Received: 6 July 2017 | Revised: 19 February 2018 | Accepted: 3 March 2018 | Published on: 3 May 2018

DOI: 10.1002/spy2.20

SURVEY PAPER

WILEY

Challenges of securing Internet of Things devices: A survey

Musa G. Samaila[1,2] | **Miguel Neto**[1] | **Diogo A. B. Fernandes**[1] | **Mário M. Freire**[1] | **Pedro R. M. Inácio**[1]

[1]Instituto de Telecomunicações and Department of Computer Science, Universidade da Beira Interior, Covilhã, Portugal

[2]Centre for Geodesy and Geodynamics, National Space Research and Development Agency, Toro, Nigeria

Correspondence
Musa G. Samaila, Department of Computer Science, Universidade da Beira Interior, Rua Marquês d'Ávila e Bolama, 6201-001 Covilhã, Portugal.
Email: mgsamaila@it.ubi.pt

Funding Information
This research was supported by the Fundação para a Ciência e a Tecnologia, UID/EEA/50008/2013. Centre for Geodesy and Geodynamics, National Space Research and Development Agency, Toro.

The current vision of the Internet of Things (IoT) is to ensure that everything from everywhere is connected to the Internet at all times using Internet Protocol (IP). This idea has the potential of making homes, cities, electric grids, among others, safer, more efficient, and easier to manage. Nevertheless, a number of obstacles still remain to fully realize the IoT vision, with security and privacy among the most critical. Ensuring security and privacy in the IoT is particularly complicated, especially for the resource-constrained devices due to finite energy supply and low computing power. These factors are typically at odds with most of the existing security protocols and schemes proposed for the IoT because of the intensive computational nature of the cryptographic algorithms involved. This paper performs an extensive comparison of previous surveys on the subject, and shows its novelty with respect to the previous work. It describes 9 application domains and presents, in detail, security requirements, system models, threat models along with protocols and technologies for those 9 application areas. The survey also performs an exhaustive examination of some existing mechanisms and approaches proposed in the literature for ensuring security and privacy of IoT devices. Finally, it outlines some open research issues associated with IoT security.

KEYWORDS

application domain, Internet of Things, privacy, protocols, security, security requirements, system model, threat model

1 | INTRODUCTION

The *Internet of Things* term, coined by Kevin Ashton in 1999,[1] is a paradigm of communication that is rapidly gaining ground in different application areas. In this paradigm, industry objects[2] and everyday devices, such as ordinary household gadgets that are part of our daily lives like washing machines, thermostats, door locks, refrigerators, TVs, among others, are expected to have sensors, and network connectivity through Internet protocol (IP)-based communication protocols, allowing them to transmit and receive data via computer networks. Thus extending Internet connectivity beyond traditional devices like computers, tablets and smartphones to a wide range of everyday consumer products,[3] especially leveraging the large address space of Internet Protocol Version 6 (IPv6).[4] Internet of Things (IoT) devices use IP-based connectivity and short-range communication technologies and standards that include Bluetooth, ZigBee, Z-Wave, and Near-Field Communication (NFC) to communicate with each other, Machine-to-Machine (M2M), with the environment, or with people.[5]

Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSNs) are examples of technologies that enable the interconnection of the virtual world and these physical objects.[6] Advancements in these technologies coupled with the recent developments in the field of embedded systems, motivated by the technological advancements in the fields of wireless communications, digital electronics and Micro Electro-Mechanical Systems (MEMS) technology[7] have revolutionized how *things* are manufactured.[8,9] Nowadays, many devices are manufactured smart,[10] meaning that they include some features that enable them to connect to the web, interact with, and learn from their environment.[11] Some IoT devices are small, portable, inexpensive, and can even be connected versions of the disposable devices that surround us.[7,12] These devices range from simple household appliances such as bread toasters[13] to autonomous vehicles.[14]

Cloud computing facilitates the operations of the IoT by providing a powerful, flexible and affordable framework that offers real-time end-to-end services to numerous businesses and users to access applications at any time and from anywhere.[15,16] While IoT is generally characterized by limited resources in terms of energy supply, computation power and memory, cloud computing can be said to have unlimited capabilities in terms of resources. Thus, merging the 2 technologies together, described in[17] as CloudIoT, can enable a variety of efficient application scenarios.

In recent years, IoT is becoming deeply interwoven into our daily lives by automating our homes, routine work, and personal tasks.[18,19] It is envisaged that IoT will be among the technologies that will play a leading role in shaping the destiny of humanity in the near future.[20] As a result, it is increasingly gaining more attention from both academia and industry. IoT is envisioned to extend the Internet connection or local networking connectivity to almost every useful physical object, thereby agreeing with the concept of ubiquitous computing proposed in the early 1990s by Mark Weiser.[21,22] As a huge network, consisting of a variety of heterogeneous networks and devices, the application areas of the IoT is rapidly growing and opening new opportunities for various businesses. It is expanding from simple logistics to Wireless Body Area Networks (WBANs), industrial manufacturing, and smart infrastructures such as smart grids, smart cities, and smart cars.[23,24]

Although the number of connected devices is rapidly growing,[25] enabling the creation of new innovative business models, security and privacy are not usually given the attention they deserve.[26,27] Hence, there are many traditional and new[28] security and privacy issues associated with the IoT,[29] which threaten its acceptability.[30–33] Connecting smart devices with weak or no security to the Internet may ultimately translate to a larger attack landscape and increased entry points for potential adversaries.[34,35] Consequently, the focus of this survey is to provide an overview of security and privacy issues in the IoT, with special emphasis on the security of the resource-constrained devices, which are more vulnerable, considering that a number of security and privacy issues of the IoT originate from them. Other main contributions of this work include the definition and discussion of system and threat models, and delineation of security requirements, contextualized against well-defined application domains, with which the discussion is organized. Research gaps are also identified herein.

The remainder of the paper is organized as follows. Section 2 presents a review of related works and outlines the major contributions of this survey. Section 3 discusses IoT architecture, and 9 application domains. Section 4 presents detailed discussions on IoT security requirements, system model, threat model, and protocols/technologies per domain. Section 5 reviews schemes and technologies for securing IoT, covering proposals for solutions based on cryptographic primitives; solutions based on authentication and access control protocols; proposals for hardware solutions; solutions for specific application domains; and current security mechanisms. Section 6 highlights some open research issues that have not been fully addressed. Finally, section 7 provides a brief summary and wraps up with some conclusions.

2 | RELATED WORK

The IoT has been extensively studied for more than a decade now and, in recent years, a number of researchers from academia, industry, and government agencies worldwide have carried out several studies investigating different aspects of this technology. One of the aspects that has attracted the attention of many researchers is that of security/privacy. Although the main focus of this section is to review the surveys on the security and privacy issues associated with the IoT devices, some surveys that do not focus exclusively on these topics are also considered, namely the ones on applications, trust management and other technical issues. Previous related works are then compared with this survey.

2.1 | Security and privacy issues

Kumar and Patel[36] discussed the basic concept of IoT and explored its evolution, covering everything from the beginning of communications between 2 computers in the late 1960s to this era. Most importantly, they critically examined the security concerns in the IoT and studied the possible threats associated with the different layers, which they classified as: *front-end sensors and equipment, network and back-end of Information Technology (IT) systems*. The authors also discussed privacy concerns that need to be addressed, namely: *privacy in device, privacy during communication, privacy in storage and privacy at processing*.

Zhao and Ge[37] proposed a 3-layer security architecture for the IoT and explained a number of security issues within the context of that architecture. They pointed out the security problems of each of the layers, and highlighted the possible damages that these problems might inflict on the IoT network and services. They particularly elaborated on the security issues of the perception layer, which include key management and algorithm, security routing protocols, data fusion technology and authentication, and access control.

