AVAILABILITY

Availability guarantees that the entire system, its components, functional properties, and required services are available at any time. The availability of these services and components may be hampered due to security attacks [18], [101]. Such attacks may physically harm IoT nodes and networks. The connected things should be available and functional whenever they are required. The following security goals on availability must be considered for constant data and system availability.

- **Fault Tolerance:** The system must be able to use the self-protection approach along with self-healing in case of a failure or an attack.
- **Scalability:** IoT nodes can be organized hierarchically to support scalability. The packet flow can be centralized to achieve this feature [102].

6) PRIVACY

Privacy refers to the state or condition in which data or service is meant to be accessed by an individual. To keep the nodes scalable and to consider various IoT applications, a robust privacy policy is required to be developed. IoT devices are equipped with RFID tags, which can be tracked easily. The privacy of those devices should be protected. Several research works have been done to provide privacy for IoT [103]–[107]. The privacy goals are categorized as follows [38].

- **Non-Link-Ability:** It refers to a specified private data that is not linkable to any user. Unauthorized users should not be able to create a profile from the personal data of other users. Group-signature-based mechanism is proposed to solve privacy non-link-ability issues in [107].
- **Location Privacy:** It guarantees that the current or previous location of an IoT device is not revealed. An efficient privacy prevention framework for location privacy is presented in [103]. The authors proposed anonymous authentication for wireless body area networks. The proposed framework achieves low computation cost during the authentication process.
- **Data Privacy:** Wearable devices connect the human body to the internet, thus personal information (e.g., healthcare) should be kept secured.
- **Device Privacy:** RFID tags make the sensor nodes to be traceable and identifiable. Anonymous communication is required to hide the identity of devices for resource-constrained communication protocols. The authors in [106] proposed a decentralized identifier based method to provide privacy for IoT devices. The authors claimed that the model could be deployed in small IoT devices.

7) SERVICE LEVEL AGREEMENTS

In order to protect and transmit data in an efficient way, there must be standardized policies and mechanisms to enforce the policies. It is also important to ensure that the standards and policies are applied to every entity in the network. All services should clearly identify a Service Level Agreement (SLA), which is one way of maintaining the policies and standards. Considering the nature of IoT, the classical SLAs may not be applicable; thus, there should be an autonomous decision on policies to meet SLAs according to diverse services. These policies are to be enforced in order to foster trust in the IoT paradigm.

C. METHODS OF SECURITY ATTACK

The representation of different types of attacks based on the properties of IoT assets and their available solutions are provided in this section. The adversary may be an insider or outsider of a network and can be a threat to these assets, such as communication channels, a protocol stack, devices, and personal information. Based on device, network, location or other

properties, the adversary performs malicious activities to interrupt IoT services, obtain unauthorized access or physically damage the device. The following sections provide the taxonomy of types of security attacks based on IoT assets and their properties according to the literature [87].

1) DEVICE PROPERTY

IoT devices are heterogeneous. Therefore, an invader may attack IoT devices based on device properties. Two such methods are given below.

- **Low-End Device Attack:** Devices with low memory, power and computational capabilities are considered as low-end devices. The attacker uses such devices to launch attacks on other IoT devices. For example, an adversary gets unauthorized access to a smart TV or smart refrigerator and may launch several attacks using wearable IoT devices such as smartwatch which may threaten privacy, integrity or confidentiality [108].
- **High-End Device Attack:** A high-end device refers to a powerful and fully functional device. An adversary may launch attacks using high-end devices (i.e., PC, laptop) in order to gain access and cause damage to IoT devices and networks from anywhere.

2) LOCATION PROPERTY

IoT devices are connected globally and are prone to attacks from the internet or within 6LoWPAN networks. The methods of such attacks are as follows [109].

- **Internal Attack:** An adversary's attack from a native network either using his/her own device or a compromised legitimate device. Such attacks may include routing attacks, namely Flooding, Blackhole, and Sinkhole attacks.
- **External Attack:** Initiating an attack on IoT devices or networks, the attacker might be deployed outside and far from a native network. Examples of such attacks are Brute-force, malware, Secure Sockets Layer (SSL), and Domain Name System (DNS) attacks.

3) ATTACK LEVEL

An adversary may attack IoT devices or network at different levels such as active or passive in order to either disrupt usual functionality or just to acquire vital information. The methods are described below.

- **Active Attacks:** The direct attacks to interrupt the regular serviceability of IoT networks or devices are known as active attacks. DoS and Blackhole attacks are two examples of such attacks.
- **Passive Attacks:** This type of attacks are launched to gather important information from IoT networks and devices, but the normal functionality of a device or network is not disrupted. They are also initiated to disrupt the IoT privacy such as eavesdropping and monitoring of data transmission

4) ATTACK STRATEGY

An attacker may belong to different interest groups. They may attack the IoT device or network using different strategies.

- **Physical Attacks:** The attacks are launched in order to cause physical damage to IoT devices or change device configurations. Malicious Code Injection and Tampering are examples of physical attacks.
- **Logical Attacks:** The attacks are initiated in order to make IoT devices or networks dysfunctional without doing any physical damage to them. Traffic analysis of the communication channel is the example of a logical attack.

5) DAMAGE LEVEL

IoT devices, networks, and applications are prone to a multitude of security attacks, which may cause different levels of damages. They may range from information leaks, service disruptions to physical damages of the IoT device. Two such methods are provided as follows.

- **Service Unavailability Attack:** In the context of a service shut down, the power outage and other resource exhaustion may occur naturally, which in turn makes service unavailable. Service may be interrupted by such attacks (for instance, DoS attack). Thus, recovery mechanisms for such interruptions should be available [71]. Such intrusions can be detected using an effective Intrusion Detection System (IDS).
- **Interruption Attacks:** In this type of attack, an invader sits between two IoT nodes, intercepts the communication and tricks them by communicating with both. In other words, the attacker listens to the private messages which are transmitted through private communication links. Eavesdropping, Alteration, Fabrication, and Man-in-the-Middle (MitM) attacks are examples of such kinds. These attacks may mislead or create confusion among IoT users. The intruder may alter or fabricate additional data. Such attacks can be made either externally or internally. RFID devices are vulnerable to such attacks.

6) HOST-BASED ATTACKS

The devices used in IoT are embedded with software that may contain private information, cryptographic keys and other sensitive information. The data can be targets of the attackers. Some of these attack methods are as follows.

- **User Credential:** An adversary may trick a user into discovering their personal credentials such as usernames and passwords. User credentials should be protected or be shared in a secured manner.
- **Software Compromise:** IoT devices and their embedded software are not much powerful. Therefore, the operating system and other software might be vulnerable to security threats. An adversary may take advantage of that and compromise the embedded software.
- **Hardware Compromise:** An adversary can damage IoT devices by extracting hardware credentials such as keys, data, or program code that are embedded in the devices. Physical access is usually required to initiate such attacks. IoT devices should be tamper-resistant in order to remain protected from such attacks.

7) PROTOCOL ATTACKS

Malicious attackers compromise standard protocols of IoT devices and networks in order to disrupt communication among the devices. Examples of such attacks include the following.

- **Protocol Deviation:** An adversary breaches and diverges from standard communication or application protocols and becomes an insider in order to launch attacks.
- **Protocol Disruption:** An intruder may disrupt standard protocols such as synchronization, data aggregation or key management protocols from inside or outside of a network.

IV. LAYER-BASED ATTACK TAXONOMY

IoT architecture comprises of different technologies which work independently to make a complete system. In the previous section, we considered the IoT's three-layered architecture. In this section, we classify IoT attacks based on the three-layered architecture that consists of application, network and physical layers. Security attacks may lead to millions of dollars in losses to large business and intellectual property theft. The following sub-sections present the proposed attack taxonomy, which has been summarized in Figure 5.

We have classified IoT attacks based on application, network and physical layers. Some attacks are categorized as multi-layer/dimensional attacks as they exploit more than one layer of the IoT architecture; for instance, DoS or cryptanalysis attacks may take place in application, network and physical layers of IoT. Table III provides an analytical comparison of different attacks in different IoT layers, the method of launching them and the impact of those attacks on IoT.

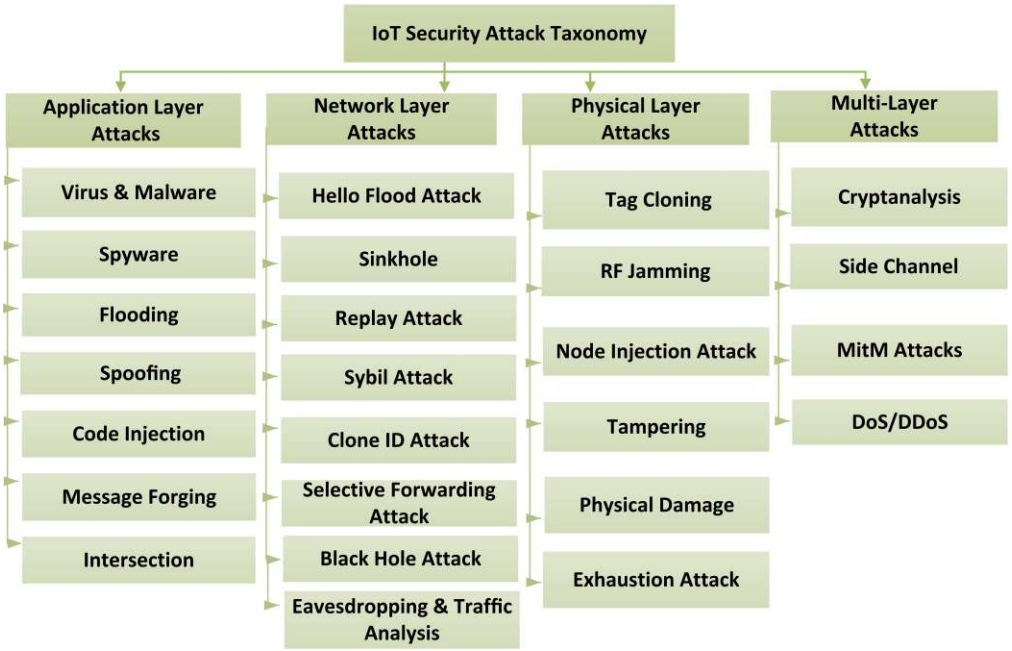

FIGURE 5. Layer-based IoT security attack taxonomy.

1) APPLICATION LAYER ATTACKS

Since global standards and policies are yet to be established for IoT to govern the development and interactions for IoT applications, IoT application layer is still susceptible to many security attacks. Diverse applications of IoT use different authentication techniques, which makes it difficult to integrate them in order to ensure authentication and data privacy. The number of applications is growing, and a huge number of devices are being connected that will share a tremendous volume of data. Applications, which analyze those data or information, may have a large overhead and service may become unavailable due to security attacks. The major attacks on the IoT application layer and their impacts are described below.

- ***Virus and Malware*:** These attacks are targeted at the system with the goal of breaching confidentiality. They usually occur in the form of applications such as Trojans, spams, and worms or other viruses [36], [110]. In IoT networks, smartphones, sinks or gateways and other high-end IoT devices are significantly at higher risk of these kinds of attacks than sensor-based motes. Furthermore, Bluetooth technologies such as 802.15.4 enabled devices are at high risk [38]. Therefore, mitigation of such viruses and malware in IoT applications must be taken into serious consideration.
- ***Spyware*:** Spyware is a program that is installed on users' IoT devices without the users' consent. The main goal of this attack is to spy or monitor users' behavior and gather sensitive information such as user IDs, passwords, keystrokes, and credit card information. Spyware generally does not cause any damage to the IoT devices or users directly; it mainly steals private information and sends back to the distributor [36]. The information is then used as the basis for marketing analysis or pop-up ads. Traditional spyware detection approaches are signature, behavior, and specification-based techniques. Signature-based techniques detect only known spyware; therefore, unknown spyware instances remain unattended [110].
- ***Spoofing*:** An attacker may impersonate a node to launch a spoofing attack. A spoofing attack is one of the high-risk attacks due to its attacking method. With a suitable portable reader, a transmission might be recorded. As the attacker impersonates the node, the retransmission might appear from a valid node. This attack may exist in all three IoT layers. Spoofing attacks by impersonating of nodes are categorized as the attack of authentication, and it also violates the privacy principle [111].

- ***Code Injection*:** An attacker inserts malicious code into a smart application/system by misusing faulty programs [101]. The attacker launches such attacks in order to gain access, and steal users' sensitive data, take over the system control or transmit worms [56]. Code injection attacks may take place in a variety of forms such as HTML script injection and shell injection. This attack may result in compromising users' privacy, or a system may lose control, thereby resulting in a total system shutdown.
- ***Message Forging*:** This attack occurs when a malicious node modifies or creates a message to deliver contents other than the original. It can be classified as a type of Replay attack in the case of modifying information synchronization.
- ***Intersection*:** This attack is also known as a composition attack. It targets the system's privacy by gaining secondary information from the system [25], [112]. The attackers gather such information from third party sources or public records [113]. The adversary targets and makes use of the non-linkable element. The anonymized data of the privacy information from different sources are then being used to link them.

2) NETWORK LAYER ATTACKS

IoT network layer communication is different from that of conventional internet due to M2M communication between heterogeneous devices. This layer may suffer from security compatibility issues and is prone to different security attacks such as Hello Flood, Sybil and Blackhole attacks. Examples of such attacks are as follows.

- ***Hello Flood*:** Message flooding is one of the major attacks in the network layer, where, an attacker aims to exhaust network or node resources such as battery or bandwidth by sending a multitude of route establishment requests [57], [114]. Destination Oriented Directed Acyclic Graph (DODAG) Information Object Message, namely DIO, is used for advertising information about destination/root that is used to build the topology of RPL. Any node that received a hello message considers that it originates from within the network and marks it as a communication route. In this case, an attacker or intruder whose intention is to place his/herself as a neighbor of other nodes in the network may convince other nodes that it is a normal node. It means the attacker node will broadcast a hello message to all nodes on the network to let them know that the attacker is a neighboring node [57]. This may lead to bandwidth, and network throughput inefficiency as the attacker drops the incoming packets, and therefore, that packet(s) will be lost. Hello Flood may also result from unequal transmission areas. It is considered a low impact attack.
- ***Replay Attack*:** This attack occurs commonly during synchronization to mislead the destination node such that a malicious node stores transmitted information, and only to retransmit it at a later time. Missed frames retransmission request is usually made by transmitting packets repeatedly across a network with the sequence numbers to senders and receiver nodes. For example, it may occur during communication between an RFID reader and a tag. This attack exhausts network/system resources such as RFID and back-end database resources (memory, battery and processor). Additionally, the adversary may broadcast the radio signal in order to gain reader grant access [115]. Replay attacks are classified as high-risk attacks, but they can be mitigated and prevented relatively easily. However, network efficiency will drop if the mitigation of this attack fails.
- ***Sinkhole*:** In this kind of attack, an attacker trespasses and compromises a central node of a network in order to make it unavailable which leads to packet dropping as well as DoS attacks. The risk level of sinkhole attacks is higher than that of tempering attacks, where a few numbers of nodes are compromised. Regarding the infrastructure-based system, the sinkhole attacks could control the whole network.
- ***Sybil Attack:*** Sybil Attack is launched by creating a node and presenting its own numerous identities in the network in order to gain huge influence, which in turn leads to the elimination of original active nodes from the routing table. Here, the system's weakness depends on a few factors such as the ease with which those multiple identities are created, the level of influence to which the system agrees to take inputs from a trusted entity, which is not linked to a chain of trust. A survey on Sybil attacks and its available defense mechanisms for IoT is presented in [116]. Based on the attacker's skills, the authors categorized Sybil attacks into three different types, namely, SA-1, SA-2, and SA-3.
- ***Clone ID*:** The name implies that the adversary clones the identity of legitimate IoT node in order to gain access to user data traffic [117]. The malicious clone node can be identified by storing the geographical location and identity of each node at 6BR (6LoWPAN border router). It can also be traced, using a distributed hash table.
- ***Selective Forwarding (SF) attack*:** In SF attacks, a malicious attacker enters into a network and drops selective packets. The adversary casually drops some packets and selectively forwards some to the next node. IoT networks are lossy by nature; therefore, it is difficult to identify the real reason for packet dropping [79]. This may lead to bandwidth deprivation and delay in the entire network [118]. This can result in compromising availability and confidentiality. Possible solutions to this attack may include redundancy checks and probing. Some solutions focus on providing network complete recovery, whereas others try to lessen the damage being caused [118].
- ***Blackhole Attack*:** During a Blackhole attack, the malicious node drops all the packets that it encounters and the entire network operations get affected. This attack is classified as a high impact attack as it absorbs all routing information. An intruder floods out malicious routing information to claim the best route to the destination [57], [62]. The sender then chooses the malicious route to transmit the packets. The attacker frequently sends fake route-reply (RREP) to the sender. The source node keeps transmitting its packets through the malicious route, the attacker drops all the packets, and he/she does not forward any traffic to the destination.
- ***Eavesdropping/Traffic Analysis*:** These attacks can be active or passive. They act as pre-requisites of other types of

security attacks. A network is usually unaware of the existence of such attacks [119]. In active eavesdropping, an attacker transmits a control message to initiate the attacks, and the replies from the destination device are analyzed further to pave the way for other attacks. Passive eavesdropping, on the other hand, overhears the communication traffic to extract vital information from the transmission medium to launch other attacks. These attacks may affect users' privacy and data confidentiality. Information can eavesdrop at either M2M, network or cloud layers [120]. Eavesdropping attacks are relatively easier on the M2M layer; however, the attacker can overhear only a selected part(s) of the system and most of the cases raw data is not as useful [121]. IoT devices on a wireless medium are greatly vulnerable to such attacks. MitM attack is one of the examples of an active attack, where the attacker acts as a router and connects with both sender and destination nodes independently, and transfers information between them. The vital information is captured to analyze further and modify.