Granjal et al[38] observed that security will certainly be a fundamental enabling factor for most IoT applications and services, thus they emphasized the need for measures to be put in place to secure communications across diverse technologies. The authors critically examined several existing protocols and mechanisms for securing communications in the IoT, and analyzed how these approaches meet the fundamental security requirements. They also presented a number of proposals, for example, for key management, security against packet fragmentation attacks and solutions against internal attacks. Furthermore, they pointed out some security challenges that need to be addressed in the near future.

Sicari et al[39] extensively reviewed the existing solutions within the IoT security topic, covering integrity, confidentiality, authentication, privacy, and trust issues in the IoT field. They also studied proposals on security middlewares and secure solutions for mobile devices, as well as explored some ongoing projects. The authors observed that IoT services can only gain the trust of users when there is a proper enforcement of security and privacy policies. They further highlighted some open research issues, one of which is the need for a unified vision pertaining to the insurance of security and privacy requirements in heterogeneous environments like IoT.

Grabovica et al[40] considered security measures of IoT enabling technologies. The authors explored security protocols of relevant communication technologies that are used in the IoT, including RFID, wireless networks and ZigBee. Their work presents an overview of the security attributes of the given technologies as well as introduce practical implementation and possible intrusions. Furthermore, they presented analysis that provides basic information pertaining to security modes, cryptography possibilities and functional appliance in the IoT that need attention. The authors, finally, identified some issues that can arise in practical applications, and provided comparison and summary of the advantages of the technologies they described.

Granjal et al[41] analyzed many existing surveys aimed at addressing different security mechanisms for the WSNs applications. They particularly focused on current investigations from the research community and proposals from the industry pertaining to the integration of these low-power devices with the Internet. The authors also provided detailed discussions of the analysis of the security requirements for this integration and the corresponding attack and threat models. Finally, they highlighted some challenges regarding the usage of the existing security mechanisms for protecting the Internet-integrated WSNs.

Benabdessalem et al[42] reviewed research progress on IoT security models, techniques and tools. The authors first analyzed a number of security requirements, and then explored the different approaches and mechanisms used for ensuring security and privacy in IoT. They also provided a summary of existing security methods and mechanisms.

Suo et al[43] explored the progress of research in the field of IoT. They specifically focused on the security aspects, and provided a concise analysis of the security features and requirements. The authors reviewed some key security techniques, which include cryptographic algorithms, encryption mechanisms, and secure communications. They also considered protection of sensor data, and concluded by pointing out some research challenges.

Oracevic et al[44] provided a quick review of IoT security issues and challenges, focusing specifically on recent security solutions. The authors attempted to provide a holistic overview of IoT security rather than focusing on a single layer of the architecture. Their work also identified some open issues that have not been properly addressed.

Yang et al[45] presented a survey of recent hardware designs of Ultra-Low-Power (ULP) devices in the IoT. Their work focused on optimizing the tradeoffs between power, cost of the ULP devices and security. The authors discussed both cryptography-based entity authentication and hardware designs for Physical Unclonable Functions (PUFs)-based entity authentication, and thereafter highlighted the need for better hardware blocks in order to support device authentication and data security. Their work identified open issues and future research directions for security-focused ULP hardware designs. The authors also showed that it is the type of application that determines which design and protocol are to be employed. For instance, PUFs-based authentication protocols are best for systems that require encryption engines.

Chen et al[46] provided an in-depth review of threats and solutions associated with Location-Based Services (LBSs) in the IoT. The authors reviewed both Global Navigation Satellite System (GNSS) and non-GNSS-based solutions. After describing certain security and privacy solutions for LBSs based on cryptography, the authors discussed in detail the most recent policies, regulations, and legal implications regarding location data privacy. The authors concluded by highlighting some privacy-preserving issues in LBSs solutions, and presented some recommendations that will foster the development of more secure LBSs in the future.

Qiu et al[47] investigated the heterogeneity and relationship among diverse networks of the IoT, including WSNs, Wireless Fidelity (Wi-Fi), Wireless Mesh Networks (WMNs), and vehicular networks, which they termed HetIoT. The authors presented a comprehensive review of the state-of-the-art in the HetIoT research area, and proposed a 4-layer architecture for the HetIoT consisting of sensing, networking, cloud computing and applications layers, and discussed them extensively. For example, the authors analyzed a number of classical application areas in the application layer, such as WeChat, Skype, and smart home.

Their survey highlighted some open issues in a few application domains, and also presented open research issues for building large-scale HetIoT, which include smart hardware design, big data fusion, and security and privacy.

Sezer et al[48] presented an extensive and comprehensive survey in context-aware computing, learning algorithms, and big data in IoT. The authors also reviewed extended IoT research fields, namely Web of Things (WoT) and semantic. They categorized IoT survey papers into 7 categories, including general purpose surveys and open issues, context awareness, machine learning on specific topics, and data mining surveys. Their work identified a number of open issues which include security and privacy in the IoT.

2.2 | Applications, trust management and other technical issues

Starting with the vision and motivations for IoT, Miorandi et al[49] provided a broad concept of the IoT by defining a smart *thing* as any object that possess physical features like specific size and shape, some communication functionalities and some basic computing capabilities. They also presented some key system features that should be supported by IoT, namely devices heterogeneity, scalability, energy-optimized solutions, and so on. The authors outlined some research challenges in some key areas, including computing, communication and identification, distributed systems technology and distributed intelligence. Furthermore, they highlighted the importance of security as a critical component that will enable the widespread adoption of the IoT.

Yan et al[50] did an extensive study on trust, its properties and trust management, and concluded that trust management makes people overcome fears and perceptions of uncertainty concerning the risks associated with the adoption of IoT devices, applications and services. They reviewed current researches on trustworthy IoT and pointed out 7 open research issues. They further outlined some challenges facing trust management in the IoT, which include the heterogeneous nature of the IoT and power efficiency. Moreover, they proposed an holistic trust management framework for IoT that is based on both interlayer and cross-layer trust management, and provides practical and intelligent IoT applications and services.

Al-Fuqaha et al[51] focused on enabling technologies, protocols and applications. After providing a horizontal overview of IoT, the authors discussed the IoT enabling technologies, protocols and applications in detail. Their survey provides a compressive summary of the most relevant protocols and application issues for researchers and developers to work with, without having to begin a thorough search process all over again. They also outlined some key IoT challenges in the recent literature, which include security and privacy. The authors also presented service use-cases in detail in order to illustrate how the protocols they presented work together to provide the desired IoT services.

Xu et al[12] thoroughly reviewed current research works on IoT and the enabling technologies, such as identification and tracking, communication and service management. They also explored the applications of IoT in key industries like healthcare, mining, transportation and logistics. The authors highlighted some research challenges, including technical, standardization and information security and privacy protection related challenges. They concluded by identifying other research trends, which include integrating social networking with IoT solutions, developing green IoT technologies, developing context-aware IoT middleware solutions and employing artificial intelligence techniques to create intelligent *things* or smart objects.

Atzori et al[52] provided descriptions of IoT and its visions in different contexts. They surveyed the enabling technologies in the literature and explained the impacts and applications of the new paradigm in everyday-life, which they grouped into the following domains: transportation and logistics, healthcare, smart environment and personal and social domains. The authors further analyzed some open issues, including standardization activity, addressing and networking, and security/privacy issues.

Kraijak and Tuwanut[53] surveyed a number of subjects on IoT, namely architecture and protocols, applications, security and privacy concerns as well as implementation and future trends. Their work starts by considering the evolution of IoT and its importance to humanity. The authors then focused on the security and privacy concerns in the IoT. They also presented a real-world implementation using an Arduino platform and a lightweight communication protocol for IoT. Finally, they highlighted some future trends.

Li et al[1] reviewed a number of definitions, architectures, applications and basic technologies of IoT, and then proposed a service-oriented architecture for the heterogeneous network, consisting of 4 layers, namely sensing layer, network layer, service layer, and interface layer. The authors presented some open issues, which include technical challenges, standardization, security and privacy protection and innovation in IoT environment, and thereafter discussed potential solutions to the issues presented.

Razzaque et al[54] focused on middleware for the IoT. The authors presented a number of IoT middleware requirements that are grouped into 2 different sets, namely middleware service requirements and architectural requirements. They provided a comprehensive review of existing middleware solutions against the given requirements. They also presented open issues and challenges, which include security and privacy; and finally, outlined some future research directions.

Moness and Moustafa[55] reviewed the advances and the state-of-the-art technologies enabling Wind Energy Conversion System (WECS) for the Internet of Energy (IoE), and then highlighted the potentials of Cyber-Physical System (CPS). The authors then discussed the requirements and challenges of the future WECS and CPS, including abstractions, networking, control, safety, security, sustainability, and social components.

Whitmore et al[56] focused on reports on the current research on the IoT by reviewing the literature, which they classified into 6 different categories, viz.: *technology*, *applications, challenges, business models, future directions*, and *overview/survey*. Using their classification scheme, they pointed out distinct trends in the distribution of the published works on IoT, emphasizing, for example, the areas that are not adequately treated. The authors identified *security*, *privacy*, *and legal/accountability* as some of the major challenges preventing its widespread adoption.

2.3 | Comparison of previous surveys on the subject

As the IoT threat landscape continues to expand, it is important to explicitly characterize the security of every IoT system in accordance with the modern cryptographic best practices.[57] This should involve a definite characterization of the system (system model), clear identification of attacker and his capabilities (threat model) and security goals one is aiming to achieve (security requirements). While this work pays particular attention to these and other aspects of the IoT security, no other previous reviews focused on this essential ingredient of cyber security. Along with the thorough survey on the specialized literature, this comprises one of the major contributions of this work. Table 1 provides comparison of the reviewed works with this survey. The surveys are compared with respect to system model, threat model, protocols and technologies, security requirements, scenario considerations, review of existing solutions, as well as with respect to security and privacy open issues. Four symbols are used to denote how an aspect of the subject matter is covered in a particular survey article. While **x** is used to denote aspects that are not treated in a survey, ☆, ★ and ✓ show the degree to which a particular aspect is covered. For instance, a ☆ indicates a shallow coverage, a ★ signifies that a given aspect is sufficiently covered, and a ✓denotes an in-depth coverage. The key contributions of this survey include:

- detailed survey of the specialized literature;
- description of different IoT application domains, and using them to organize the work;
- identification of assets per domain;
- definition of security requirements per domain;
- definition of system and threat models, as well as identification of protocols and technologies for the application domains defined within the scope of the work;
- thorough review of schemes for securing the IoT.

To the best of our knowledge, this survey is the first work that addresses the characterization of IoT security using system model, threat model, protocols/technologies, and security requirements; and at the same time not losing focus on the typical scenario considerations, review of existing solutions, and security/privacy issues.

3 | ARCHITECTURE AND APPLICATION DOMAINS

This section discusses IoT architecture, and considers 9 application domains.

3.1 | IoT architecture

The extremely large variety of connected heterogeneous networks and devices has made building a general architecture for the IoT a very complex task.[11] Nonetheless, IoT structure can generally be divided into 3 distinct layers, namely, the perception layer (also referred to as recognition layer), the network layer and the application layer,[6,36,37] as shown in Figure 1.

The perception layer is responsible for gathering all kinds of data/information from the physical world using physical end devices, such as RFID tags and readers, cameras, Global Positioning System (GPS) receivers and all sorts of sensors.[43,58] The network layer, which is in the middle, consists of different kinds of communication networks, which serve as access networks.[58] This layer is also responsible for assortment of data, initial processing and transmission of data.[59] The topmost layer is the application layer, which provides support for business services and different kinds of personalized services to individual users.[60] Application layer protocols include Constrained Application Protocol (CoAP), Message Queue Telemetry Transport (MQTT), Extensible Messaging and Presence Protocol (XMPP), Advanced Message Queuing Protocol (AMQP), and Data Distribution Service (DDS). Using the application layer interface, users can access the IoT via personal computers, mobile devices such as smartphones and tablets. Depending on the services, other device like smart refrigerators, smart televisions, etc. can also be used.

The network layer is critical because it serves as the link between the perception and the application layers.[59] Long-range communication can be achieved using IP based Internet, such as 2G, 3G, 4G, LTE or the impending 5G network, while IEEE

TABLE 1 Comparison of this work with reviewed surveys with respect to several security related subjects

Articles	Survey subject	Year	System model	Threat model	Protocols and technologies	Security requirements	Scenario considerations	Review of existing security Solutions	Security/privacy open issues
Atzori et al[52]	Survey on IoT	2010	x	x	☆	x	★	x	✓
Suo et al[43]	Security in the IoT	2012	x	x	☆	★	x	x	★
Miorandi et al[49]	IoT vision, applications and research challenges	2012	x	x	☆	x	★	x	★
Zhao and Ge[37]	A survey on the IoT security	2013	x	x	☆	x	x	x	x
Kumar and Patel[36]	A survey on IoT security and privacy issues	2014	x	x	x	☆	★	x	★
Xu et al[12]	IoT in industries	2014	x	x	☆	x	★	x	★
Yan et al[50]	Trust management for IoT	2014	☆	x	★	☆	★	x	✓
Benabdessalem et al[42]	Survey on security models, techniques, and tools for IoT	2014	x	x	☆	☆	☆	☆	★
Granjal et al[38]	IoT security protocols	2015	x	☆	★	✓	☆	✓	★
Sicari et al[39]	Security, privacy and trust in IoT	2015	x	x	★	★	★	★	★
Granjal et al[41]	Security in integration of low-power WSNs with Internet	2015	x	✓	★	★	☆	✓	★
Li et al[1]	Survey on IoT	2015	x	x	★	x	☆	x	★
Whitmore et al[56]	Survey of IoT topics and trends	2015	x	x	☆	x	☆	x	★
Al-Fuqaha et al[51]	IoT survey on enabling, technologies, protocols and applications	2015	x	x	★	x	★	x	★
Kraijak and Tuwanut[53]	Survey on IoT architecture, protocols, applications, security, privacy, implementation and future trends	2015	x	x	★	x	★	x	★
Grabovica et al[40]	Survey on IoT provided security measures of enabling technologies	2016	x	x	☆	☆	x	x	★
Razzaque et al[54]	Survey on IoT middleware	2016	x	x	★	x	x	x	☆
Moness and Moustafa[55]	Survey on cyber-physical advances and challenges of WECSs: prospects for IoE	2016	x	x	x	x	★	☆	☆
Oracevic et al[44]	Security in IoT: A survey	2017	x	x	x	☆	☆	★	★
Yang et al[45]	Hardware designs for security in ULP IoT systems: an overview and survey	2017	x	x	★	x	x	☆	☆
Chen et al[46]	Robustness, security and privacy in LBSs for future IoT: a survey	2017	x	x	☆	x	x	★	☆
Qiu et al[47]	How can heterogeneous IoT build our future: a survey	2018	☆	x	★	x	★	★	★
Sezer et al[48]	Context-aware computing, learning, and big data in IoT: a survey	2018	x	x	★	x	★	x	★
This article	Challenges of securing IoT devices	—	✓	✓	✓	✓	✓	✓	✓

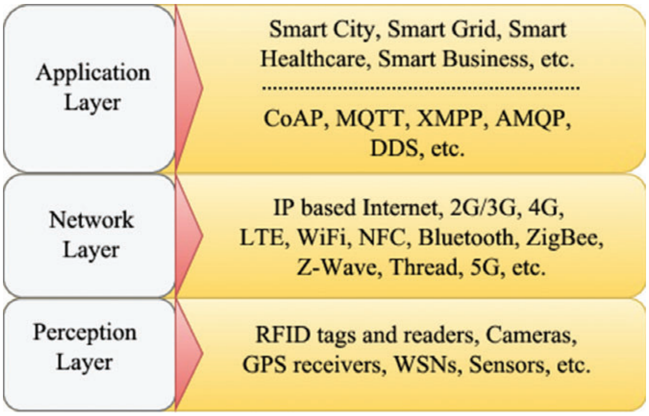

Application Layer
Smart City, Smart Grid, Smart Healthcare, Smart Business, etc.
CoAP, MQTT, XMPP, AMQP, DDS, etc.
Network Layer
IP based Internet, 2G/3G, 4G, LTE, WiFi, NFC, Bluetooth, ZigBee, Z-Wave, Thread, 5G, etc.
Perception Layer
RFID tags and readers, Cameras, GPS receivers, WSNs, Sensors, etc.