3) PHYSICAL LAYER ATTACKS

The main components of the physical layer are sensors, RFID tags, WSNs, cameras, and so on. This layer of IoT suffers from a number of security attacks and threats. There are some solutions available to those attacks. However, implementing autonomic security solutions in the hardware at the physical layer is more robust and faster. Complex schemes are usually more costly and should be avoided. Lightweight approaches should be implemented in order to increase device lifetime and reduce complexity. Attacks in the physical layer are described as follows.

- ***Tag Cloning*:** RFID tags can easily be cloned by an adversary. It may be done by attaining the required information by direct access to a device or using reverse engineering [56]. The literature [101] presented a tag cloning attack where an RFID reader is unable to distinguish between genuine and compromised tags.
- ***RF Jamming*:** Radio Frequency (RF) jamming causes the sharing of wireless bandwidth to be ineffectual for the underlying devices. There is a significant threat level from jamming based attacks in IoT because of the feature of remote, unmonitored deployment of smart devices. It is a physical layer attack in which RFs are interrupted for interference and saturated noise signals. A DoS attack can result from RF signal jamming of underlying channels. Proper monitoring of the cognitive spectrum may prevent it [122].
- ***Node Injection Attack*:** This attack is a variation of the MitM attack. It is one of the most powerful attacks on the physical layer of IoT. The attacker injects or deploys additional node in between two or more IoT nodes in the network topology. The injected node takes part in communication and takes control of the traffic in the network [19].
- ***Tampering*:** This attack violates confidentiality and accessibility. In this type of attack, the information of the end device is modified, added, or deleted by an attacker. The attacker physically captures and compromises an end node from the network. Thus, all information can be collected by the attacker. In addition, reprogramming, redeployment, and recovery of data from the field can be done by such an attack. An attacker recovers the format and type of transmitted information, then tampers and regenerates the same type of data [123]. Therefore, the precision of data generated by the network becomes remarkably doubtful.
- ***Physical Damage*:** An attacker physically damages IoT nodes by removing or deactivating them. Hence, the service becomes unavailable [19]. As a result, the necessity of mitigation methods for such an attack is significant for IoT. Today, smart cities are packed with IoT elements such as sensors, cameras and smart lights that can easily be damaged or stolen by adversaries. The adversary tries to attack onto the interface of IoT nodes for shutting down or physically damaging them. A multitude of these attacks will cause the network to fail [123].
- ***Exhaustion Attack:*** Jamming or previously mentioned DoS attacks may result in exhaustion attacks. Particularly, the battery-operated devices may suffer from energy exhaustion if an attacker continuously attacks the network [38]. Repeated attempts of retransmission may cause collisions in IoT MAC protocols, which leads to high-energy exhaustion. Exhaustion is considered as a high impact DoS attack and is linked to deactivation attacks in order to reduce the network size and permanently remove the nodes from the network.

4) MULTI-LAYER/DIMENSIONAL ATTACKS

The following attacks may take place in different layers based on their architectures and policies. These attacks are discussed below.

- ***Cryptanalysis Attack*:** The cryptanalyst or attacker, in this kind of attack, tries to access an encrypted message without owning the encryption key [123]. A Brute-force attack is one of the cryptanalysis attacks in which the attacker systematically tries and guesses every possible passphrase or password combination. The cryptanalyst eventually finds the correct one to gain access to the system. The Known-plaintext attack, Ciphertext-only attack and Chosen-plaintext attack are some of the other examples of cryptanalysis attacks [123].
- ***Side-Channel Information Attacks*:** During the process of the encryption operation, the attacker obtains information and performs a reverse-engineering process to gather the cryptographic credentials of an IoT device [124], [125]. This information can be gained from the encryption devices, not from plaintext or ciphertext during the encryption process. Side-channel attacks the use of some or all of the data to gain the key that the device is using. Timing attacks, power or fault analysis and electromagnetic attacks are some of the instances of such attacks. The adversary makes use of information leakages and recovers block cipher keys. The attacks can be succeeded by directly defeating the intrusion prevention system such as Boolean masking.

TABLE III
ANALYTICAL COMPARISONS OF DIFFERENT ATTACKS

Architecture	Attack names	Objective	Method of attack	Impact
Application layer	Virus & Malware [126]–[128]	To hack and attack confidentiality of application, steal user credential and system shutdown	In the form of Trojans, Spams, Worms	Cause damage or harm to IoT high-end device, applications and Bluetooth technologies
	Spyware [129]	To spy or monitor users' activities and gain users' credential	In the form of the application installed in the user device	Indirect harm to users or device
	Flooding [38], [100]	To exhaust node resources	By broadcasting a multitude of messages	Reduces device lifetime
	Spoofing [130]	To hamper authentication and user privacy	By impersonating a node	May cause losing trust and confidentiality
	Message forging [131]	To send wrong information to the user	By modifying or creating a message	Mislead user by different message other than the original may cause great harm
	Code injection [132]–[134]	To steal user ID and password	By injecting malicious code into an application	Hack into users vital account
	Intersection [135], [136]	To hamper system privacy	By gaining the system's secondary information	May lead to other attacks
Network layer	Hello flood [139], [140]	To mislead routing path	By broadcasting many invalid routing paths	Hello message from intruder may mislead the routing and drop an important message
	Sinkhole [141]–[143]	To launch several other attacks	By making the central node of the network unavailable	Network failure
	Replay [144], [145]	To exhaust network/system/database resources	By retransmitting packets	Network failure or system unavailable
	Sybil [116], [146]–[149]	To eliminate original and valid node from the network	By creating its own numerous identities	Lead to dropping packets
	Clone ID [150]	To gain and access user traffic	By cloning identity of a legitimate node	Missing of user data
	SF [151]–[154]	To deprive bandwidth and delay network transmission	By dropping certain incoming packets	Compromising of availability and confidentiality
	Blackhole [155]	To affect network operation	By dropping all incoming packets	The entire network may fail
	Eavesdropping & Traffic analysis [120]	To gain information to launch other types of attacks	Gain information by sending control message and make an analysis of the gained messages	Affect user privacy and confidentiality
Physical layer	RF jamming [148]–[154]	To make the sharing bandwidth ineffective	By interrupting radio frequency and by making interference	May cause interference and noise in the signal. May lead to DoS attack
	Tag cloning [156]	To make the victim confuse about genuine tags	By replicating data from direct access to RFID device or by reverse engineering	To hamper the authenticity of an object, cause financial loss, jeopardize personal safely
	Node injection [38]	To take part in communication among the legitimate node and may	By deploying additional node in a network topology	Take control of the network traffic
	Tampering [160]	To modify, add or delete data from end device	By physical capture and compromise of an end node	To hamper confidentiality and accessibility
	Physical damage [38]	To deactivate the network or to make service unavailable to the user	By removing node physically or deactivating a node by sending kill command	Shutting down a network node makes service unavailable to the user
	Exhaustion [161]	To exhaust network resources	By launching other attacks such as retransmission, flooding, repay attack.	Reduces node and network lifetime.
Multi-layer attacks	Side Channel Information Attacks	To recover key information	By time, power, fault analysis of a system	Lead to other attacks
	DoS [137], [138]	To make service unavailable	One way is to attack by exhausting network	Service unavailability may cause serious damage to large organization
	Cryptanalysis [162], [163]	To find encryption key	In the form of trial and error by guessing every possible key	Break encryption system and gain access to ciphertext

- ***Man-In-The-Middle (MitM) attacks*:** The adversary sits between two IoT devices to monitor, control, get access to private information and interfere in communication between the two IoT nodes [164]. The MitM attacks are the kind of attacks, which can be devastating to all the IoT layers. In this case, the cryptanalyst tries to sit between two nodes to gain access to the ciphertext and break the encryption system to find the encryption key. The cryptanalyst then obtains access to the plaintext and possibly alter the message of those two parties without their consent.
- ***DoS/DDoS*:** Denial-of-Service/Distributed (DoS) attack may shut down any IoT device, network or application and make service inaccessible to its users. These attacks may occur in many forms. One way to attack is by generating huge network traffic and broadcasting a tremendous request to the victim. The main purpose of this attack is to make devices, software, network services, and resources unavailable to the target consumers [56], [101]. Additionally, the adversary may leak users' sensitive information. DDoS attack is more dangerous than that of the DoS attack, which combines a number of attacking platforms to invade one or more systems. The impact of DoS attacks in IoT gateway has been assessed in [137]. The study developed a prototype using wired and wireless interfaces to analyze the DoS attacks.

V. COUNTERMEASURES FOR SECURITY ATTACKS IN IoT

Each IoT layer is comprised of a set of security protocols, techniques, algorithms, and security kits employed to make it harder for an adversary to attack or hack into the system. A better understanding of these notions will enable the researchers to analyze the security breaches and the level of defense that is needed. In addition, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and other complete security solutions can be applied to protect IoT from security threats. This section brings together the existing countermeasures including learning-based, encryption-based, autonomic, and other methods to secure IoT systems from application, network and physical layers. We present learning-based, encryption-based and autonomic approaches and discuss their relevance for constrained IoT.

A. LEARNING-BASED COUNTERMEASURES

Learning-based approaches have been extensively used in almost all areas, including intrusion detection because of their distinctive nature of resolving real-time problems. Machine Learning (ML)/Deep Learning (DL) methods mainly learn from existing data and predict the future behavior of a system. It can improve system performance by classifying normal or abnormal behavior of a system. The performance of such learning-based models could be evaluated in terms of classification accuracy. There are four categories of a learning algorithm in practice, such as supervised, semi-supervised, unsupervised, and reinforcement learning. In this section, we gather and analyze some of the learning-based algorithms that are proposed to secure the IoT system. There are few studies done on ML and DL for IoT security. Interested readers can refer to the literature [165] for working principles and applicability of various ML/DL method in IoT security. In this segment, we are focusing on listing down and analyzing some advanced countermeasure approaches for IoT security based on learning algorithms.

Various learning-based countermeasures are available for detecting intrusions in IoT, such as Decision Tree (DT), Recurrent Neural Network (RNN), Random Forest (RF), Deep Eigenspace Learning (DEL), Deep Belief Network (DBN), Auto-Encoder (AE), Generative Adversarial Network (GAN), Support Vector Machine (SVM), Principle Component Analysis (PCA), Convolutional Neural Networks (CNN), and Artificial Neural Networks (ANN). Table IV presents some state-of-the-art learning-based security countermeasures for IoT in different layers. The table summarizes the objectives, advantages, performance accuracy, dataset used, and limitations of each learning-based security measures. The following subsections bring together and explain some state-of-the-art proposed methods based on ML/DL as countermeasures to various security attacks and intrusion in the IoT system for application, network and physical layers.

- **Countermeasures to Application Layer Attacks:** A linear SVM algorithm is proposed in [128] to detect malware in Android. They analyzed the detection accuracy of SVM with other machine-learning algorithms in terms of malware detection and showed that the proposed approach outperforms other algorithms. A novel distributed deep learning method was proposed to detect attacks in fog-to-things computing [166]. The results prove that deep-learning models are better than shallow models in terms of detection accuracy, false alarm rate, and scalability. The authors in [167] proposed a method with a combination of the Elman Neural Network and the SVM algorithm. They introduced Back Propagation Through Time (BPTT) algorithm to transform the processing of the network at various times into a forward network.

  The authors in [168] presented a three-layer architecture to detect impersonation attacks using the AWID dataset. First, the feature extraction is done using stacked sparse AE, and feature selection is done using SVM, DT, and ANN algorithms. Finally, normal or abnormal traffic is classified using the ANN algorithm. The experimental results showed that the support vector machine had better accuracy; however, it took the longest training time.

TABLE IV
STATE-OF-THE-ART LEARNING-BASED APPROACHES

Ref	Year	Learning method	Learning type	Dataset	Objective	Data Preprocess	Working principle	Advantage	Performance accuracy	Limitation
[169]	2019	DBN-based DNN	Supervised	Simulated using Cooja	Detect Sinkhole, DDoS, Blackhole, Wormhole attacks	Yes	Employs DL model using supervised training	Can detect real-world intrusions effectively	Precision rate of 95% and recall rate of 97%	Require high processing power and large dataset
[176]	2016	Q-learning and Dyna-Q	RL	--	Detect Physical layer spoofing	--	Formulates interactions between a receiver and Spoofer as a zero-sum Spoofing detection game	Robust against environmental Changes	Average detection error rate is less than 5%	Detection may be limited for high-speed mobility devices
[171]	2019	Scale-hybrid-IDS-alertnet based on MLP-DNN	--	NSL-KDD, KYOTO, UNSW-NB15, CICIDS-2017	Comparative study of ML methods	--	Analyzes network and host-level activities. It employed distributed model with DNNs.	Able to perform better in both HIDS and NIDS.	Varies with various datasets, proposed DNN architecture and ML methods	Accuracy can be improved
[172]	2018	DL	Supervised	IRAD	Detects Version Number, Blackhole and Hello Flood	Yes	Deep layers are trained with regularization and dropout mechanisms	Very high training accuracy	Training accuracy up to 99.5% and F1-Scores up to 99%	High training time, computation cost
[170]	2016	Optimum-Path Forest ML based of graph theory	Unsupervised	--	Detects SF, sinkhole and wormhole suspicious nodes	--	Utilizes an agent which is based on map reduce architecture work in a distributed platform	Light IDS agent that will eliminate the local analysis	Detection accuracy up to 96.02%	Detection accuracy can be be improved
[237]	2019	LR, SVM, DT, RF and ANN	Supervise & unsupervised	DS20S	Dos, Probing, Malicious Control, Scan, Spying	Yes	Several ML algorithms are compared to predict attacks	Comparative study is given	Accuracy up to 99.4%	No new algorithm is devised
[238]	2019	Naive Bayes, K-Nearest Neighbor	Supervised & unsupervised	NSL-KDD	Detects U2R And R2L attacks	Yes	Backbone networks uses two-layer dimension reduction and two-tier classification detection techniques	Relatively lower Resource requirements	Detection accuracy up to 84.86%	Can detect only low frequency attacks
[239]	2018	NDAE and RF	Unsupervised	KDD Cup '99 and NSL-KDD	Detects DoS, Probe, U2R and R2L attacks	Yes	Utilizes stacked NDAEs and the RF classification algorithm. The model is implemented in TensorFlow	Reduced Training time	F-score of 87.37%, recall of 85.42% And precision of 100.00%	High computational cost
[167]	2020	Elman neural network and SVM	--	DARPA	Ensures safety of information systems	No	Elman neural network puts safety protection on the gateway. SVM detects and analyses log information	Focused to improve training time	Detection rate is100% and false alarm rate is 2.8%.	Difficult to select the number of hidden layers
[168]	2017	Stacked sparse AE, SVM, DT, and ANN	Supervised and unsupervised	AWID	Detect Impersonation attacks	Yes	Feature extraction and selection done by stacked sparse AE, SVM, DT, and ANN. Intrusion s are classified using ANN	SVM shows better accuracy	Detection accuracy 99.918% and false alarm rate 0.012%	Long training time

- **Countermeasure to Network Layer Attacks:** A Deep Belief Network (DBN) approach based on a Deep Neural Network (DNN) has been proposed in [169] to detect network attacks. They created a dataset using the Cooja simulator, which is trained to detect sinkhole attack, DDoS, Blackhole, and Wormhole attack. Their deep-learning model utilized supervised training and binary classification for identifying abnormal activities. The proposed intrusion-detection system can detect real-world intrusions effectively. They achieved an average precision rate of 95% and a recall rate of 97% for different attack scenarios. Optimum-Path Forest (OPF) based on the ML method using graph theory has been proposed to detect SF, sinkhole, and wormhole suspicious nodes [170]. The specification-based and anomaly-based agents were utilized in the router and root nodes, respectively, to analyze the behavior of the host node and incoming data packets. They achieved a detection accuracy of 96.02%. In [171], a Scale-Hybrid-IDS-AlertNet based on the MLP-DNN model was compared with various existing datasets. The hybrid alert technique applied a highly scalable DL architecture to analyze the network and host-level activities. The proposed framework provides better accuracy than traditional machine learning classifiers.