FIGURE 1 Basic architecture of IoT

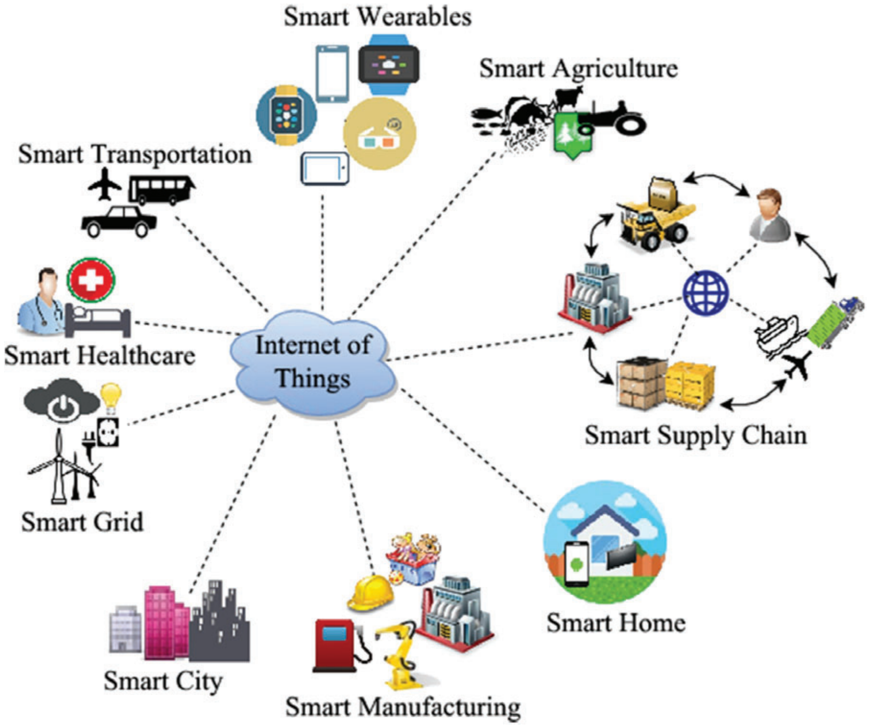


FIGURE 2 Typical IoT ecosystems setup

802.15.4 (ZigBee), Z-Wave, Thread, ultra-wideband (UWB), Bluetooth and NFC are used for short-distance communications among the IoT devices due to power, computation and storage constraints.[61]

3.2 | Application domains

Presently, IoT might not have widespread visible effects on the society, but its impact is already noticeable in many industrial sectors. This article considers a few among many of the IoT application domains that have emerged in recent years. It focuses mainly on some of the domains that have great potential for exponential growth in the fourth industrial revolution, namely home automation,[62] energy,[63] developed urban areas,[64] transportation,[65] healthcare,[66] manufacturing,[67] supply chain,[68] wearables,[69] and agriculture,[70] as depicted in Figure 2.

3.2.1 | Application domains and their associated cyber assets

In cyber security, knowing the assets that need to be protected is fundamental to identifying vulnerabilities, threats, and risks. For the purpose of this study, we define an asset as tangible or intangible resource of value to an individual or a company that is exposed on an IoT network, which is also of interest to an attacker. Such a resource can be hardware, software, or a piece of data that can be found in any of the 3 layers of the IoT architecture. Typical IoT assets include devices, smart or connected equipment, communication channels, communication protocols, and applications. Brief discussions of the application areas shown in Figure 2 are presented below along with the list of identified cyber assets per domain. Figure 3 depicts some of the important assets that can be found on the application domains.