  A simple DL algorithm was deployed to train the IRAD dataset, which was created using Cooja to detect version number, Blackhole, and Hello Flood attacks in [172]. After pre-processing, the datasets were labelled and mixed with attack and benign data. These datasets were then fed to a deep learning algorithm. The model achieved very high training accuracy of up to 99.5% and F1-scores up to 99%. The authors in [168] presented a three-layer architecture to detect impersonation attacks using the AWID dataset. First, the feature extraction is done using stacked sparse AE, and then feature selection is made using SVM, DT, and ANN, and finally, the normal or abnormal traffic is classified using the ANN algorithm. The experiment results showed that the SVM had better accuracy; however, it took the longest training time.

  Authors in [173] utilized the restricted Boltzmann machine (RBM) algorithm to detect DoS, User to Root (U2R) and probing attacks. They used an RBM method for feature learning and then forwarded the weighted result to next RBM layer to form a deep belief network (DBN). Finally, the multi-class intrusion detection was performed with a softmax activation function. The authors benchmarked their detection results with [174] and the hybrid method [175], utilizing the same dataset. Their experiments provided a high accuracy of 97.9% compared with [175] and [174], which had an accuracy rate of 93.94% and 92.1%, respectively.
- **Countermeasures to Physical Layer Attacks:** Q-learning and Dyna-Q-based on RL are applied to detect physical-layer spoofing in [176]. This method is based on interactions between a receiver and Spoofers as a zero-sum spoofing detection game. Simulation results show that the spoofing detection is robust against environmental changes. The authors of [177], [178] initiate a jamming attack using a deep neural network and proposed mitigation methods for this type of attack. This protection system does not adopt the information of the jammer and permits the transmitter to regulate its protection level on the fly based on its attained throughput.

  Dynamic watermarking [179], [180] is an algorithm that is capable of detecting and preventing cyber-physical attacks such as data injection and eavesdropping. The method is based on Long Short-Term Memory (LSTM) framework that allows IoT devices to extract a set of stochastic properties from their produced signals and dynamically watermarks these features into the signal. This algorithm enables the IoT gateway to authenticate the reliability of the signals effectively. However, authentication requires high computational resources. A scheme based on channel-based machine learning was proposed in [181] to detect both Clone and Sybil attacks. Simulations and experiments have been carried out in real environments. Both results confirm that the accuracy rate of authentication of the method achieves 84% without requiring manual labeling. The authors in [125] proposed a learning-based algorithm to detect side-channel attacks and showed 82% and 90% detection accuracy on high-end and low-end IoT devices, respectively.

B. AUTONOMIC APPROACHES

Security approaches should be dynamic and with minimal human intervention. Although different security attacks/issues may require different security solutions, however, some researchers proposed self-secure/autonomic approaches. The term 'autonomic' refers to 'self-sufficient' or 'self-healing', and 'self-protection' mechanism, which manages the resources of the security system without user intervention [38]. Self-healing solution uses specific countermeasures after an attack has been detected, and self-protection is used to prevent the attacks before they happen. Self-protection refers to a system which is capable of identifying and protecting itself from random attacks. The combination of a self-healing and self-protecting mechanism is called a hybrid approach. This section presents and analyzes the possible solution approaches that are classified based on different IoT architectures. Different intrusion mitigation and detection approaches follow autonomous methods for securing for IoT.

An autonomic manager module is used in self-sufficient mechanisms, which manages resource elements using a structural arrangement called MAPE (monitoring, analysis, planning, and execution) control loop. Autonomic approaches are the most popular techniques for mitigating IoT attacks. The basic working principle is as follows. Sensors collect information from the environment. This symbolizes the monitoring segment of the

MAPE architecture. This information is being matched with recognized patterns and acute values for certain parameters at the analyzing module. The planning module is responsible for further planning system goals and objectives on the basis of system constraints. Finally, the executing module implements the plan. In the autonomic approach, authentication and device identities are properly checked for self-protection. Table V shows the up-to-date autonomic countermeasure approaches and summarizes the objectives, advantages and limitations of each approach. The following subsections explain some state-of-the-art autonomic approaches as countermeasures to various security attacks and intrusion in the IoT system for application, network and physical layers.

- **Countermeasures to Application Layer Attacks:** In the MAPE architecture, viruses or malware patterns can be classified through analyzing them, and then they can be mitigated by executing the mitigation service(s) [126]. A constant vulnerability scan is one of the mitigation solutions, which applies risk mitigation services and malware pattern classification. The authors in [127] studied industrial mobile-IoT malware detection techniques and analyzed them in terms of static, dynamic, and hybrid approaches. A hybrid approach is proposed in [129] for detecting Spyware using and comparing various antivirus software. This technique is based on three parameters: description mapping, interface analysis and source code analysis. The parameters determine the malicious behavior of an application.

TABLE V
AUTONOMIC AND OTHER COUNTERMEASURES

Ref.	Title	Objective	Description	Advantage(s)	Limitation(s)
[129]	Spyware Detection in Android…	Detects Spyware	Uses three parameters namely, description mapping, interface analysis and source code analysis	Determines the malicious behavior	Code obfuscation may affect the detection accuracy
[132]	GMSA : Gathering Multiple…	Defends against Code Injection attack	Used a tool called gathering multiple signatures approach (GMSA)	Showed 99.45% of the accuracy	High computational cost
[136]	A model for protecting…	Resists Intersection attack	A systematic design called Buddies in practical anonymity systems	Can choose appropriate mitigation policy for each pseudonym	If any buddy is offline, the user is unable to transmit data
[139]	Rate limiting client puzzle…	Mitigates Hello Flood attack.	A puzzle scheme used for authentication which can be included in the autonomic solution	Autonomic solution	Exhaust resource due to recursion of solving the puzzle
[141]	A specification-based IDS…	Mitigates Sinkhole attack.	A semi-auto profiling RPL specification-based IDS	Successfully mitigate attack when IDS agent is functional	May not work if IDS agent is shutdown
[148]	Lightweight sybil attack…	Detects Sybil attacks	A lightweight detection scheme resides in the lower layer and supports variation of transmit powers	Lightweight	A powerful attacker may bypass the received signal strength indicator values
[151]	Defending Selective Forwarding…	Detects SF attack	Consists of detection and localization phases. A packet counter is used to monitor control messages from the wireless link.	Prevents SF attacks	May end up with few or no routes if eliminates the poor performing nodes from routing path
[156]	Deterministic Detection of…	Detects Tag Cloning attack	Deterministic detection used three protocols namely BASE, declone, and declone+.	Can detect Tag Cloning attack for large anonymous RFID systems	Demands both genuine and clone tags to be presented in a specific location at the same time
[182]	Wireless Jamming Localization…	Detects Jamming attack	Wireless devices' hearing range in inside the Jammer area		Not able to handle combined Jamming attacks
[160]	IoT-based Efficient…	Tamper detection	A tamper detection (TD) mechanism for IoT real data for healthcare applications	Great deal with security violations	May not be efficient for other IoT application

An autonomic solution is necessary to mitigate Spoofing attacks. A detection algorithm called Enhanced Location Spoofing detection using Audibility (ELSA) was developed for IoT [130]. The implementation of the proposed algorithm can be at the existing IoT backend server. The algorithm uses statistical decision theory. The authors in [132] proposed a tool called Gathering Multiple Signatures Approach (GMSA) to defend against code injection attacks and showed an accuracy of 99.45% for the

proposed algorithm. Readers also can refer to the framework proposed in [133] and [134] to detect this attack. A model called differential-linear cryptanalysis has been presented in [162] to evaluate a combined Cryptanalysis attack. The evaluation was done on a complex cryptographic security system.

The authors in [163] investigated the patterns of various Brute Force attacks to help IoT researchers and administrators to further analyze the attack type. They utilized a time-sensitive statistical relationship approach to identify the pattern and its configuration. The various forms of forging attacks and their design and implementation were presented in [131]. They proposed an infrastructure supported detection approach for detecting Forging attacks in vehicular networks. Intersection attacks can be mitigated by using a self-protecting approach. K-anonymity technique proposed by [135] to mitigate the intersection attacks. The authors in [136] proposed a systematic design for resisting an intersection attack called Buddies in practical anonymity systems. In this design, users are able to choose appropriate mitigation policies for each pseudonym.

- **Countermeasures to Network Layer Attacks**: The existing security protocol is not suitable for IoT. The integration of autonomic approaches may protect the network efficiently. Existing studies [138] proposed Naïve Bayes classification-based IDS by using multi-agents to detect misbehaving traffic of the network nodes to detect DoS attacks. Flooding attacks application can be mitigated using an automatic self-protection mechanism by establishing connection barriers [38]. One way to mitigate Hello Flood attack is by means of a parameter, namely the link-layer metric, while selecting a default route [62]. The authors in [183] proposed a solution to recover exhausted bandwidth automatically to save resources and defend against Flooding attacks. However, due to continuous broadcasts of route requests by an intruder, the interference may not be prevented by this solution. The authors in [184] presented a fundamental solution for counter-measures which is an acknowledgement-based system. However, acknowledgement-based solutions require huge energy resources which IoT devices are not capable of supplying. A puzzle scheme in [139] was proposed to mitigate this attack. This scheme and the use of the authentication mechanism can be included in the autonomic solution to mitigate Hello Flood attacks.

  An IDS scheme known as a compression header analyzer intrusion detection system (CHA-IDS) is proposed in [140], which analyzes compression header information. This scheme is capable of eradicating both individual and combined routing attacks in 6LoWPAN. Several countermeasures exist to mitigate Replay attacks such as TDMA-based approach. However, TDMA-based countermeasures are vulnerable due to several attempts of retransmission where the authorized node's time slot is consumed, and the packet gets lost. Other countermeasures are presented in [144], where, two separate methods are explained for both single and multi-hop routing. Data encryption is also an effective method against Replay attacks. The authors in [145] proposed a group authentication called TCGA approach, which changes the session key dynamically to confront the Replay attack.

  Many self-healing approaches have been proposed for sinkhole attacks. A semi-auto profiling RPL specification-based IDS proposed in [141] to protect from sinkhole attack. However, this system may fail to detect Sinkhole attacks due to the centralization approach. This detection mechanism becomes non-functional if the IDS agent shuts down because of such attacks or low power. The authors in [142] proposed an IDS-based routing protocol using Link Quality Indication (LQI) and managed to detect the Sinkhole attacks for the network layer. However, once the detection occurs, such an autonomic system urges to take reactive action. Another IDS-based detection of Sinkhole attacks on 6LoWPAN for IoT called INTI has been presented in [143]. This scheme analyzes the behavior of IoT devices by associating reputation, watchdog and trust policies for detecting the adversary. A model [185] is proposed to mitigate MitM attacks for software-defined IoT networks. The authors made use of traffic separation mechanism using deep packet inspection. They implemented the proposed model in Raspberry Pi. Combined with an intrusion detection technique, a hybrid routing protocol is designed and proposed in order to prevent MitM attacks [186]. The authors utilized a trusted third party to best deal with the performance difference of the protocol across various networks

  Sybil attacks are better mitigated using hybrid approaches. A Local Sybil Resistance (LSR) scheme has been presented in [146]. It studied the accessibility of a Roadside Unit (RSU) to detect and stand against Sybil attacks in vehicular networks. The authors in [147] aim to detect Sybil attacks for vehicular networks through workload and passive overhearing by preserving privacy and minimal network delay and overhead. A lightweight detection scheme mentioned in [148], which resides in the lower layer and supports various transmit powers and mobility. However, this scheme might not work well on all circumstances as the measures depend on the Received Signal Strength Indicator (RSSI) values; however, a powerful attacker may bypass the scheme. A comprehensive study of the behavior of a Sybil attack has been offered in [149], which may help to formulate an effective countermeasure to defend IoT from such attacks. Authors defined the defense mechanisms as Behavior Classification-Based Sybil Detection (BCSD), Mobile Sybil Detection (MSD), and Social Graph-Based Sybil

Detection (SGSD) [116] to defend against such attack in IoT.

Another network layer attack is called the Clone ID attack that can be prevented by using the instances' tracking number of each node. A lightweight and efficient mobile agent-based detection algorithm against the Clone ID attack is presented in [150]. A scheme presented in [151] consists of detection and localization phases to detect Selective Forwarding attack. In this scheme, a packet counter is used to monitor a sequence of control messages from the wireless link. A method called SVELTE was proposed for mitigating SF attacks in 6LoWPAN-based IoT. The authors designed and implemented their IDS in the Contiki operating system and evaluated using Cooja simulator [187]. Game theory-based detection model presented in [152], [153] to model and detect SF attacks for wireless mesh networks (WMNs) efficiently. The authors in [154] proposed a solution, which allows breaking the data packets into a number of smaller pieces. Those smaller packets transmitted through specific routes detect the presence of an attacker. Some autonomic solutions such as message-based detection, redundancy and probing can be used to protect IoT from SF attacks.

In [155], the Blackhole attack was studied and tested on the 6LoWPAN network. The simulation was done in ContikiRPL, using the Cooja simulator [188]. IDS and autonomic solutions for detecting, preventing, and confronting such attacks still require further research. An efficient sensor scheduling technique for protecting wireless transmission against eavesdropping attacks for the smart industry has been reported in [120]. In this scheme, a node with the capacity of the highest secrecy is scheduled in order to transmit data to its sink node.

- **Countermeasures to Physical Layer Attacks:** The mitigation approaches of Jamming attack usually fall under the self-healing paradigm. The suitable mitigation method is executed by the system when a possible Jamming attack is assumed. Inside the jammer area, the hearing range of the wireless devices is analyzed using the technique proposed in [182]. In [189], [190], cancellation and the usage of different parts of the spectrum are introduced for neutralizing the jammer signals, whereas some attempt to estimate the position of the jammer for further action. Some of them have utilized autonomic computing [157]–[159] to detect jammer's location. Node Injection is another vital attack in the physical layer. Monitoring and verification of device identity may prevent

Node Injection attacks. A unified security solution that integrates both self-protecting and self-healing methods are required to detect and mitigate this attack appropriately. The authors in [156] proposed a deterministic detection and presented three protocols, namely BASE, DeClone, and DeClone+ in order to detect Tag Cloning attacks for large anonymous RFID systems. Tampering attacks can be mitigated by implementing the MAPE framework. For instance, nodes generate data packets which are monitored by the MAPE system periodically to see whether the node has been compromised or not. Suspicious data generation can be mitigated based on this data control method. For example, the system may remotely control the node for deleting data in it (i.e., security patch). A Tamper Detection (TD) mechanism has been proposed for IoT healthcare applications to deal with security violations [160].

Physical damage of IoT nodes is considered a high-risk attack and cannot effectively be protected using software methods. The software method may disable the remote kill command, but physical damage of the device cannot be stopped [38]. The only way to protect the smart devices is to ensure physical security by surrounding them with a protective case. The IoT devices should be monitored physically as these attacks are more physical. Exhaustion in end nodes can be prevented and mitigated through the use of timers, rate limitation and cross-layer designing cognitive adaptation [161]. The autonomic system decides on duty cycling and cognitive adaption, which protects the availability and prolongs network lifetime [38].

C. ENCRYPTION-BASED COUNTERMEASURES

In this section, we discuss various existing symmetric and asymmetric cryptographic countermeasures for securing IoT. Cryptography is the representation of standard mathematical methods to defend against cybersecurity attacks against confidentiality, entity authentication, integrity and authentication [191]. The network of things is composed of several constrained nodes that communicate with each other using IPv6-6BR. The key properties of lightweight cryptography primitives [41], [42], [200], [201], [192]–[199] are listed in Table VI which summarizes different encryption algorithms and their characteristics including algorithm structures, key size, security strength and their implementation environment. Based on the literature, the security strength of cryptographic primitives can be measured as follows: low = below 55%; good = 55% to 69%; very good = 70% to 85%; excellent = 86% and above [41], [42], [200], [201], [192]–[199]. For instance, if an algorithm is capabe of providing 90% protection of a system then the security strength is considered excellent. The table also shows that the algorithms with larger key size provide very good or excellent security strength. Table VII summarizes some up-to-date encryption-based countermeasures for IoT. The table analyzes and presents the techniques used in the schemes, their objectives, advantages, limitations, and applied area.

The following sections do not exactly follow the structure of reviews seen in sub-sections of learning-based and autonomic countermeasures for three layers of architecture as discussed before. The reason for discontinuing the same structure here is that we think those may not be fully applicable in the context of encryption-based security measures. The following variations of

encryption-based countermeasures are applicable to different attacks of IoT architecture.

- **Countermeasures using Symmetric Key Cryptography:** This is also called secret-key encryption, where the sender and receiver share a single key for both encryption and decryption. Some of them are Advanced Encryption Standard (AES), Data Encryption Standard (DES), 3DES, International Data Encryption Algorithm (IDEA), Tiny Encryption Algorithm (TEA), Twofish, RC6 and Blowfish [40], [193], [196]. Various symmetric encryption distributions are available like Probabilistic Key Distribution where a shared symmetric key or bytes are selected randomly from a secured key pool and flashed at a constrained IoT device. In Deterministic Key Distribution, a key pool is created, and the keys are distributed homogeneously in such a way that a common key is utilized for every two nodes to guarantee secure connectivity.

  For Offline Key Distribution, either each node shares one key in the same network, or two nodes share network key pairwise depending on the utilized protocol. This scheme is also known as an offline key distribution. Another type of symmetric encryption is known as Server-Based Key Distribution [39]. In such schemes, two or more nodes and one or more trusted and powerful servers engage in message exchanges. The server acts as a Key Distribution Center (KDC). Many sessions can be created during communication process and each session can be secured through forward secrecy technique. Forward secrecy is an encryption technique for safeguarding communications conducted over the Internet. This method prevents an adversary to access past data from a set of transmission sessions. In forward secrecy, the key use in one session has no relation to the key use for another session.

  A lightweight encryption algorithm has been proposed in [202], which uses a chaos map-based key applied in The Field-Programmable Gate Array (FPGA). The scheme uses 1550 logic gates and 128 bit of key size and achieves 200 kbps of maximum throughput. In [203], a scheme which depends on the deployment knowledge is provided. This scheme gets rid of excessive key assignments. A mitigation technique [124] was proposed for side-channel attacks called leaky noise. The authors carried out a leakage assessment and characterized noise using statistical methods. They provided key recovery using Advanced Encryption Standard (AES). However, the method is not robust in terms of mitigating the attacks.

  Authors in [204] proposed a solution in which they mapped the keys on two-dimensional states. The authors added a probability density function to it in order to offer better key connectivity. A lightweight image encryption algorithm using probabilistic cipher has been proposed in [205]. The scheme encrypts the visual contents using image encryption prior to transmission. The algorithm is capable of producing a number of ciphered images with limited processing and memory requirements and ensures a high level of security.

  There are several existing approaches based on the offline key distributed mechanism available, that may be applicable in the context of IoT. Few of such schemes namely, SPIN, BROSK and SNAKE [206] generate session key without the necessity of key server. A master secret key is shared among all nodes in the same network in these schemes. In the SNAKE scheme, two random nonces are hashed to obtain the secret key. The communicating nodes generate random nonce using a pre-shared key. In BROSK approach, the session key is constructed from a broadcasted nonce in the network.

  A standard IPsec is implemented into IP-based WSN using 6LoWPAN in [207]. In this work, the authors proposed a header compression mechanism to support both the Authentication Header (AH) and Encapsulation Security Payload (ESP) header. However, one drawback of offline key distribution schemes is, they do not support the re-keying services. The Protocol for Carrying for Network Access (PANA) has been proposed as a key distribution solution for IoT based on an external assisted server [208]. Pre-shared key distribution is one of the authentication methods supported by Extensible Authentication Protocol (EAP) and PANA, and it uses EAP and runs over UDP. An improved version of PANA is proposed by Kanda *et al.* [209], which can be adopted by resource-constrained IoT. In this work, the authors have removed unnecessary PANA header fields and minimized the number of cryptographic primitives. However, it may reduce the code size for implementation, but it failed to provide a gain estimation, which might be achieved in terms of response time or consumption of the energy.

  The authors in [210] proposed a Secure Authentication and Key Establishment Scheme (SAKES) for IP-based M2M communication between an external internet host and a sensor node. In this scheme, the PBS authenticates the nodes using unconstrained 6LBR when it receives the node request. Diffie-Hellman (DH) [211] key agreement is then applied with the distant server, and the session key (SK) is calculated for the IoT device. Finally, using the SK, which the sensor node received from PBS, it can communicate securely with the server placed remotely.

TABLE VI
PROPERTIES OF LIGHTWEIGHT CRYPTOGRAPHY PRIMITIVES DIFFERENT LAYERS

Cryptography primitives	Algorithm	Key size/range (bits)	Block size/range (bits)	Code length (bits)	Algorithm structure	Security against attacks	Security strength	Layers: Software/ Hardware
Symmetric scheme	AES [40]–[42], [194], [196], [197]	128/192/256	128	2606	Substitution–permutation network	MitM, Chosen Plaintext, Known Plaintext, Brute-Force, Side-Channel attacks	Very good	SW and HW
	DES [40], [195]	64	64	-	Balanced Feistel network	Brute-Force attack	Good	HW
	3DES [42], [194]	56/112/168	64	-	Feistel network	MitM, Brute-Force, Chosen Plaintext, Known Plaintext	-	HW
	Blowfish [41], [192]	32–448	64	-	Feistel network	Brute-Force, Dictionary attack	-	SW
	HEIGHT [196]	128	64	5672	-	-	Good	HW
	PRESENT [41]	80/128	64	936	Substitution–permutation network	Brute-Force, MitM, Linear, Differential, Side-Channel attacks	Excellent	-
	TEA [41], [198]	128	64	1140	Feistel network	Brute-Force, MitM, Linear, Differential, Differential-linear, Side-Channel attacks	Excellent	-
	RC5 [195]	0–2040	32/64/128	Variable	Feistel-like network	Brute-Force, MitM, Linear, Differential, Differential-linear, Side-Channel attacks	Excellent	SW and HW
	Simon [41]	64/72/96/128/144/192/256	32/48/64/96/128	-	Balanced feistel network	Brute-Force, MitM, Linear, Differential, Differential-linear, Distinguishing (known key), Side-Channel attacks	Good	HW
	Speck [199], [200]	64/72/96/128/144/192/256	32/48/64/96/128	-	Add–rotate–xor (ARX)	Side-Channel attacks	Good	SW
Asymmetric scheme	RSA [40], [194]	1024 – 4096	1712–3760	900	Public key	Timing attacks, Adaptive Chosen Ciphertext, Side-Channel analysis attacks	-	SW and HW
	ECC [40], [41]	160	Variable	8838	Public key algorithm	Side-Channel Analysis, Backdoors, Quantum Computing attacks	Excellent	SW and HW
	DSA [41], [195]	-	-	-	Public key algorithm	Authentication, Integrity, Non-Repudiation, Chosen Plaintext attack	Good	SW
	MD5 [201], [212]	128	512	-	Public key algorithm	Collision, Preimage, Birthday, Brute-force, Rainbow, Side-Channel, Length Extension attacks	Low	SW
	DH [40], [193], [194]	Variable	-	-	Public key algorithm	Eavesdropping and MitM attacks	-	SW and HW

- **Countermeasures using Asymmetric Key Cryptography:** Asymmetric Key Cryptography (AKC) is a well-known approach to form an efficient and secure communication among nodes and is also known as Public-Key Cryptography (PKC) [213]. In the AKC, the sender encrypts a message using the recipient's public key. The receiver decrypts the message by using his private key. Various asymmetric algorithms have been developed and implemented so far, such as Rivest–Shamir–Adleman (RSA), DH, Elliptic-Curve Cryptography (ECC), and Pretty Good Privacy (PGP). AKC is also used to create Message Digest-5 (MD5), and Digital Signature Algorithms (DSA) [40]. The major drawbacks of AKCs application for IoT are higher energy consumption and computation, and operating cost. Regardless of those drawbacks, researchers still pursue to apply AKCs in the IoT environment [39]. It is because AKCs is a very powerful tool to secure communication over the internet.

  In AKC, if a public key or private key is used to encrypt a message, the same algorithm and the matching private key or public key can only be able to decrypt that message [214]. There are many variations of AKC algorithms. Key Transport Based Scheme is similar to the conventional key transport scheme that emphasizes on the secure transmission of information using the public key. In order to establish a safe and secure communication between two nodes in IoT, a Certificate-Based Encryption algorithm is the best choice. Each node in IoT maintains a certificate signed by a well-known and trusted third party (i.e., a CA). In fact, the CA guarantees the trustable relationship between the nodes [39].

Identity-Based Encryption (IBE) allows an arbitrary string to be the public key such as a receiver's email address. In IBE, a Public Key Generator (PKG) generates the private key from its public key of each node. Attribute-Based Encryption (ABE) [215] has changed the traditional concept of public-key cryptography relatively recently. It is the extension of the IBE scheme. Key Agreement Based Scheme is another technique based on asymmetric primitives and key agreement protocols by sharing the secret key among two or more parties in IoT.

NtruEncrypt [216] and Rabin's approach [217] are examples of Raw Public Key (RPK) encryption methods that have been proposed for WSNs. Rabin's approach is similar to the conventional RSA algorithm. This scheme consumes the same energy for decrypting messages like that of the RSA algorithm with the same level of security. As one squaring is needed for encrypting a message, this encryption scheme is much faster. A lattice-based cryptosystem, namely NtruEncrypt, is a substitute option to ECC and RSA algorithms. The scheme is most suitable and efficient for highly resource-limited things such as RFID tags and smartcards. With the inspiration from [218], the authors in [219] proposed the IBAKA approach using pairing-based cryptography, which is mainly a combination of the IBE-ECDH scheme. However, in order to establish a session key, the IBE scheme is tailored into an Elliptic Curve Diffie-Hellman exchange (ECDH) [220] key exchange.

Lightweight encryption for smart home, namely LES [221] proposed for home applications and the scheme consists of two sub-algorithms, called "KEYEncrypt" for session key encryption and "DATAEncrypt" for encrypting data. The scheme achieves confidentiality, adaptability and reduces overhead costs. The feasibility of implementing Attribute-Based Encryption (ABE) in IoT is still under investigation. A CP-ABE based lightweight ABE security approach is proposed in [215]. A lightweight with a no-pairing method using the ECC scheme for IoT has been presented in [222]. This is an efficient scheme for broadcasting encryption and access control based on the ciphertext.

A lightweight scheme has been proposed in [223], which aids distributed access control of Protected Health Information (PHI) among different healthcare applications by providing an efficient keyword search. Major heavy calculations are done by a semi-trusted computation center in the data encryption phase. The security of this scheme is based on Elliptic Curve Decisional Diffie–Hellman (ECDDH) technique. An efficient HIP-based lightweight encryption has been proposed to ensure end-to-end security for IoT [224]. It is a 6LoWPAN header compression of HIP packets. This scheme significantly reduces communication overhead, energy, and memory consumption.

- **Countermeasures using Hybrid Key Cryptography:** Symmetric and asymmetric ciphers combined to form a cryptographic technique called Hybrid Key Cryptography (HKC). Hybrid schemes utilize the benefits of the strengths of both approaches [225]. A great number of researches have shown that the combination of symmetric and asymmetric cryptography utilizes the strengths of both schemes and makes it suitable for IoT networks [42], [226]–[228]. However, more research works are still needed to improve hybrid security schemes to be a more lightweight and stronger solution at the same time. Existing hybrid schemes are advantageous for large hierarchical networks, which can utilize the benefits of both public and secret key schemes.

  There are numerous versions of hybrid cryptography available for resource-limited devices and networks. An Efficient and Hybrid Key Management (EHKM) [228] is a hybrid scheme which is mainly designed for heterogeneous WSNs. The lightweight public key encryption method, ECC is placed at cluster heads and BSs, while adjacent nodes in the same cluster use a one-way hash function based symmetric encryption method. A hybrid lightweight encryption algorithm for IoT called LEA-IoT has been proposed in [229]. This hybrid algorithm utilizes asymmetric encryption based on a linear block cipher and symmetric encryption based on a conventional private key and achieves data security. Key generation time and data encryption-decryption time were calculated as the lowest. This scheme achieved a low-latency communication.

  Secure IoT (SIT) utilizes symmetric key encryption of 64-bit block cipher with 64-bits key size and having five rounds. It is a lightweight hybrid solution based on Feistel and Substitution-Permutation (SP) networks [230]. Some researchers proposed Compressive Sensing (CS) technique to provide signal compression to make the scheme lightweight and encryption simultaneously. For instance, a Lightweight Secure Scheme (LSS) is proposed in [231] to secure IoT network from Chosen-Plaintext Attack (CPA) and to prolong the network lifetime. LSS consists of three stages; key generation stage where BS and IoT nodes generate random numbers, key exchange stage where BS and nodes exchange the number in a secure way, and compression/encryption stage to generate secret compressed samples in order to mitigate CPA.

TABLE VII
STATE-OF-THE-ART LIGHTWEIGHT ENCRYPTION SCHEMES

Ref	Year	Title	Base technique(s)	Objective(s)	Description	Advantage(s)	Limitation(s)	Application Domain (s)
[231]	2019	Lightweight Security….	RSA, ECC, CS	To secure the network from CPA attack	This method utilizes CS to avoid complex computation. Compress data traffic to reduce data dimension	Good at signal compression and lowering computational cost	Weakly encrypted	Communication between BS and IoT nodes
[229]	2018	LEAIoT:A Lightweight….	NtruEncrypt, Rabin scheme, RSA, AES	To provide low-latency communication and achieve data security	It utilizes a linear block cipher and symmetric encryption based on a private key	Key generation time, data encryption–decryption time and latency are low	Did not consider energy and memory utilization	Applications of IoT
[205]	2018	Secure Surveillance…	Nonlinear chaotic map, Probabilistic cipher	To reduce the bandwidth consumption and transmission cost	Image encryption algorithm uses one chaotic map in PRNG and a cryptosystem structure	Low processing time and high level of security	Applies only for video traffic	Industrial IoT
[230]	2017	SIT:A Lightweight….	AES, PRESENT, DES	To provide security and resource utilization	Lightweight hybrid solution based on feistel and SP networks using symmetric key encryption	Energy and memory efficient	It uses only an XORed key	Secure IoT
[223]	2017	Lightweight Distributed….	Decisional Bilinear DH (DBD), HER	To reduce computation and communication overhead, and to provide security.	It provides distributed access control on cross-domain PHI among many healthcare domains	Better data encryption	Access right verification and session key management are not available in the scheme	Smart healthcare
[221]	2016	Lightweight Encryption for…	PKI, IBE, DH	To reduce computation time	LES utilizes “KEYEncrypt” for session key encryption and “DATAEncrypt” for encrypting data	Reduced overhead cost	The focus is mainly on confidentiality	Smart home
[202]	2016	Establishment of Light Weight…	Blowfish XTEA	To maximize resource utilization and provide security	Lightweight encryption algorithm was designed using a chaos map-based key for FPGA	Achieved of 200 kbps of throughput	Occupancy of memory size is key issue	WSNs of IoT
[222]	2015	A Lightweight Attribute-Based…	ECC, DH, ECDDH, ABE	To address the security and privacy issues in IoT and to reduce overhead	Elliptic curve cryptography uses a no-pairing ABE technique and ECDDH scheme	Efficient for broadcasting encryption	Not scalable and flexible for IoT applications	Single authority applications
[224]	2015	Efficient HIP-based Approach to….	DTLS, HIP-DEX, HIP-BEX, CD-HIP, DH	To achieve lightweight E2E security and to reduce energy consumption	6LoWPAN header is compressed for HIP packets	Reduced communication overhead, energy and memory consumption	Incompatible	WSNs of IoT

VI. DISCUSSION

In this paper, we have addressed the key security issues, presented existing advanced countermeasures and emphasized the areas that require further research. Figure 6 presents a taxonomy and summarized the methods of attack, respective actual attacks and their existing countermeasures. The following subsections provide an analytical discussion, suggest the appropriate security schemes for IoT, and proposes future research directions for the researchers.