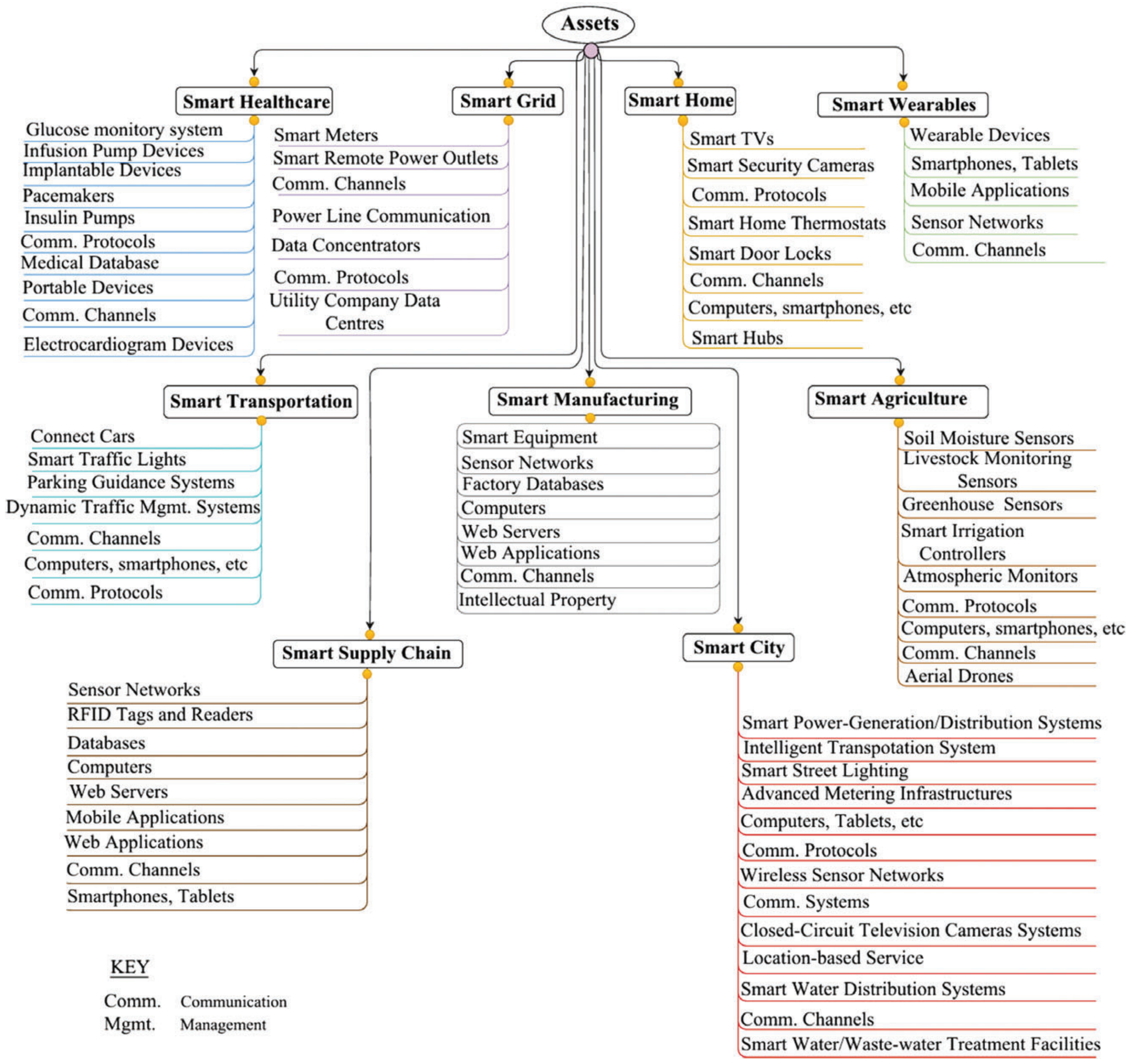


FIGURE 3 Overview of typical IoT assets for 9 application domains

- *Smart home*: Is a house or living environment where household appliances like toasters, washing machines and other everyday devices can be remotely monitored and controlled[71] using smartphones, tablets, or laptop computers from anywhere in the World via the Internet or private network. This might enhance home care and monitoring, access control, energy efficiency, convenience and quality of everyday life. Smart TVs, security cameras, thermostats, refrigerators, door locks, garage door openers, and smart hubs are typical cyber assets in the smart home domain.
- *Smart grid*: This is an energy delivery concept that promises to optimally and efficiently deliver the highest quality of energy at the lowest cost possible.[72] It will provide more accurate monitoring and control adaptation, where consumers can analyze their consumption pattern via the 2-way communication between their smart meters and the operators.[73] Typical smart grid cyber assets are: smart meters, remote power outlets, transformers, Power Line Communication (PLC), data concentrators, load balancing systems, and data centers.
- *Smart city*: Is the city that employs digital technologies to improve services in key sectors of the economy like healthcare,[74,75] water,[76] energy,[64,77] transport,[78] and waste-water treatment[79] for the well-being of its citizens. A smart city is also expected to be proactive to global challenges.[80] Examples of smart city cyber assets include: power-generation/distribution systems, Intelligent Transportation System (ITS), street lights, Advanced Metering Infrastructure (AMI), water/waste-water treatment facilities, water distribution systems, WSNs, communication systems, Closed-Circuit Television (CCTV) cameras, and LBSs.
- *Smart transportation*: An IoT based ITS is expected to provide a safer,[81] cleaner and more efficient transport system[82] by using real-time traffic information and interconnecting vehicles and roadside infrastructures for more efficient data acquisition,

processing and decision making.[83] Additionally, it will improve quality of life by decreasing congestion, and hence shortening travel time, as well as reducing fuel/electricity usage.[84] While smart transportation may sometimes be considered part of smart city, it is actually a distinct application domain.[85–87]Typical cyber assets in smart transportation include: connected cars, traffic lights, parking guidance systems, and dynamic traffic management systems.

- *Smart healthcare*: Refers to a health care paradigm that allows for remote healthcare monitoring[88] and Telehealth,[89] where doctors and other medical practitioners can examine, diagnose and treat patients remotely. Smart healthcare services are becoming commonplace, especially in countries like India.[88,90] Typical cyber assets in this domain include: glucose monitoring systems, infusion pumps, implantables, pacemakers, insulin pumps, electrocardiograms, medical databases and mobile devices like smartphones.
- *Smart manufacturing:* Is the fourth revolution of the manufacturing industry (Industry 4.0),[91] a technological convergence between the existing manufacturing technologies and other technologies such as IoT, CPS, Internet of Services (IoS), WSNs, cloud computing, Artificial Intelligence (AI) and machine learning, creating a manufacturing paradigm that responds in real-time to changes in factory conditions, and customer needs. By analyzing massive data collected from smart devices and sensors, early warning of product quality defects, as well as impending machine failures can be predicted in real-time to guarantee efficiency and quality.[92] Typical cyber assets include smart equipment, WSNs, factory databases, computers, web servers, web applications, communication channels, and intellectual property.
- *Smart supply chain*: Refers to a proactive and customer-centric monitoring, tracking, and remote asset management system that integrates different technologies to provide information on location, status, environment, and functionality of products and services. Typical technologies used include IoT, WSNs, RFID, CPS, big data, cloud computing, advanced analytics, and semi-autonomous decisions enabled by AI to build an optimized supply chain that reduces operational costs,[68] improves assets identification along the chain,[93] and allows for timely responses to unexpected events. Blockchain is another novel technology that will greatly facilitate smart supply chain, and is recently being use in smart supply chain management.[94] Smart supply chain uses enormous amount of real-time data derived from different sources, allowing multiway communication between partners, thus making it is fully transparent to all stakeholders, from suppliers of raw materials to the shippers of the raw materials and the finished products, and finally to the customers. Typical cyber assets include WSNs, RFID devices, databases, computers, web servers, mobile applications, web applications, smartphones or tablets, and communication channels.
- *Smart wearables*: Are end-to-end integrated gadgets embedded with smart sensors and actuators that connect wirelessly to the smartphone or tablet of the user, often using Bluetooth Low Energy (BLE) technology. They are usually worn on the wrist, clipped to the body, or hung around the neck for the purpose of staying fit, being more organized, losing weight, staying active, or for tele-medicine purposes.[95] The applications of smart wearables span across different domains, including sports, healthcare, entertainments, and military.[96] Typical cyber assets in smart wearables include wearable devices, smartphone or tablet, mobile applications, WSNs, and communication channels.
- *Smart agriculture*: Is a sustainable farming practice that employs IT and other relevant technologies to increase the per unit yield of farming land by optimizing water use and preserving other natural resources in order to increase crop yields and financial returns.[97,98] Smart farming also enhances precision livestock farming, where farm animals are monitored for prompt disease detection, early treatment and nutrition interventions.[99] Examples of cyber assets in this domain include: soil moisture sensors, livestock monitoring sensors, greenhouse sensors, irrigation controllers, atmospheric monitors, and aerial drones.

4 | SECURITY REQUIREMENTS, SYSTEM MODELS, THREAT MODELS, AND PROTOCOLS

This section defines security requirements, presents a system and threat models, as well as outlines typical protocols and communication technologies for each of the 9 application domains described in the previous section.

4.1 | Security requirements

There exist different security issues to be addressed within the 3 layers of the IoT architecture. For example, the perception layer is vulnerable to all sorts of physical attacks, such as malicious tampering of end devices and their communication links, and Denial-of-Service (DoS) attacks. The network layer is exposed to several threats found in the traditional computer networks; it also has some vulnerabilities that are more specific to the IoT, including network protocol issues, privacy disclosure, and compatibility issues. Like any other IT client with Human-Machine Interface (HMI), the application layer also has some vulnerability issues such as data access, security authentication, and malware.[100]

Security requirements, which are essentially the basis for measuring security, can be defined as a set of conditions that describe properties of IoT security goal. Security goals such as confidentiality, integrity, availability, and nonreputation are considered as properties to achieve security objectives.[101] Considering the diversity in the IoT ecosystem, there is need to effectively specify the security requirements that describe more concretely what measures and controls must be prescribed to assure the security of each of the application domains.

Generally, the primary goals of network security can be described in terms of 3 fundamental security properties: confidentiality, integrity and availability, usually coded by CIA.[102,103] However, the aforementioned security properties have been broaden over time to include other security properties like authenticity, authorization, nonrepudiation, accountability, reliability, privacy, and physical security. Below, we provide brief descriptions of these security properties.