A. DISCUSSION ON EXISTING SECURITY APPROACHES

Several learning-based, autonomous, symmetric, asymmetric security schemes or mechanisms are mentioned above. However, not all of them are suitable for IoT. This section analyzes and discusses the advantages and trade-offs among existing countermeasures.

- **Learning-Based Countermeasures:** The efficiency of learning-based approaches depends on attack detection accuracy, true and false-positive rates, F1-score and some other performance matrix. The training time of the model also plays an important role in the selection of the model. There are trade-offs among ML/DL-based algorithms. Deep learning algorithms can be trained on devices with relatively high processing and memory capabilities because they require large datasets and the structure of neural networks are complex. Machine learning algorithms, on the other hand, can be trained on devices with somewhat lower processor and memory properties. In terms of performance, the DL approaches provide higher accuracy and reliability compared to ML algorithms. Some learning algorithms are less computationally costly; some are complex in terms of their structures. Decision Tree algorithm, for example, can be constructed with only a few or several trees for either simple or complex classification. Naive Bayes classifiers are incapable of finding relationships among features to be learned from. Consequently, they classify the intrusions inaccurately. RNN algorithms suffer from vanishing gradients.

  Some learning-based algorithms (e.g., CNN and SVM) are capable of breaking cryptographic implementations. Further research is required to investigate these algorithms in terms of their purposes and performances. The structure of DL algorithms is more complex than that of ML algorithms and requires larger dataset to be trained on. The training time and computational complexity of DL methods depend on how complex the structure is. There are various tools and inbuilt libraries available such as Keras, Tensorflow, and so on to automate the training process. Ensemble-based and stack-based DL algorithms are computationally costly. The deployment of these methods may create bottlenecks during real-time implementation. Therefore, designing and developing a learning-based algorithm must be taken into consideration in adapting it to the real implementation.

  Learning-based methods depend on the existing data or information from where the models learn and classify the incoming traffic as normal or abnormal. These datasets can be either smaller or larger. However, finding real-world IoT-dedicated dataset to train learning-based algorithms is challenging. Machine learning algorithms require a smaller size of datasets to train the model compared to deep learning algorithms. Finding publicly available intrusion detection datasets is another challenge, as there are very limited datasets available on public platforms. Moreover, ML and DL algorithms may produce a higher false-positive rate if the dataset used in training is not realistic. High quality real-world and comprehensive IoT training datasets are required to train these methods. Generating high-quality training dataset remains a challenge for contemporary scholars in the field of IoT-related academic investigations.

- **Autonomic Approaches:** The autonomic approaches have the advantages of an automatic architecture where different modules accomplish different tasks to detect and mitigate attacks. It is encouraged to design security solutions where human physical intervention requirement is low instead of relying on a complete autonomic solution. Integration between software and network virtualization would help to achieve the CIA triad with self-healing and self-protecting capacity in the IoT environment. Some autonomic systems demand complex cognitive structures to provide a self-repair mechanism. However, due to the resource limitation, it is encouraged to design a lightweight and energy-efficient autonomic system for the IoT. IoT devices transfer data to other devices or to a central location; therefore, autonomic security solutions should be compatible with dynamic communication protocols and heterogeneous environments.

  Designing autonomic security without taking into consideration the complexity level will serve as a roadblock in terms of evaluating and implementing them in the IoT system. Existing self-securing standards may require a constant power supply to keep them operational. An intelligent power monitor and control system is required to keep the autonomic system up and running without having energy exhaustion. Developing a fully automated security solution remains a shared vision among researchers. Contemporary researchers are still working towards designing a complete, portable, and robust self-securing system. Currently, a fully autonomic solution does not exist, and such an anticipated solution remains under continuous research consideration. There is a need for more research in this vital field in order to develop a holistic, dynamic and robust autonomic security solution for current and future IoT architecture.

- **Encryption Algorithms:** Whenever asymmetric cryptography is used, the light-duty nodes will experience performance inefficiency. On the other hand, the heavy-duty nodes will lose the opportunity for better security implementation using symmetric cryptography. In order to resolve this dilemma, a security system should be able to adapt automatically to the cryptographic capabilities

[232]. Generating suitable small keys is challenging using public-key cryptography. The existing cryptosystems are designed to provide security for a specific security goal. However, achieving all the security goals simultaneously using conventional encryption-based countermeasure is not possible. Research work has been initiated to provide quantum cryptography. However, quantum cryptography is still at its infancy stage. Designing and developing such cryptosystems should take into consideration the compatibility issue that might arise with the diverse IoT technology and protocols.

The main criteria for evaluating IoT key management schemes include computational, communicational, energy and storage complexity; connectivity; scalability and security resilience. These measures are usually used to validate the effectiveness of security schemes. Communication capacity refers to the number and size of packets transmitted and received by IoT nodes. Connectivity refers to the probability of connection for a pair of nodes that have the same pre-distributed key or set up a key path among them. The applied key scheme must be scalable so that the network supports adding or removing IoT nodes anytime. Resilience refers to the probability of an attacker compromising a link or whole network depending on the number of nodes captured by an attacker. These are important factors to evaluate the performance of the cryptographic schemes [235]. Due to less computational complexity, the symmetric-key techniques are commonly used as they are appropriate for the resource-limited characteristics of the IoT networks. However, the shortages of efficient symmetric key cryptography for IoT are also obvious. There is still some weakness in the existing approaches such as security resilience, connection probability and scalability.

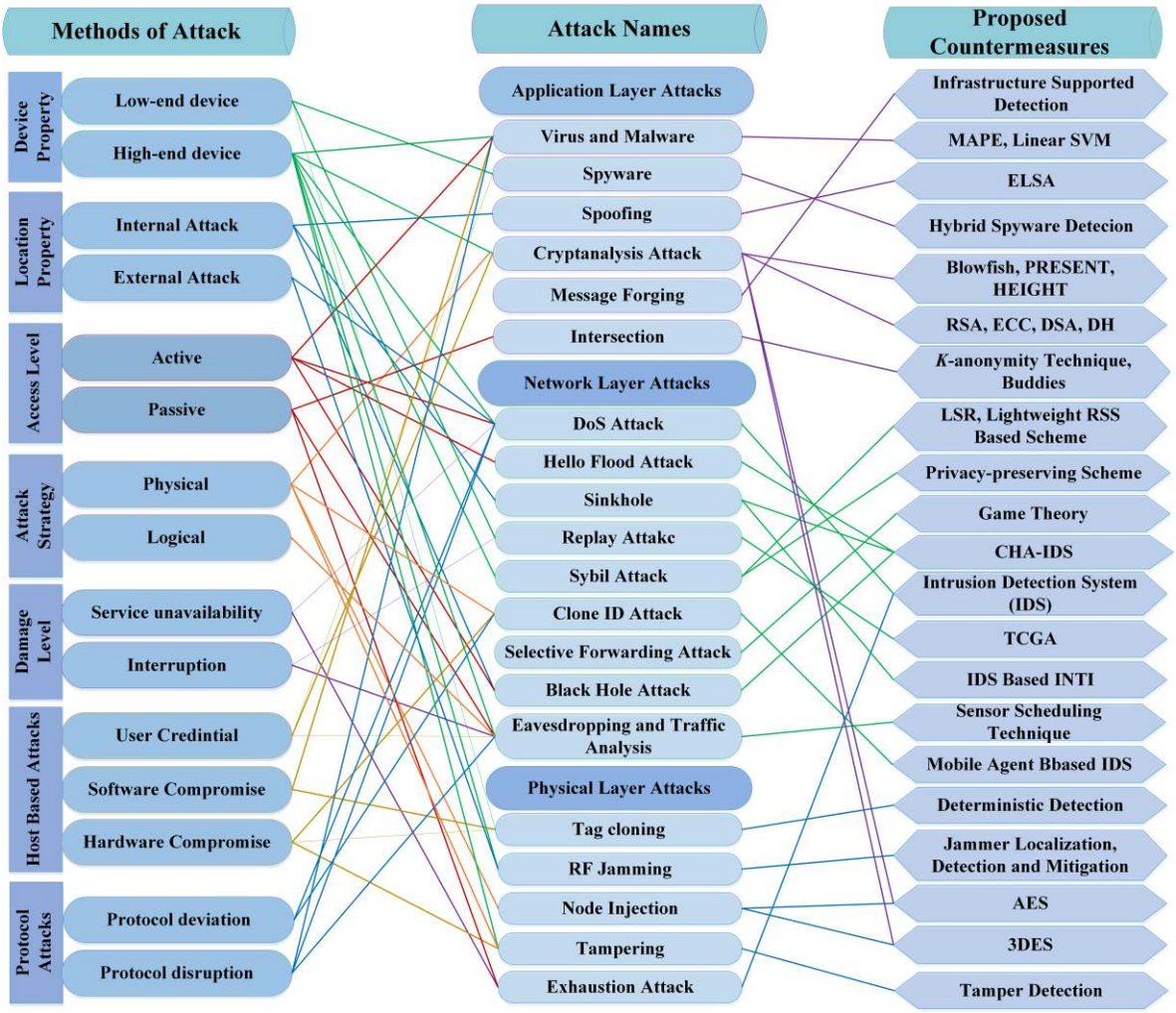

FIGURE 6. A relation diagram to present the methods of attack, actual attacks and their existing countermeasures. Infrastructure Supported Detection [131], **MAPE** [126], **Linear SVM** [128], **IoT Malware Detection** [127], **ELSA** [130], **Hybrid Spyware Detection** [129], **BLOWFISH, PRESENT, HEIGHT, AES, 3DES, RSA, ECC, DSA, DH** [233], **[40], K-Anonymity Technique** [135], **BUDDIES** [136], **LSR** [146], **Lightweight RSS-Based Scheme** [148], **Privacy-Preserving Scheme** [147], **Game Theory** [152], [153], [234], **CHA-IDS** [140], **TCGA** [145], **INTI** [143], **Sensor Scheduling Technique** [120], **Mobile Agent-Based IDS** [150], **Determeministic Detection** [156], **Jammer Localization, Detection and Mitigation** [157]–[159], [182], [189], [190] **and Tamper Detection** [160].

Public key schemes, on the other hand, have more security strength (resilience), storage capacity, communication overhead, and scalability. Asymmetric approaches are more complex with mathematical calculations but provide much stronger security solutions. However, some researches proved that improved versions of public-key encryption schemes are suitable for low resource nodes [213], [236]. Furthermore, there is ongoing research to improve energy supply via ultra-low power circuitry in order to support continuous energy supply to IoT nodes. This can potentially address the problem of resource limitation and complex computational issues in public-key cryptography. Moreover, with the improvements of lightweight public key schemes, it will no longer be impractical to utilize them in constrained environments [213]. More research work on the analysis of the strength of different schemes in the context of the IoT needs to be carried out. The research direction is, therefore, to secure IoT by combining encryption techniques to make it stronger, a lightweight and optimal solution for the heterogeneous IoT environment.

B. DISCUSSION ON IMPLEMENTATION CHALLENGES

As mentioned in earlier sections, IoT devices are often deployed in remote areas and might be unattended, which may result in physical layer attacks in particular. The sensor-equipped connected things are often battery operated, embedded with small memory chips, and limited computation and communication capabilities. Therefore, there exists a roadblock in implementing complex and robust security protocols. Designing lightweight solution with all security features are also a challenge. The communication may take place via popular wireless technologies, which are easier to compromise and vulnerable to interference and interception attacks. DoS attack may result in a single point of failure and severe service unavailability due to centralized communication. Finally, providing a complete self-securing and autonomic security architecture is necessary, but it is incredibly challenging to implement because of the IoT features like resource-limited characteristics.

C. OPEN ISSUES AND RESEARCH DIRECTIONS

Some works of literature indicate that the diversity and complexity in IoT might increase in the years to come. There are noteworthy approaches towards securing mission-critical applications on the go. Some of them may complicate the attack mitigation process and demand full automation in terms of securing the system independently or as a whole. A careful system-wide strategy for a unified security system is required for IoT. Our findings and future directions are outlined briefly in the following points.

- More researches need to be conducted to develop a lightweight and robust trust management system for both ultra-low power and powerful devices. In addition to this, physical security, risk management, trustworthiness and intrusion detection should be ensured at all layers of IoT.
- Although best practice security solution may require very low resources of IoT nodes since they are still prone to many devastating attacks.
- A well-defined standard for security is needed for catering to diverse applications, industries, and businesses in a pragmatic way. Distinct security policies and frameworks are mandatory for ensuring stable and reliable communication to take place.
- The security protocols should be improved in accordance with the application's need. Information about the deployment location or identity of a device may require hiding from anonymous users. K-anonymity approach may be suitable for performing that task for low- powered devices. Routing path is another crucial element to provide fast, secure communication, which is ensured by creating multiple paths to detect errors of the system and assist it to keep performing.
- Real-time data analysis in the IoT node using appropriate ML and DL-based approaches can be developed before the transmission of data.
- Learning-based algorithms are trained with datasets and may sometimes produce inaccurate output. The inaccuracy appears due to the lack of real-world dataset from the IoT environment or selection of inappropriate algorithm.
- A more lightweight cryptographic algorithm can be designed for IoT hardware and end-to-end communication. The encryption algorithms can be combined with autonomic approaches to provide a holistic security solution for security threats for IoT applications.
- Other than the security challenges we have mentioned in this study, there could be many more unique and lethal security threats in the years to come. Based on the frequency and severity of the attacks, a priority-based learning algorithm can be designed.
- Future researchers can carry out research in designing hybrid approaches such as combining learning and encryption-based algorithms. For example, based on the available resources, the system should learn and adapt which encryption method to be utilized for detecting certain intrusion.
- Right plans and strategies are essential while deploying IoT applications in public platforms.
- All data should be encrypted before storing and transferring to IoT devices.
- Quantum cryptography can be introduced for real-time encryption for resource-limited applications.

VII. CONCLUSION

In this paper, we have studied and presented an overview of IoT, its enabling technologies, and compared the factors related to implementing a comprehensive security approach in IoT with traditional internet. A focus has been given on security attacks

based on IoT architecture. Attack taxonomy and comparisons have been provided. It is important to consider IoT architecture, its limitations and diversity when providing comprehensive protection. Furthermore, we discussed the different factors related to the capacity and limitations of IoT in the design of security solutions. In this regard, we have considered the need for IoT security, including conventional Confidentiality, Integrity and Availability (CIA) triad.

Unlike other studies we aggregated and discussed various advanced security countermeasures including cryptographic, autonomic, and learning-based schemes which ensure secure communication for IoT in contrast to existing surveys which considered only certain types of countermeasures. This survey study will serve as a useful manual for researchers to access a wide range of security attacks and solutions that may be of benefit to them. Finally, a discussion on existing approaches, implementation challenges and future research directions was also provided. Many researchers have proposed lightweight schemes for IoT, yet more research work in this field is needed to design a holistic, unified, and well-suited security countermeasures for the IoT as a whole.

APPENDIX

The following table presents the common and popular acronyms used throughout this paper.

LIST OF ACRONYMS

Acronyms	Definition	Acronyms	Definition
IoT	Internet of Things	**DL**	Deep Learning
RFID	Radio-Frequency Identification	**PCA**	Principle Component Analysis
IT	Internet Technology	**RNN**	Recurrent Neural Network
DTLS	Datagram Transport Layer Security	**DEL**	Deep Eigenspace Learning
MQTT	Message Queuing Telemetry Transport	**DBN**	Deep Belief Network
ML	Machine Learning	**CNN**	Convolutional Neural Networks
DDS	Data Distribution Services	**DNN**	Deep Neural Networks
XMPP	Extensible Messaging and Presence Protocol	**AE**	Auto-Encoder
WiFi	Wireless Fidelity	**SVM**	Support Vector Machine
BLE	Bluetooth Low Energy	**ANN**	Artificial Neural Networks
UDP	User Datagram Protocol	**LSTM**	Long Short-Term Memory
AMQP	Advanced Message Queuing Protocol	**RF**	Random Forest
MIC	Message Integrity Check	**AES**	Advanced Encryption Standard
IDS	Intrusion Detection Systems	**DES**	Data Encryption Standard
IPS	Intrusion Prevention Systems	**IDEA**	International Data Encryption Algorithm
LLN	Low Power and Lossy Networks	**TEA**	Tiny Encryption Algorithm
DODAG	Destination Oriented Directed Acyclic Graph	**KDC**	Key Distribution Centre
6LoWPAN	IPv6 over Low Power Wireless Personal Area Network	**AKC**	Asymmetric Key Cryptography
CIA	Confidentiality, Integrity, and Availability	**PKC**	Public-Key Cryptography
SLA	Service Level Agreement	**RSA**	Rivest–Shamir–Adleman
CoAP	Constrained Application Protocol	**DH**	Diffie-Hellman
RPL	Low Power and Lossy Networks	**AH**	Authentication Header
WLAN	Wireless Local Area Network	**RPK**	Raw Public Key
SLA	Service Level Agreement	**ESP**	Encapsulation Security Payload
DNS	Domain Name System	**ECDH**	Elliptic Curve Diffie-Hellman exchange
MitM	Man-in-the-Middle	**HKC**	Hybrid Key Cryptography
CPA	Chosen-Plaintext Attack	**ABE**	Attribute-Based Encryption
DoS	Denial-of-Service	**ECC**	Elliptic-Curve Cryptography
SF	Selective Forwarding	**MD5**	Message Digest-5
LSR	Local Sybil Resistance	**DSA**	Digital Signature Algorithms
DT	Decision Tree	**PHI**	Protected Health Information
RF	Radio Frequency	**CS**	Compressive Sensing

ACKNOWLEDGMENT

This paper is supported by Impact-Oriented Interdisciplinary Research Grant Programme (IIRG) IIRG003A-19IISS and Fundamental Research Grant Scheme (FRGS) FP055-2019A.

REFERENCES

[1] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, Vision and Challenges for Realising the Internet of Things The meaning of things lies not in the things themselves, but in our attitude towards them. Antoine de Saint-Exupéry, no. March. 2010.

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

[3] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," J. Netw. Comput. Appl., vol. 42, pp. 120–134, 2014.

[4] G. Svensson, "Auditing the Human Factor as a Part of Setting up an Information Security Management System," pp. 1–29, 2013.

[5] E. D. Frangopoulos, M. M. Eloff, and L. M. Venter, "Psychosocial risks: Can their effects on the security of information systems really be ignored?," Inf. Manag. Comput. Secur., vol. 21, no. 1, pp. 53–65, 2013.

[6] M. Aazam, M. St-Hilaire, C. H. Lung, and I. Lambadaris, "PRE-Fog: IoT trace based probabilistic resource estimation

at Fog," 2016 13th IEEE Annu. Consum. Commun. Netw. Conf. CCNC 2016, pp. 12–17, 2016.
[7] F. Li, Y. Han, and C. Jin, "Practical access control for sensor networks in the context of the Internet of Things," Comput. Commun., vol. 89–90, pp. 154–164, 2016.
[8] S. Li, T. Tryfonas, and H. Li, "The Internet of Things: a security point of view," Internet Res., vol. 26, no. 2, pp. 337–359, 2016.
[9] PricewaterhouseCoopers (PwC), "Information Security Breaches Survey," HM Government: London, UK, 2015.
[10] R. Klahr, J. N. Shah, P. Sheriffs, T. Rossington, and G. Pestell, "Cyber Security Breaches Survey 2017: Main report," UK Gov., 2017.
[11] R. Vaidya, "Cyber Security Breaches Survey 2018: Statistical Release," Univ. Portsmouth, 2018.
[12] R. Vaidya, "Cyber Security Breaches Survey 2019 - GOV.UK," Cyber Secur. Breaches Surv. 2019 Stat. Release Contents, 2019.
[13] B. Sudqi Khater, A. Abdul Wahab, M. Idris, M. Abdulla Hussain, and A. Ahmed Ibrahim, "A Lightweight Perceptron-Based Intrusion Detection System for Fog Computing," Appl. Sci., vol. 9, no. 1, p. 178, 2019.
[14] R. Vaidya, "Cyber Security Breaches Survey 2019 - GOV.UK," Cyber Secur. Breaches Surv. 2019 Stat. Release Contents, 2019.
[15] M. Gulzar and G. Abbas, "Internet of Things Security : A Survey and Taxonomy," 2019 Int. Conf. Eng. Emerg. Technol., pp. 1–6.
[16] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," Inf. Syst. Front., vol. 17, no. 2, pp. 243–259, 2015.
[17] E. Vasilomanolakis, J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier, and P. Kikiras, "On the Security and Privacy of Internet of Things Architectures and Systems," Proc. - 2015 Int. Work. Secur. Internet Things, SIoT 2015, pp. 49–57, 2016.
[18] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," in 2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015, 2016, pp. 336–341.
[19] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017, 2017, pp. 32–37.
[20] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," J. Netw. Comput. Appl., vol. 88, no. April, pp. 10–28, 2017.
[21] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," Wirel. Networks, vol. 20, no. 8, pp. 2481–2501, 2014.
[22] Y. Lu and L. Da Xu, "Internet of things (IoT) cybersecurity research: A review of current research topics," IEEE Internet Things J., vol. 6, no. 2, pp. 2103–2115, 2019.
[23] K. Chen et al., "Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice," J. Hardw. Syst. Secur., vol. 2, no. 2, pp. 97–110, 2018.
[24] Y. Yang, L. Wu, G. Yin, L. Li, and Hongbin Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," IEEE Internet Things J., vol. 4, no. 5, pp. 1250–1258, 2017.
[25] T. Lu, P. Yao, L. Zhao, Y. Li, F. Xie, and Y. Xia, "Towards attacks and defenses of anonymous communication systems," Int. J. Secur. its Appl., vol. 9, no. 1, pp. 313–328, 2015.
[26] M. Agrawal and P. Mishra, "A comparative survey on symmetric key encryption techniques," Int. J. Comput. Sci. Eng., vol. 4, no. 5, p. 877, 2012.
[27] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," IEEE Access, vol. 7, pp. 82721–82743, 2019.
[28] V. Sharma, I. You, K. Andersson, F. Palmieri, M. H. Rehmani, and J. Lim, "Security, Privacy and Trust for Smart Mobile-Internet of Things (M-IoT): A Survey," IEEE Access, 2019.
[29] B. Liao, Y. Ali, S. Nazir, L. He, and H. U. Khan, "Security Analysis of IoT Devices by Using Mobile Computing: A Systematic Literature Review," IEEE Access, vol. 8, pp. 120331–120350, 2020.
[30] T. Nandy et al., "Review on Security of Internet of Things Authentication Mechanism," IEEE Access, vol. 7, pp. 151054–151089, 2019.
[31] L. Chen et al., "Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey," IEEE Access, vol. 5, pp. 8956–8977, 2017.
[32] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques," IEEE Commun. Surv. Tutorials, vol. 21, no. 3, pp. 2671–2701, 2019.
[33] A. Kim, J. Oh, J. Ryu, and K. Lee, "A review of insider threat detection approaches with IoT perspective," IEEE Access, vol. 8, pp. 78847–78867, 2020.
[34] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," IEEE Internet Things J., vol. 6, no. 5, pp. 8182–8201, 2019.
[35] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Comput. Networks, vol. 57, no. 10, pp. 2266–2279, 2013.
[36] R. Tahir, "A Study on Malware and Malware Detection Techniques," Int. J. Educ. Manag. Eng., vol. 8, no. 2, pp. 20–30, 2018.
[37] H. Lin and N. W. Bergmann, "IoT privacy and security challenges for smart home environments," Inf., vol. 7, no. 3, 2016.
[38] Q. M. Ashraf and M. H. Habaebi, "Autonomic schemes for threat mitigation in Internet of Things," J. Netw. Comput. Appl., vol. 49, pp. 112–127, 2015.
[39] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," Ad Hoc Networks, vol. 32, pp. 17–31, 2015.
[40] S. Chandra, S. Paira, S. S. Alam, and G. Sanyal, "A comparative survey of symmetric and asymmetric key cryptography," 2014 Int. Conf. Electron. Commun. Comput. Eng. ICECCE 2014, no. May 2015, pp. 83–93, 2014.
[41] I. K. Dutta, B. Ghosh, and M. Bayoumi, "Lightweight Cryptography for Internet of Insecure Things: A Survey," 2019 IEEE 9th Annu. Comput. Commun. Work. Conf., pp. 0475–0481, 2019.
[42] M. Faheem, S. Jamel, A. Hassan, Z. A., N. Shafinaz, and M. Mat, "A Survey on the Cryptographic Encryption Algorithms," Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 11, pp. 333–344, 2017.
[43] M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," pp. 1–42, 2018.
[44] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," pp. 1–23, 2019.
[45] A. Al-fuqaha, S. Member, M. Guizani, M. Mohammadi, and S. Member, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Commun. Surv. TUTORIALS, vol. 17, no. 4, pp. 2347–2376, 2015.
[46] S. Horrow and A. Sardana, "Identity management framework for cloud based internet of things," Proc. First Int. Conf. Secur. Internet Things - Secur. '12, pp. 200–203, 2012.
[47] A. Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of Cloud computing and Internet of Things: A survey," Futur. Gener. Comput. Syst., vol. 56, pp. 684–700, 2016.
[48] P. S. and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," J. Electr. Comput. Eng., vol. 07, no. 06, pp. 85–88, 2017.
[49] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet : The Internet of Things Architecture , Possible Applications and Key Challenges," 2012 10th Int. Conf. Front. Inf. Technol., pp. 257–260, 2012.

[50] Z. Yang et al., "Study and Application on the Architecture and Key Technologies for IOT," 2011 Int. Conf. Multimed. Technol., pp. 747–751, 2011.

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

[52] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," Comput. Networks, vol. 144, pp. 17–39, 2018.

[53] M. Wu, T. J. Lu, F. Y. Ling, J. Sun, and H. Y. Du, "Research on the architecture of Internet of Things," ICACTE 2010 - 2010 3rd Int. Conf. Adv. Comput. Theory Eng. Proc., vol. 5, pp. 484–487, 2010.

[54] I. Yaqoob, I. A. T. Hashem, Y. Mehmood, A. Gani, S. Mokhtar, and S. Guizani, "Enabling Communication Technologies for Smart Cities," IEEE Commun. Mag., vol. 55, no. 1, pp. 112–120, 2017.

[55] D. P. Alexander Gluhak, Srdjan Krco,Michele Nati, "A Survey on Facilities for Experimental Internet of Things Research," no. November, pp. 58–67, 2011.

[56] W. Zhang and B. Qu, "Security Architecture of the Internet of Things Oriented to Perceptual Layer," Int. J. Comput. Consum. Control, vol. 2, no. 2, pp. 37–45, 2013.

[57] P. Pongle and G. Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT," 2015 Int. Conf. Pervasive Comput. Adv. Commun. Technol. Appl. Soc. ICPC 2015, vol. 00, no. c, pp. 0–5, 2015.

[58] D. T. Tschofenig, H., J. Arkko, "Architectural Considerations in Smart Object Networking," vol. 119, no. 3, p. 859{\textendash}867, 2015.

[59] E. R. Naru, H. Saini, and M. Sharma, "A recent review on lightweight cryptography in IoT," in Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017, 2017, pp. 887–890.

[60] D. Airehrour, J. Gutierrez, and S. K. Ray, "A Lightweight Trust Design for IoT Routing," Proc. - 2016 IEEE 14th Int. Conf. Dependable, Auton. Secur. Comput. DASC 2016, 2016 IEEE 14th Int. Conf. Pervasive Intell. Comput. PICom 2016, 2016 IEEE 2nd Int. Conf. Big Data, pp. 552–557, 2016.

[61] M. R. Palattella et al., "Internet of Things in the 5G Era: Enablers, Architecture, and Business Models," IEEE J. Sel. Areas Commun., vol. 34, no. 3, pp. 510–527, 2016.

[62] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the RPL-based internet of things," Int. J. Distrib. Sens. Networks, vol. 2013, 2013.

[63] S. Elhadi, A. Marzak, N. Sael, and A. Mamouni, "Comparative study of IoT protocols," pp. 1–9, 2018.

[64] C. L.-S. Y.-H. L.-H. Lin, "Transmission apparatus and transmission method thereof," 2018.

[65] A. J. Jara, L. Ladid, A. Skarmeta, A. J. Jara, L. Ladid, and A. Skarmeta, "The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities The Internet of Everything through IPv6," J. Wirel. Mob. Networks, no. 3, pp. 97–118, 2013.

[66] D. Dragomir, L. Gheorghe, S. Costea, and A. Radovici, "A Survey on Secure Communication Protocols for IoT Systems," 2016.

[67] L. Catarinucci et al., "An IoT-Aware Architecture for Smart Healthcare Systems," IEEE Internet Things J., vol. 2, no. 6, pp. 515–526, 2015.

[68] Y. Choi, Y. Choi, D. Kim, and J. Park, "Scheme to guarantee IP continuity for NFC-based IoT networking," in International Conference on Advanced Communication Technology, ICACT, 2017, pp. 695–698.

[69] P. P. Ray, "A survey on Internet of Things architectures," J. King Saud Univ. - Comput. Inf. Sci., vol. 30, no. 3, pp. 291–319, 2018.

[70] J. G. Andrews, "Seven Ways that HetNets Are a Cellular Paradigm Shift," no. March, pp. 136–144, 2013.

[71] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review," in Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012, 2012, vol. 3, pp. 648–651.

[72] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," IEEE Commun. Surv. Tutorials, vol. 16, no. 4, pp. 1933–1954, 2014.

[73] S. S. I. Samuel, "A review of connectivity challenges in IoT-smart home," in 2016 3rd MEC International Conference on Big Data and Smart City, ICBDSC 2016, 2016, pp. 364–367.

[74] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and Privacy Challenges in Internet of Things," in 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC). IEEE, 2015.

[75] A. Kotsev, S. Schade, M. Craglia, M. Gerboles, L. Spinelle, and M. Signorini, "Next generation air quality platform: Openness and interoperability for the internet of things," Sensors (Switzerland), vol. 16, no. 3, pp. 1–16, 2016.

[76] J. Colding and S. Barthel, "An urban ecology critique on the 'Smart City' model," J. Clean. Prod., vol. 164, pp. 95–101, 2017.

[77] Z. PANG, "Technologies and Architectures of the Internet-of-Things (IoT) for Health and Well-being ZHIBO PANG Doctoral Thesis in Electronic and Computer Systems," 2013.

[78] S. B. Baker, W. Xiang, and I. Atkinson, "Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities," IEEE Access, vol. 5, pp. 26521–26544, 2017.

[79] A. Mathur, T. Newe, and M. Rao, "Defence against black hole and selective forwarding attacks for medical WSNs in the IoT," Sensors (Switzerland), vol. 16, no. 1, 2016.

[80] L. Alonso, V. Milanés, C. Torre-Ferrero, J. Godoy, J. P. Oria, and T. de Pedro, "Ultrasonic sensors in urban traffic driving-aid systems," Sensors, vol. 11, no. 1, pp. 661–673, 2011.

[81] G. Stefansson and K. Lumsden, "Performance issues of Smart Transportation Management systems," Int. J. Product. Perform. Manag., vol. 58, no. 1, pp. 55–70, 2009.