- *Confidentiality*: Is the property that ensures that information is not disclosed or made available to any unauthorized entity. There are growing concerns over the confidentiality of the IoT[104,105] since such connected devices are often used for transmitting confidential data.
- *Integrity*: Is the property of safeguarding the correctness and completeness of assets in an IoT system. Connected devices often store sensitive data locally,[106] which include personal user data like credit card numbers and medical records, manufacturers data, and service providers data. They may include data that is critical to the security of the system, such as media decryption keys, business plans, product designs, billing logs, and so on.
- *Availability*: Refers to the property which ensures that an IoT device or system is accessible and usable upon demand by authorized entities. Availability can be affected by technical issues like device malfunctioning, natural disaster such as storm or flood, or human activities, which may be accidental or deliberate. Availability can be ensured by preventive maintenance and using up-to-date software. Redundancy and fail-over minimize the effects caused by hardware issues.
- *Authenticity*: Is the assurance that information transaction is from the source it claims to be from. Device authenticity can be verified through authentication, which involves proof of identity. Device authentication enables a device to access a network based on credentials stored in a (presumably) safe location. The device authenticates itself prior to receiving or transmitting any information.
- *Authorization*: A property that determines whether the user or device has rights/privileges to access a resource, or issue commands.
- *Non-repudiation (NR):* NR is the security property that ensures that the transfer of messages or credentials between 2 IoT entities is undeniable. It is often achieved by using a Trusted Third Party (TTP),[107] which provides an evidence of the transaction.
- *Accountability*: Is the property that ensures that every action can be traced back to a single user or device.
- *Reliability:* Refers to the property that guarantees consistent intended behavior of an IoT system.
- *Privacy*: In the context of IoT, privacy refers to the control of the user over the disclosure of his data. Privacy is becoming specially relevant in the context of IoT,[108,109] where devices monitor and collect data from the life of users.
- *Physical security*: Refers to the security measures designed to deny unauthorized physical access to IoT devices and equipment,[110] and to protect them from damage or harm.

The following are some security services or mechanisms that can be used to achieve security requirements.

- *Authentication*: Is the security service that verifies the identity of a user or device.
- *Access control*: In the context of IoT, access control refers to the security mechanism that limits the actions or operations of a legitimate user or device in an IoT system, as well as defining a limit for programs executing on behalf of the legitimate user.
- *Encryption*: Is the process of translating or encoding an information into a secret code such that only authorized entities can decode it.
- *Secure booting*: This security feature enables a device to check every software using digital signature or checksums, including the operating system, when the device is first powered on, or whenever it restarts. This will ensure that only authorized software run on the IoT device.
- *Secure updates*: Ensure that smart devices authenticate security patches from operators using digital signatures so that patches cannot be intercepted, extracted, and modified, thereby preventing updating interfaces from turning into security holes themselves.
- *Back-up*: Is copying and archiving of valuable data for the purpose of restoring the original in the event of data loss.
- *Securing physical location*: Refers to putting obstacles like locks and fencing in the way of people with malicious intention, as well as hardening physical sites against accidents and environmental disasters.
- *Device Tampering Detection (DTD):* In the context of IoT, DTD refers to the security mechanism that ensures that any attempt to tamper with an IoT device or network (whether logically or physically) is detected.

4.1.1 | Security requirements per domain

Essentially, security requirements should be specified based on the analysis of the services and assets to be protected, and the cyber threats from which such services and assets should be protected. This section outlines the security requirements for each

TABLE 2 Summary of security requirements for nine application domains

	Security requirements									
Application domains	**Conf**	**Intg**	**Avail**	**Authnt**	**Authrz**	**Nr**	**Acct**	**Reli**	**Priv**	**Phys Sect**
Smart home	✓	✓	✓	✓		✓	✓	✓	✓	✓
Smart grid	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Smart city	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Smart transportation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Smart healthcare	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Smart manufacturing	✓	✓	✓	✓	✓	✓	✓	✓		✓
Smart supply chain	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Smart wearables	✓	✓	✓	✓	✓			✓	✓	✓
Smart agriculture	✓	✓	✓	✓	✓		✓	✓		✓

Abbreviations: Acct, accountability; Authnt, authenticity; Authrz, authorization; Avail, availability; Conf, confidentiality; Intg, integrity; Nr, nonrepudiation; Phys sect, physical security; Priv, privacy; Reli, reliability.

of the 9 application domains. The security requirements are presented in a holistic manner, approaching the issue from a system perspective rather than a layered approach. Table 2 provides a summary of the security requirements for the 9 application domains.

Smart home security requirements—Given the characteristics of Smart Home, the following security requirements should be guaranteed, that:

1. information is protected from disclosure to unauthorized individuals or devices (confidentiality, privacy);
2. no data are modified or deleted by unauthorized persons for any malicious reasons (integrity, accountability);
3. only authorized devices and users are allowed to access any information on the network (authenticity, authorization);
4. an attacker cannot be able to decipher any captured or sniffed data (confidentiality)
5. the services of smart devices should be available to authorized entities whenever needed (availability, reliability);
6. even if an attacker gains physical access into a smart home, it should be unfeasible for the attacker to have access to any meaningful data (confidentiality, authenticity, physical security, privacy);
7. actors with malicious intent cannot have physical access to smart device (physical security).

Smart grid security requirements—The most important security requirements that should be guaranteed in smart grid include:

1. ensuring that information is protected from disclosure to unauthorized devices or individuals (confidentiality, privacy);
2. ensuring that the accuracy, trustworthiness and consistency of information is maintained throughout the life cycle of a message (integrity);
3. access to information is limited to authorized devices and users only (authenticity, authorization);
4. devices should be able to verify the source of a message, and that the message is in the same condition as it was sent (message authenticity);
5. ensuring that authorized devices or persons are able to access information or service when needed (availability, reliability);
6. ensuring that no party can deny participating in the transfer of a message (NR, accountability);
7. no data are changed or deleted by unauthorized entities (integrity, accountability);
8. ensuring that any attempt to tamper with a smart device is detected (physical security, accountability);
9. ensuring that all sensitive smart grid devices are physically secured (physical security).

Smart city security requirements—The most important security requirements for smart city include:

1. ensuring that no authorized users or devices are denied access to any smart city service (availability, reliability);
2. ensuring that access to any smart city services is limited to authorized users and devices only (authenticity, authorization);
3. ensuring that the source of messages are verified, and the message is not altered (message authenticity);
4. ensuring that no information is disclosed to unauthorized users and devices (confidentiality, privacy);
5. ensuring that no party can deny participating in any transaction (NR, accountability);
6. ensuring that no part of stored data or data in transit is modified (integrity);
7. ensuring that any attempt to tamper with a smart city device is detected (physical security);
8. ensuring that all sensitive smart city devices are physically secured (physical security).

Smart transportation security requirements—The following are some of the security requirements that should be guaranteed in smart transportation:

1. data in transit should be protected such that no captured data should reveal any part of the message (confidentiality, privacy);
2. sensors on smart cars, smart trains and road/rail infrastructures should only respond to queries from authorized entities, so that no unauthorized parties are allowed to access or inject data (authenticity, authorization);
3. no transmitted or received data is allowed to be maliciously modified (integrity);
4. the origin of every message should be verified (message authenticity);
5. that the services of smart vehicles and infrastructure are always available to authorized entities (availability, reliability);
6. that no sensing devices and infrastructure are tampered with (physical security);
7. ensuring that no party can deny participating in any transaction (NR, accountability);
8. ensuring that sensitive smart transportation devices are protected physically (physical security).

Smart healthcare security requirements—The following security requirements are the most critical for smart healthcare:

1. privacy of patients should be protected such that no medical records or any sensitive data are read by any unauthorized person (confidentiality, privacy);
2. no unauthorized entities are allowed to have access to any smart medical devices or networks (authenticity, authorization);
3. no medical records or data are modified or deleted by unauthorized persons for any malicious reasons (integrity);
4. no authorized persons, such as patients or physicians are denied access to any medical device or a healthcare service (availability, reliability);
5. smart medical devices should be able to verify the source of a message, and that the message is in the same condition as it was sent (message authenticity);
6. smart medical devices are not physically accessible to unauthorized users (physical security);
7. any attempt to tamper with medical devices is detected (physical security, accountability);
8. any breach of patient confidentiality can be traced back to perpetrators (NR, accountability).