[82] K. Mahmood, S. Ashraf Chaudhry, H. Naqvi, T. Shon, and H. Farooq Ahmad, "A lightweight message authentication scheme for Smart Grid communications in power sector," Comput. Electr. Eng., vol. 52, pp. 114–124, 2016.

[83] E. Borgia, "The internet of things vision: Key features, applications and open issues," Comput. Commun., vol. 54, pp. 1–31, 2014.

[84] P. Kasinathan, G. Costamagna, H. Khaleel, C. Pastrone, and M. A. Spirito, "DEMO: An IDS framework for internet of things empowered by 6LoWPAN," in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security - CCS '13, 2013, pp. 1337–1340.

[85] S. Pinto, T. Gomes, J. Pereira, J. Cabral, and A. Tavares, "IIoTEED: An Enhanced, Trusted Execution Environment for Industrial IoT Edge Devices," IEEE Internet Computing, vol. 21, no. 1, pp. 40–47, 2017.

[86] L. S. Sayana and B. K. Joshi, "Security issues in internet of things," in UGC Sponsored National Conference on Global Challenges – Role of Sciences & Technology in Imparting their Solutions, 2016, no. April.

[87] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things," in Proceedings - 2015 IEEE World Congress on Services, SERVICES 2015, 2015, pp. 21–28.

[88] Y. H. Chuang, N. W. Lo, C. Y. Yang, and S. W. Tang, "A lightweight continuous authentication protocol for the Internet of Things," Sensors (Switzerland), vol. 18, no. 4, pp. 1–2, 2018.

[89] FTC Staff Report, "'Internet of Things - Privacy & Security in a Connected World,'" 2015.

[90] C. Lu and R. Jain, "Overview of Security and Privacy Issues in the Internet of Things," CSE WUSTL, pp. 1–11, 2014.

[91] S. Tata, R. Jain, H. Ludwig, and S. Gopisetty, "Living in the Cloud or on the Edge: Opportunities and Challenges of IOT Application Architecture," in Proceedings - 2017 IEEE 14th International Conference on Services Computing, SCC 2017, 2017, pp. 220–224.

[92] C. Pham, Y. Lim, and Y. Tan, "Management architecture for heterogeneous IoT devices in home network," in 2016 IEEE 5th Global Conference on Consumer Electronics, GCCE 2016, 2016.

[93] N.-N. Dao, T. V. Phan, U. S. Ad, J. Kim, T. Bauschert, and S. Cho, "Securing Heterogeneous IoT with Intelligent DDoS Attack Behavior Learning," arxiv.org, pp. 1–7, 2017.

[94] Egham, "Gartner says 8.4 billion connected 'things' will be in use in 2017, up 31 percent from 2016." .

[95] "Nokia Networks to power Internet of Things with 5G connectivity." [Online]. Available: https://www.theinternetofallthings.com/nokia-networks-to-power-internet-of-things-with-5g-connectivity-2015-02-19/.

[96] B. Brik, M. Esseghir, L. Merghem-Boulahia, and H. Snoussi, "ThingsGame: when sending data rate depends on the data usefulness in IoT networks," 2018 14th Int. Wirel. Commun. Mob. Comput. Conf., pp. 886–891, 2018.

[97] M. Katagi and S. Moriai, "Lightweight cryptography for the Internet of Things," 2008.

[98] V. Petrov, S. Edelev, M. Komar, and Y. Koucheryavy, "Towards the era of wireless keys: How the IoT can change authentication paradigm," 2014.

[99] M. Xiang, Q. Bai, and W. Liu, "Trust-based Adaptive Routing for Smart Grid Systems," J. Inf. Process., vol. 22, no. 2, pp. 210–218, 2014.

[100] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "ReTrust: Attack-resistant and lightweight trust management for medical sensor networks," IEEE Trans. Inf. Technol. Biomed., vol. 16, no. 4, pp. 623–632, 2012.

[101] M. U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," Int. J. ofComputer Appl., vol. 111, no. 7, 2015.

[102] A. H. Ahmed, N. M. Omar, and H. M. Ibrahim, "Modern IoT Architectures Review : A Security Perspective," 2017, pp. 73–81.

[103] P. Vijayakumar, M. S. Obaidat, M. Azees, S. H. Islam, and N. Kumar, "Efficient and Secure Anonymous Authentication with Location Privacy for IoT-Based WBANs," IEEE Trans. Ind. Informatics, vol. 16, no. 4, pp. 2603–2611, 2020.

[104] W. Ali, I. Ud Din, A. Almogren, M. Guizani, and M. Zuair, "A Lightweight Privacy-aware IoT-based Metering Scheme for Smart Industrial Ecosystems," IEEE Trans. Ind. Informatics, vol. 3203, no. c, pp. 1–1, 2020.

[105] K. Gu, W. Zhang, S. J. Lim, P. K. Sharma, Z. Al-Makhadmeh, and A. Tolba, "Reusable mesh signature scheme for protecting identity privacy of IoT devices," Sensors (Switzerland), vol. 20, no. 3, pp. 1–23, 2020.

[106] Y. Kortesniemi, D. Lagutin, T. Elo, and N. Fotiou, "Improving the Privacy of IoT with Decentralised Identifiers (DIDs)," J. Comput. Networks Commun., vol. 2019, 2019.

[107] L. Garms and A. Lehmann, "Group Signatures with Selective Linkability," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 11442 LNCS, pp. 190–220, 2019.

[108] O. Hahm, E. Baccelli, H. Petersen, and N. Tsiftes, "Operating Systems for Low-End Devices in the Internet of Things: A Survey," IEEE Internet Things J., vol. 3, no. 5, pp. 720–734, 2016.

[109] A. K. Bairagi, R. Khondoker, and R. Islam, "An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures," Inf. Secur. J., vol. 25, no. 4–6, pp. 197–212, 2016.

[110] N. K. Gyamfi and D. E. Owusu, "Survey of Mobile Malware Analysis, Detection Techniques and Tool," 2018, pp. 1101–1107.

[111] P. Schaffer, K. Farkas, Á. Horváth, T. Holczer, and L. Buttyán, "Secure and reliable clustering in wireless sensor networks: A critical survey," Comput. Networks, vol. 56, no. 11, pp. 2726–2741, 2012.

[112] E. Erdin, C. Zachor, and M. H. Gunes, "How to Find Hidden Users: A Survey of Attacks on Anonymity Networks," IEEE Commun. Surv. Tutorials, vol. 17, no. 4, pp. 2296–2316, 2015.

[113] S. R. Ganta, S. P. Kasiviswanathan, and A. Smith, "Composition Attacks and Auxiliary Information in Data Privacy," pp. 265–273, 2008.

[114] S. Aluvala, K. R. Sekhar, and D. Vodnala, "An Empirical Study of Routing Attacks in Mobile Ad-hoc Networks," Procedia Comput. Sci., vol. 92, pp. 554–561, 2016.

[115] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classification of RFID Attacks," Gen 1569314443, pp. 73–86, 2011.

[116] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the internet of things," IEEE Internet Things J., vol. 1, no. 5, pp. 372–383, 2014.

[117] P. Pongle and G. Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT," 2015 Int. Conf. Pervasive Comput. Adv. Commun. Technol. Appl. Soc. ICPC 2015, vol. 00, no. c, pp. 1–6, 2015.

[118] L. K. Bysani, "A Survey On Selective Forwarding Attack in Wireless Sensor Networks," in In Proceedings of the 2011 International Conference on Devices and Communications, ICDeCom.

[119] H. Dai, Q. Wang, D. Li, and R. C. Wong, "On Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas," Int. J. ofDistributed Sens. Networks Dir., 2013.

[120] Y. Zou, S. Member, and G. Wang, "Intercept Behavior Analysis of Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack," IEEE Trans. Ind. Informatics, vol. 12, no. 2, pp. 780–787, 2016.

[121] A. Rabbachin, A. Conti, and M. Z. Win, "Intentional Network Interference for Denial of Wireless Eavesdropping," in 2011 IEEE Global Telecommunications Conference - GLOBECOM 2011, 2011, pp. 1–6.

[122] W. Liu et al., Various Detection Techniques and Platforms for Monitoring Interference Condition in a Wireless Testbed. Measurement methodology and tools.Berlin Heidelberg: Springer, 2013.

[123] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in IEEE Symposium on Computers and Communication (ISCC)., 2015.

[124] D. R. E. Gnad, J. Krautter, and M. B. Tahoori, "Leaky Noise : New Side-Channel Attack Vectors in Mixed-Signal IoT Devices," vol. 2019, no. 3, pp. 305–339, 2019.

[125] A. Sayakkara and M. Scanlon, "Leveraging Electromagnetic Side-Channel Analysis for the Investigation of IoT Devices," Digit. Investig., vol. 29, pp. S94–S103, 2019.

[126] R. Canzanese, M. Kam, and S. Mancoridis, "Toward an automatic, online behavioral Malware classification system," Int. Conf. Self-Adaptive Self-Organizing Syst. SASO, pp. 111–120, 2013.

[127] S. Sharmeen and S. Huda, "Malware Threats and Detection for Industrial Mobile-IoT Networks," IEEE Access, vol. 6, pp. 15941–15957, 2018.

[128] H. Ham, H. Kim, M. Kim, and M. Choi, "Linear SVM-Based Android Malware Detection for Reliable IoT Services," J. Appl. Math., vol. 2014, 2014.

[129] P. Kaur and S. Sharma, "Spyware Detection in Android Using Hybridization of Description Analysis , Permission Mapping and Interface Analysis," in Procedia - Procedia Computer Science, 2015, vol. 46, no. Icict 2014, pp. 794–803.

[130] J. Y. Koh, I. Nevat, D. Leong, and W. Wong, "Geo-Spatial Location Spoofing Detection for Internet of Things," IEEE Internet Things J., vol. 3, no. 6, pp. 971–978, 2016.

[131] J. Grover, V. Laxmi, and M. Singh, "Attack models and infrastructure supported detection mechanisms for position forging attacks in vehicular ad hoc networks," CSI Trans. ICT, vol. 1, no. September, pp. 261–279, 2013.

[132] H. Alnabulsi, "GMSA : Gathering Multiple Signatures Approach to Defend Against Code Injection Attacks," IEEE Access, vol. 6, pp. 77829–77840, 2018.

[133] T. K. George, K. P. Jacob, and R. K. James, "A Proposed Framework Against Code Injection Vulnerabilities in Online Applications," J. Internet Technol., vol. 20, no. 1, pp. 4–5, 2019.

[134] T. K. George, K. P. Jacob, and R. K. James, "Token based Detection and Neural Network based Reconstruction framework against code injection vulnerabilities," J. Inf. Secur. Appl., vol. 41, pp. 75–91, 2018.

[135] L. Sweeney, "A model for protecting privacy," Int. J. Uncertain., vol. 10, no. 5, pp. 1–14, 2002.

[136] D. I. Wolinsky, E. Syta, and B. Ford, "Hang with your buddies to resist intersection attacks," in In the Proceedings

of the 20th ACM conference on Computer and Communications Security (CCS 2013), 2013, pp. 1153–1166.
[137] Y. Lee, W. Lee, G. Shin, and K. Kim, "Assessing the Impact of DoS Attacks on IoT Gateway," 2017.
[138] S. Hassan, A. Houbing, and K. M. Malik, "NBC-MAIDS : Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks," J. Supercomput., 2018.
[139] J. Y. Koh, J. T. C. Ming, and D. Niyato, "Rate limiting client puzzle schemes for denial-of-service mitigation," in IEEE Wireless Communications and Networking Conference, WCNC, 2013, pp. 1848–1853.
[140] M. N. Napiah, M. Yamani, I. Idris, R. Ramli, and I. Ahmedy, "Compression Header Analyzer Intrusion Detection System (CHA - IDS) for 6LoWPAN Communication Protocol," IEEE Access, vol. 3536, no. c, 2018.
[141] A. Le, J. Loo, K. K. Chai, and M. Aiash, "A specification-based IDS for detecting attacks on RPL-based network topology," Information, vol. 7, no. 2, 2016.
[142] B. G. C. B. G. Choi, E. J. C. E. J. Cho, J. H. K. J. H. Kim, C. S. H. C. S. Hong, and J. H. K. J. H. Kim, "A sinkhole attack detection mechanism for LQI based mesh routing in WSN," in 2009 International Conference on Information Networking, 2009, pp. 2–6.
[143] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things," in Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management, IM 2015, 2015, pp. 606–611.
[144] T. Roosta, M. Manzo, and S. Sastry, "Time Synchronization Attacks in Sensor Networks," Secur. Localization Time Synchronization Wirel. Sens. Ad Hoc Networks, pp. 325–345, 2007.
[145] P. N. Mahalle, N. R. Prasad, and R. Prasad, "Novel Threshold Cryptography-based Group Authentication (TCGA) Scheme for the Internet of Things (IoT)," in 2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace and Electronic Systems, VITAE 2014 - Co-located with Global Wireless Summit, 2014.
[146] X. Lin, "LSR: Mitigating zero-day sybil vulnerability in privacy-preserving vehicular peer-to-peer networks," IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 237–246, 2013.
[147] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "P2DAP - Sybil attacks detection in vehicular ad hoc networks," IEEE J. Sel. Areas Commun., vol. 29, no. 3, pp. 582–594, 2011.
[148] S. Abbas, M. Merabti, D. Llewellyn-Jones, and K. Kifayat, "Lightweight sybil attack detection in MANETs," IEEE Syst. J., vol. 7, no. 2, pp. 236–248, 2013.
[149] A. K. Mishra, A. K. Tripathy, D. Puthal, and L. T. Yang, "Analytical Model for Sybil Attack Phases in Internet of Things," IEEE Internet Things J., vol. 4662, no. c, pp. 1–9, 2018.
[150] R. Sathish and P. G. Scholar, "Dynamic Detection of Clone Attack in Wireless Sensor Ne etworks," in 2013 International Conference on Communication Systems and Network Technologies, 2013, pp. 501–505.
[151] D. Manikantan, S. Student, and T. A. M, "Defending Selective Forwarding Attacks in WMNs," in 2008 IEEE International Conference on Electro/Information Technology, 2008, pp. 96–101.
[152] S. Khanam, H. Y. Saleem, and A. K. Pathan, "An Efficient Detection Model of Selective Forwarding Attacks in Wireless Mesh Networks," in IDCS, 2012, pp. 1–14.
[153] A. K. Pathan, W. M. Abduallah, S. Khanam, and H. Y. Saleem, "A Pay-and-Stay model for tackling intruders in hybrid wireless mesh networks," Simulation, 2013.
[154] P. Pandarinath, "Secure Localization with Defense Against Selective Forwarding Attacks in Wireless Sensor Networks," in 2011 3rd International Conference on Electronics Computer Technology, vol. 5, pp. 112–117.
[155] K. Chugh, "Case Study of a Black Hole Attack on 6LoWPAN-RPL Case Study of a Black Hole Attack on 6LoWPAN-RPL," no. March, 2017.
[156] K. Bu, M. Xu, X. Liu, J. Luo, S. Zhang, and M. Weng, "Deterministic Detection of Cloning Attacks for Anonymous RFID Systems," IEEE Trans. Ind. Informatics, vol. 11, no. 6, pp. 1255–1266, 2015.
[157] Y. Cai, K. Pelechrinis, X. Wang, P. Krishnamurthy, and Y. Mo, "Joint reactive jammer detection and localization in an enterprise WiFi network," Comput. Networks, vol. 57, no. 18, pp. 3799–3811, 2013.
[158] Q. M. Ashraf, M. H. Habaebi, and M. R. Islam, "Jammer localization using wireless devices with mitigation by self-configuration," PLoS One, vol. 11, no. 9, pp. 1–22, 2016.
[159] A. A. Hussein, C. Y. Leow, and T. A. Rahman, Robust multiple frequency multiple power localization schemes in the presence of multiple jamming attacks, vol. 12, no. 5. 2017.
[160] A. Elngar, "IoT-based Efficient Tamper Detection Mechanism for Healthcare Application IoT-based Efficient Tamper Detection Mechanism for Healthcare Application," Int. J. Netw. Secur., vol. 20, no. May, pp. 1–7, 2018.
[161] D. Feng, C. Jiang, G. Lim, L. J. Cimini, G. Feng, and G. Y. Li, "A survey of energy-efficient wireless communications," IEEE Commun. Surv. Tutorials, vol. 15, no. 1, 2013.
[162] B. S. Rao and P. Premchand, "Evaluation of Differential – Linear Cryptanalysis Combined Attack on Cryptographic Security System," vol. 13, no. 23, pp. 16552–16563, 2018.
[163] D. Stiawan, M. Y. Idris, R. F. Malik, S. Nurmaini, N. Alsharif, and R. Budiarto, "Investigating Brute Force Attack Patterns in IoT Network," vol. 2019, 2019.
[164] J. O. Agyemang, J. J. Kponyo, and I. Acquah, "Lightweight Man-In-The-Middle (MITM) Detection and Defense Algorithm for WiFi-Enabled Internet of Things (IoT) Gateways," Inf. Secur. Comput. Fraud, vol. 7, no. January, 2019.
[165] A. Aldweesh, A. Derhab, and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," Knowledge-Based Syst., vol. 189, p. 105124, 2019.
[166] A. Abeshu and N. Chilamkurti, "Deep Learning: The Frontier for Distributed Attack Detection in Fog-To-Things Computing," IEEE Commun. Mag., vol. 56, no. 2, pp. 169–175, 2018.
[167] W. Fang, X. Tan, and D. Wilbur, "Application of intrusion detection technology in network safety based on machine learning," Saf. Sci., vol. 124, no. December 2019, p. 104604, 2020.
[168] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, "Deep abstraction and weighted feature selection for Wi-Fi impersonation detection," IEEE Trans. Inf. Forensics Secur., vol. 13, no. 3, pp. 621–636, 2017.
[169] G. Thamilarasu and S. Chawla, "Towards deep-learning-driven intrusion detection for the internet of things," Sensors (Switzerland), vol. 19, no. 9, 2019.
[170] H. Bostani and M. Sheikhan, "Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach," Comput. Commun., vol. 98, pp. 52–71, 2017.
[171] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, vol. 7, pp. 41525–41550, 2019.
[172] F. Y. Yavuz, D. Ünal, and E. Gül, "Deep learning for detection of routing attacks in the internet of things," Int. J. Comput. Intell. Syst., vol. 12, no. 1, pp. 39–58, 2018.
[173] K. Alrawashdeh and C. Purdy, "Toward an Online Anomaly Intrusion Detection System Based on Deep Learning," 2016 15th IEEE Int. Conf. Mach. Learn. Appl., pp. 195–200, 2017.
[174] N. Gao, L. Gao, Q. Gao, and H. Wang, "An Intrusion Detection Model Based on Deep Belief Networks," Proc. - 2014 2nd Int. Conf. Adv. Cloud Big Data, CBD 2014, pp. 247–252, 2015.
[175] Y. Li, R. Ma, and R. Jiao, "A hybrid malicious code detection method based on deep learning," Int. J. Secur. its Appl., vol. 9, no. 5, pp. 205–216, 2015.
[176] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-Layer Spoofing Detection with Reinforcement Learning in Wireless