Smart manufacturing security requirements—Typical smart manufacturing security requirements include the following:

1. only unauthorized staff are allowed to have access to smart devices or networks (authenticity, authorization);
2. smart equipment and devices should be able to verify the source of a message, as well as ensure that messages are in the same condition as they were sent (message authenticity);
3. information is only accessible to authorized staff and devices (confidentiality);
4. no data on transit, or on a storage device is maliciously modified (integrity);
5. no authorized staff or devices are denied access to any smart equipment or service (availability, reliability);
6. no staff or device can deny participating in any transaction (NR, accountability);
7. no unauthorized staff or persons are allowed to physically have access to smart equipment (physical security).

Smart supply chain security requirements—The security requirements for securing smart supply chain should include:

1. ensuring that authorized entities are not denied access to any service or information (availability, reliability);
2. ensuring that no information is accessible to unauthorized entities (confidentiality, privacy);
3. making sure that no data on transit, or on a storage device is maliciously modified by any entity (integrity);
4. ensuring that unauthorized entities are not allowed to have access to any service, and that authorized entities are restricted only to what they are permitted to access (authenticity, authorization);
5. ensuring that no entity can deny participating in any transaction (NR, accountability);
6. making sure that message came from the stated sender, and it has not been modified along the line (message authenticity);
7. ensuring that both exterior and interior perimeters of smart supply chain facilities are physically secured (physical security).

Smart wearables security requirements—The security requirements needed to secure Smart wearables include ensuring that:

1. the privacy of users is protected such that no sensitive personal information are viewed by any unauthorized entity (confidentiality, privacy);
2. no unauthorized entities are allowed to access any resource on smart wearable devices or networks (authenticity, authorization);
3. an authorized user is not denied access to any device or service (availability, reliability);
4. accuracy, trustworthiness and consistency of data in transit is maintained throughout the life cycle of a message (integrity);
5. message came from the claimed sender, and has not been changed (message authenticity).;
6. smart wearable devices are not physically accessible to unauthorized users (physical security).

Smart agriculture security requirements—The following security requirements are critical to secure smart farming and agribusinesses:

1. no unauthorized entities are allowed to have access to any farm computers or automated machineries (authentication, authorization);
2. there is no disclosure of information to unauthorized parties (confidentiality);
3. farm sensors should be able to verify the origin and credibility of every message (message authenticity);
4. no part of data in transit is altered or modified (integrity);
5. authorized farm devices and equipment can access data when needed (availability, reliability);
6. any attempt to tamper with a smart device or equipment is detected (physical security, accountability).

4.2 | System models, threat models and protocols/technologies per domain

System models, threat models, and protocols/technologies are the essential components needed to describe the security status of a system and the associated threats, which can help IoT designers, developers and administrators to identify and deal with threats in the IoT. The following subsections present in detail the description of the system models, threat models, and protocols/technologies for each of the 9 application domains.

4.2.1 | System models

A system model is the conceptual model that represents a system and provides the overall description of the functionality or behavior of a system. Abstraction is one of the fundamental concepts in system modeling, which involves hiding certain underlying details in order to focus on the essential features of the system. While there are many other modeling techniques,[111,112] we present the system models using simple diagrams (Figure 4) to show clearly the interactions between system components, between actors and a system, as well as the interactions between a system and its environment. This will allow accurate characterization of the systems with respect to their associated security risks and threats.

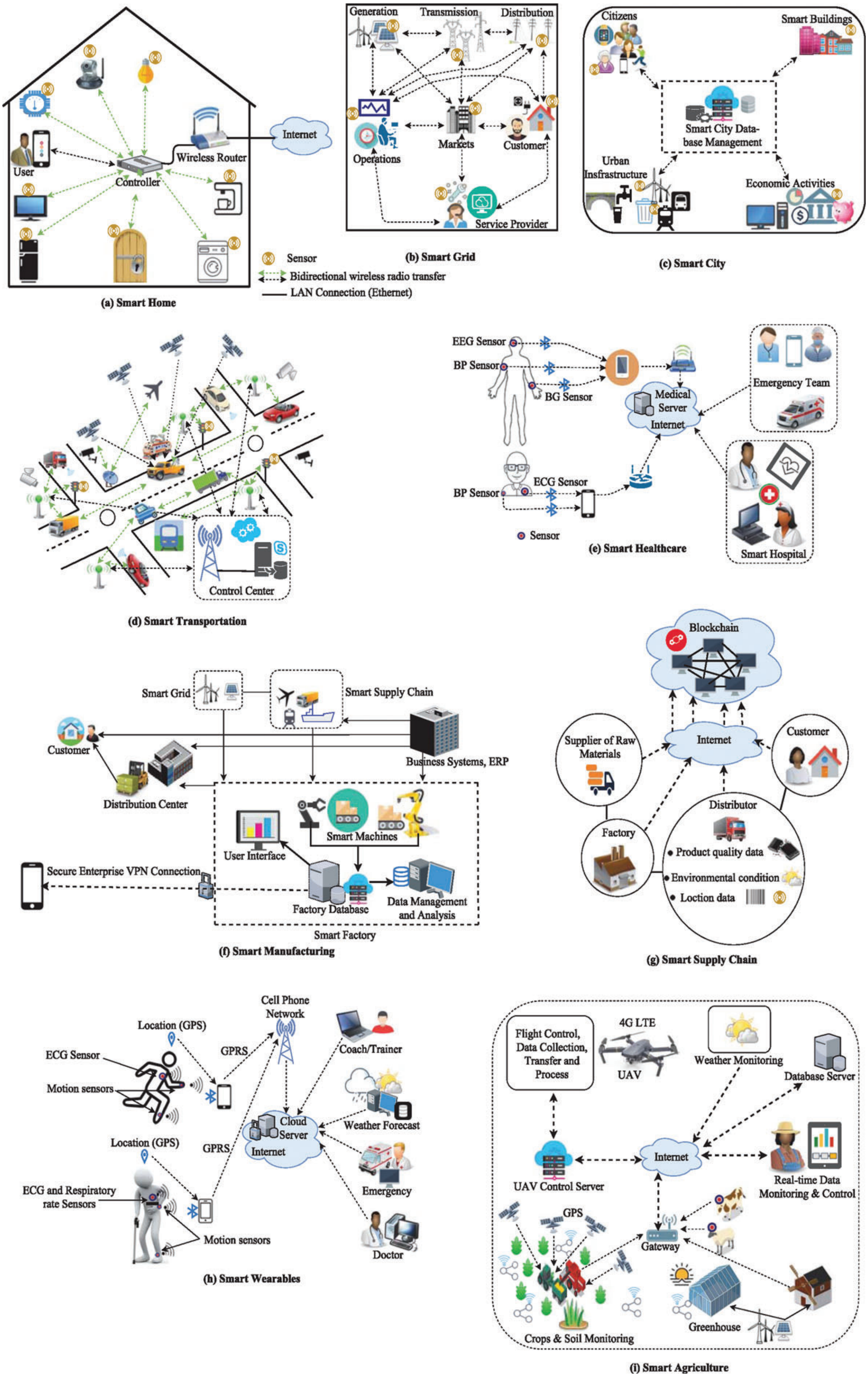
Smart home system model—The system model in Figure 4a comprised of a controller, which can be any IoT home automation hub, a wireless router, and 8 Wi-Fi enabled smart home appliances that can interface with a home automation software platform such as OpenHAB and Home Assistant. The software platform allows a user to wirelessly control devices from a smartphone or any computer on the home network. The controller is connected to the home network via the router Ethernet interface. A Raspberry Pi Single-Board Computer (SBC) can also be configured as the controller. The messaging protocol often employed for communication between the home automation software platform server and the smart devices is the MQTT. A typical lightweight server that implements the MQTT protocol is the Eclipse mosquitto.