Networks," IEEE Trans. Veh. Technol., vol. 65, no. 12, pp. 10037–10047, 2016.
[177] T. Erpek, Y. E. Sagduyu, and Y. Shi, "Deep learning for launching and mitigating wireless jamming attacks," IEEE Trans. Cogn. Commun. Netw., vol. 5, no. 1, pp. 2–14, 2019.
[178] Y. Shi, Y. E. Sagduyu, T. Erpek, K. Davaslioglu, Z. Lu, and J. H. Li, "Adversarial deep learning for cognitive radio security: Jamming attack and defense strategies," 2018 IEEE Int. Conf. Commun. Work. ICC Work. 2018 - Proc., pp. 1–6, 2018.
[179] A. Ferdowsi and W. Saad, "Deep Learning-Based Dynamic Watermarking for Secure Signal Authentication in the Internet of Things," IEEE Int. Conf. Commun., vol. 2018-May, pp. 1–6, 2018.
[180] A. Ferdowsi and W. Saad, "Deep Learning for Signal Authentication and Security in Massive Internet-of-Things Systems," IEEE Trans. Commun., vol. 67, no. 2, pp. 1371–1387, 2019.
[181] S. Chen, S. Member, Z. Pang, S. Member, H. Wen, and S. Member, "Automated Labeling and Learning for Physical Layer Authentication against Clone Node and Sybil Attacks in Industrial Wireless Edge Networks," vol. XX, no. Xx, 2020.
[182] Z. Liu, H. Liu, W. Xu, and Y. Chen2, Wireless Jamming Localization by Exploiting Nodes' Hearing Ranges, vol. 9, no. 3. Berlin Heidelberg: Springer, 2010.
[183] P. Yi, Y. Hou, Y. Zhong, S. Zhang, and Z. Dai, "Flooding attack and defence in Ad hoc networks," J. Syst. Eng. Electron., vol. 17, no. 2, pp. 410–416, 2006.
[184] V. P. Singh, S. Jain, and J. Singhai, "Hello Flood Attack and its Countermeasures in Wireless Sensor Networks," vol. 7, no. 3, 2010.
[185] A. Al Hayajneh, M. Z. A. Bhuiyan, and I. McAndrew, "Improving Internet of Things (IoT) Security with Software-Defined Networking (SDN)," computers, pp. 1–14, 2020.
[186] J. J. Kang, K. Fahd, S. Venkatraman, R. Trujillo-rasua, and P. Haskell-, "Hybrid Routing for Man-in-the-Middle (MITM) Attack Detection in IoT Networks," 29th Int. Telecommun. Networks Appl. Conf. Hybrid, 2019.
[187] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," Ad Hoc Networks, vol. 11, no. 8, pp. 2661–2674, 2013.
[188] C. Thomson, "Cooja Simulator Manual," no. C, pp. 2015–2016, 2016.
[189] M. H. Shoreh, H. Hosseinianfar, F. Akhoundi, E. Yazdian, M. Farhang, and J. A. Salehi, "Design and implementation of spectrally-encoded spread-time CDMA transceiver," IEEE Commun. Lett., vol. 18, no. 5, pp. 741–744, 2014.
[190] T. Kang, X. Li, C. Yu, and J. Kim, "A Survey of Security Mechanisms with Direct Sequence Spread Spectrum Signals," J. Comput. Sci. Eng., vol. 7, no. 3, pp. 187–197, 2013.
[191] S. V. A. Jeba, B. Paramasivan, and D.Usha, "Security Threats and its Countermeasures in Wireless Sensor Networks: An Overview," Int. J. Comput. Appl., vol. 29, no. 6, 2011.
[192] E. Surya and C.Diviya, "A Survey on Symmetric Key Encryption Algorithms," Int. J. Comput. Sci. Mob. Appl., vol. 2, no. 4, pp. 475–477, 2014.
[193] B. K. Patel and M. Pathak, "A Survey on Cryptography Algorithms," Int. J. Sci. Res., vol. 3, no. 4, pp. 398–402, 2014.
[194] O. G. Abood and S. K. Guirguis, "A Survey on Cryptography Algorithms," Int. J. Sci. Res. Publ., vol. 8, no. 7, 2018.
[195] S. S V, L. P M, and T. Bindu A, "Encryption Algorithms : A Survey," Int. J. Adv. Res. Comput. Sci. Technol., vol. 4, no. 2, pp. 81–88, 2016.
[196] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, "A survey of lightweight-cryptography implementations," IEEE Des. Test Comput., vol. 24, no. 6, pp. 522–533, 2007.
[197] S. A. Albermany and F. Radihamade, "Survey: Block cipher Methods," Int. J. Adv. Res. Technol., vol. 5, no. 11, pp. 11–22, 2016.
[198] M. Ebrahim, S. Khan, and U. Bin Khalid, "Symmetric Algorithm Survey: A Comparative Analysis," vol. 61, no. 20, pp. 12–19, 2014.
[199] R. A. F. Lustro, A. M. Sison, and R. P. Medina, "Performance Analysis of Enhanced SPECK Algorithm," in Proceedings of the 4th International Conference on Industrial and Business Engineering. ACM, 2018, pp. 256–264.
[200] B. Ryabko and A. Soskov, "The distinguishing attack on Speck, Simon, Simeck, HIGHT and LEA," IACR Cryptol. ePrint Arch., pp. 1–9, 2018.
[201] L. B. de Guzman, A. M. Sison, and R. P. Medina, "MD5 Secured Cryptographic Hash Value," in Proceedings of the 2018 International Conference on Machine Learning and Machine Intelligence. ACM, 2018, pp. 54–59.
[202] C. Baskar, C. Balasubramaniyan, and D. Manivannan, "Establishment of Light Weight Cryptography for Resource Constraint Environment Using FPGA," Phys. Procedia, vol. 78, no. December 2015, pp. 165–171, 2016.
[203] W. Du, J. Deng, and Y. S. Han, "A key predistribution scheme for sensor networks using deployment knowledge," IEEE Trans. Dependable Secur. Comput., vol. 3, no. 1, pp. 62–77, 2006.
[204] T. Ito, H. Ohta, N. Matsuda, and T. Yoneda, "A key predistribution scheme for deployable sensor networks using the node deployment probability density function," Electron. Commun. Japan, Part II Electron. (English Transl. Denshi Tsushin Gakkai Ronbunshi), vol. 90, no. 10, pp. 73–83, 2007.
[205] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang, and S. W. Baik, "Secure surveillance framework for IoT systems using probabilistic image encryption," IEEE Trans. Ind. Informatics, vol. 14, no. 8, pp. 3679–3689, 2018.
[206] B. Lai, S. Kim, and I. Verbauwhede, "Scalable session key construction protocol for wireless sensor networks," IEEE Work. Large Scale Realt. Embed. Syst., 2002.
[207] D. Y. T. V. and U. R. Shahid Raza, Simon Duquennoy, Tony Chung, "Securing Communication in 6LoWPAN with Compressed IPsec," in International Conference on Distributed Computing in Sensor Systems and Workshop, 2011.
[208] D. Forsberg and Y. Ohba, "Protocol for Carrying Authentication for Network Access (PANA)," RFC 5191, 2008.
[209] M. Kanda, S. Das, and S. Chasko, "PANA applicability in constrained environments," Smart Object Secur. Wksp., Paris, Fr., pp. 1–8, 2012.
[210] H. R. Hussen, G. A. Tizazu, M. Ting, and T. Lee, "SAKES: Secure Authentication and Key Establishment Scheme for M2M Communication in the IP-Based Wireless Sensor Network (6LoWPAN)," in 5th International Conference on Ubiquitous and Future Networks (ICUFN), 2013.
[211] E. Rescorla, "Diffie-Hellman Key Agreement Method," RFC 2631, June, 1999.
[212] R. Rivest, "The MD5 Message-Digest Algorithm," RFC 1321, vol. 4, p. 116, 1992.
[213] W. Du, R. Wang, and P. Ning, "An efficient scheme for authenticating public keys in sensor networks," in Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing. ACM, 2005, pp. 58–67.
[214] T. Bala and Y. Kumar, "Asymmetric Auctions Symmetric Auctions : A Review," Int. J. Comput. Appl. (0975, vol. 1, no. Icaet, pp. 1–7, 2015.
[215] N. Oualha and K. T. Nguyen, "Lightweight attribute-based encryption for the internet of things," in 2016 25th International Conference on Computer Communications and Networks, ICCCN 2016, 2016, pp. 1–6.
[216] G. Gaubatz, J.-P. Kaps, and B. Sunar, "State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks," in 3rd IEEE International Conference on Pervasive Computing and Communications Workshop (PERCOMW), 2005.
[217] M. O. Rabin, "Digitalized Signatures and Public Key Functions as Intractable as Factorization," MIT/LCS/TR-212, Massachusetts Institute of Technology, 1979.
[218] L. Yang, C. Ding, and M. Wu, "Establishing authenticated pairwise key using Pairing-based Cryptography for sensor networks," 2013 8th Int. ICST Conf. Commun. Netw. China, CHINACOM 2013 - Proc., pp. 517–522, 2013.

[219] D. A. N. Boneh and M. Franklin, "IDENTITY-BASED ENCRYPTION FROM THE WEIL PAIRING," Soc. Ind. Appl. Math., vol. 32, no. 3, pp. 586–615, 2003.
[220] G. De Meulenaer, F. Gosset, F. X. Standaert, and O. Pereira, "On the energy cost of communication and cryptography in wireless sensor networks," in Proceedings - 4th IEEE International Conference on Wireless and Mobile Computing, Networking and Communication, WiMob 2008, 2008, pp. 580–585.
[221] S. Al Salami, J. Baek, K. Salah, and E. Damiani, "Lightweight encryption for smart home," in Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016, 2016, pp. 382–388.
[222] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the Internet of Things," Futur. Gener. Comput. Syst., vol. 49, pp. 104–112, 2015.
[223] Y. Yang, X. Zheng, and C. Tang, "Lightweight distributed secure data management system for health internet of things," J. Netw. Comput. Appl., vol. 89, no. September 2016, pp. 26–37, 2017.
[224] S. Sahraoui and A. Bilami, "Efficient HIP-based approach to ensure lightweight end-to-end security in the internet of things," Comput. Networks, vol. 91, pp. 26–45, 2015.
[225] L. Yehia, A. Khedr, and A. Darwish, "Hybrid Security Techniques for Internet of Things Healthcare Applications," Adv. Internet Things, vol. 5, pp. 21–25, 2015.
[226] M. Xin, "A Mixed Encryption Algorithm Used in Internet of Things Security Transmission System," Proc. - 2015 Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov. CyberC 2015, pp. 62–65, 2015.
[227] R. J. Kavitha and B. E. Caroline, "Hybrid cryptographic technique for heterogeneous wireless sensor networks," 2015 Int. Conf. Commun. Signal Process. ICCSP 2015, pp. 1016–1020, 2015.
[228] Y. Zhang and P. Ji, "An efficient and hybrid key management for heterogeneous wireless sensor networks," 26th Chinese Control Decis. Conf. CCDC 2014, pp. 1881–1885, 2014.
[229] M. A. Habib, M. Ahmad, S. Jabbar, S. H. Ahmed, and J. J. P. C. Rodrigues, "Speeding Up the Internet of Things: LEAIoT: A Lightweight Encryption Algorithm Toward Low-Latency Communication for the Internet of Things," IEEE Consumer Electronics Magazine, vol. 7, no. 6, IEEE, pp. 31–37, 2018.
[230] M. Usman, I. Ahmed, M. I. Aslam, S. Khan, and U. A. Shah, "SIT: A Lightweight Encryption Algorithm for Secure Internet of Things," Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 1, pp. 1–10, 2017.
[231] A. Aziz and K. Singh, "Lightweight Security Scheme for Internet of Things," Wirel. Pers. Commun., vol. 104, no. 2, pp. 577–593, 2019.
[232] H. de Meer and J. P. G. Sterbenz, "Self-Organizing Systems," First Int. Work. IWSOS, Springer, New York, NY, USA., pp. 239–242, 2006.
[233] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions," J. Ambient Intell. Humaniz. Comput., vol. 0, no. 0, pp. 1–18, 2017.
[234] A. K. Pathan, S. Khanam, and H. Y. Saleem, "Tackling Intruders in Wireless Mesh Networks," Distrib. Netw. Intell. Secur. Appl. CRC Press. Taylor Fr. Group., pp. 167–190, 2013.
[235] J. Zhang and V. Varadharajan, "Wireless sensor network key management survey and taxonomy," J. Netw. Comput. Appl., vol. 33, no. 2, pp. 63–75, 2010.
[236] E. Glukhov, "Energy Analysis Of Public-key cryptography on small wireless devices," in Proceedings of the 3rd IEEE Int'l Conf. on Pervasive Computing and Communications (PerCom 2005), 2005.
[237] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," Internet of Things, vol. 7, p. 100059, 2019.
[238] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, and K. K. R. Choo, "A Two-Layer Dimension Reduction and Two-Tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks," IEEE Trans. Emerg. Top. Comput., vol. 7, no. 2, pp. 314–323, 2019.
[239] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," IEEE Trans. Emerg. Top. Comput. Intell., vol. 2, no. 1, pp. 41–50, 2018.