Smart grid system model—The proposed system model in Figure 4b decomposes the smart grid system into its various subsystems, showing physical/logical relationships between the various components and the necessary information flow among them. The figure illustrates a use case of a typical smart grid that generates electricity using solar and wind renewable technologies. The different components are generation, transmission, distribution, operations, service provider, and customer; and it is assumed that these components interact with each other using a number of communication protocols that will be discussed in the last subsection. Real-time remote management and control can be achieved using the operations subsystem via the network.

Smart city system model—A typical smart city is usually made up of many components, however, in the proposed system model, we assume only 5 components, namely, citizens, smart buildings, urban infrastructure, economic activities and smart city database management, as depicted in Figure 4c. Each of these components is composed of many subsystems, and it is assumed that these subsystems interact seamlessly, allowing for a smooth flow of information between the various components. For example, a few subsystems in the economic activities component include smart banking system, smart manufacturing and smart supply chain.

Smart transportation system model—The proposed system model shows a robust transportation system that exploits seamless information coordination and exchange across the different components of the network to provide an efficient and safe transportation. The system components include smart traffic lights, cameras, radar, GPS, smart vehicle, smart trains, and smart road infrastructure, as illustrated in Figure 4d. The system utilizes real-time GPS location data, traffic flow prediction mechanism, location-based services, smart traffic light scheduling management, and enormous amount of sensor data collected from different areas in the network for making final decisions.

Smart healthcare system model—Figure 4e shows a typical smart healthcare monitoring system. The proposed system model consists of 2 outpatients, a smart hospital, and an emergency team. The 2 outpatients are: a typical patient wearing Electroencephalography (EEG) sensor, Blood Pressure (BP) sensor and Blood Glucose (BG) sensor, and an elderly patient that needs constant monitoring, wearing Electrocardiogram (ECG) sensor and BP sensor. The sensors on the patients bodies continuously collect and send data to their smartphones via Bluetooth, and the smartphones in turn upload the data to the medical server via the Internet. In case patients are in critical condition, these sensors can immediately report the physical condition of the patient to the emergency team and to their doctors for appropriate actions to be taken.



User
Controller
Wireless Router
Internet
Sensor
Bidirectional wireless radio transfer
LAN Connection (Ethernet)

(a) Smart Home

(b) Smart Grid

(c) Smart City

(d) Smart Transportation

(e) Smart Healthcare

(f) Smart Manufacturing

(g) Smart Supply Chain

(h) Smart Wearables

(i) Smart Agriculture

FIGURE 4 Typical system models for the 9 application domains

Smart manufacturing system model—As manufacturing industries strive to meet and adapt to the dynamic customer requirements in the current industrial transformation (Industry 4.0), we proposed a system model represented in Figure 4f. It is comprised of smart factory with its various subsystems, distribution center, renewable energy sources, business systems and their associated process management tools like the Enterprise Resource Planning (ERP) software, smart supply chain, customer, and secure enterprise Virtual Private Network (VPN) connection that allows remote workers to securely connect to corporate networks. Sensor data and manufacturing operations across these interconnected manufacturing components can be utilized in order to achieve better business objectives. This represents a paradigm shift from centralized manufacturing towards a more decentralized production empowered by sensor data-gathering, IoT, CPS, and analytic capabilities, where information from a variety of sources and locations can be leveraged to enhance production and services.

Smart supply chain system model—In Figure 4g we proposed a system model for smart supply chain based on Blockchain comprising production and distribution systems of geographically dispersed enterprises that collaborate in a secure manner to jointly and efficiently produce and deliver end products to customers. In the context of supply chain, IoT security issues will typically revolve around authentication, connection and transaction. However, using the distributed ledger in Blockchain, the enterprises, namely, supplier of raw materials, factory, and distributor can conduct business transactions in a trusted and secure environment. The immutable record of Blockchain enables reliable creation of networks histories, allowing for tracking the actions of network devices.

Smart wearables system model—The proposed smart wearable system model shown in Figure 4h is made up of different components, including an athlete, an elderly outpatient, a coach, an emergency team, a doctor, and a weather forecast server. The athlete is wearing ECG sensor and motion sensors, and the elderly patient is wearing ECG sensor, respiratory rate sensor, and motion sensors. These sensors collect and send data to the smartphones via Bluetooth on regular basis, and the smartphones upload the data to a cloud server via cell phone network. The coach can only access information pertaining to the progress of the athlete; similarly, the doctor can only access information pertaining to the health of his patient. However, in case of emergency condition, the emergency team and the doctor will receive an urgent message from the ECG sensor on the athlete, or from the ECG sensor and/or respiratory rate sensor on the patient.

Smart agriculture system model—Figure 4i shows a diagram representing the proposed smart agriculture system model. Plants normally require specific environmental conditions for optimal growth, health and overall crop yield. Thus, the system model consists of different sensor networks for measuring soil moisture, temperature, sun light, humidity, as well as sensor networks for monitoring the location of farm animals, and for prompt disease detection. Onboard the UAV are a SBC, a flight control system (autopilot) like Pixhawk, sensor and camera. The sensor is used to collect real-time data from the flight control system every second and sent to a server via 4G LTE dongle attached to the SBC. The autopilot can also receive commands through the server, hence by connecting to the server via the Internet, the farmer can control the drone by viewing the real-time data and issuing control commands.

4.2.2 | Threat models

A threat is a person, object, or other entity capable of exploiting a vulnerability to breach security in order to cause a possible danger to an asset. Threat modeling is a process of optimizing network security by identifying potential threats to vulnerable assets and services in order to define countermeasures that can capture the characteristics of the behavior of adversaries.

This paper presents the threat models based on different possible attack scenarios for each application domain. A threat can cause different levels of negative impacts to an IoT system. We classify threat impact into 3 levels: high, medium and low threat levels. According to this classification, a high threat can potentially cause total destruction or corruption of an asset in any layer of the IoT architecture; a medium threat is capable of causing partial destruction of asset or denial of service; and a low threat level can cause disclosure of information or eavesdropping.

Smart home threat model—Threats in smart home usually originate from outside the network. The adversarial sources may include, but are not limited to criminal groups, phishers, hackers, bot-network operators, spyware authors, and malware authors. An adversary can exploit a compromised device like smart TV[113] to eavesdrop on smart home residents (low threat). Similarly, an attacker can interrupt a Bluetooth pairing communication between 2 smart home devices and masquerade himself as the real receiver or sender in order to carry out further attacks (medium threat). Furthermore, a knowledgeable adversary can leverage the fact that firmware updates for most smart home devices are usually not digitally signed and can be accessed from Trivial File Transfer Protocol (TFTP) server. As such, the attacker can redirect a smart home device to a nefarious TFTP server using Address Resolution Protocol (ARP) spoofing, or Man-in-the-Middle (MitM) attack to take control of a device or the whole network (high threat). Attackers can also exploit security vulnerabilities that exist in some smart home devices and intrude into smart home networks and launch attacks, such as DoS and MitM (medium threat). Moreover, an attacker can physically attack or tamper with a smart home device, thereby compromising the security mechanisms of the device (high threat).

Smart grid threat model—Smart grid threats may arise from both within and outside the smart grid network. The adversarial sources may comprise disgruntled employees, disgruntled customers, hackers, criminal groups, bot-network operators, malware authors, and spyware authors. Malicious parties can eavesdrop on communication traffic between a smart meter and a central system, or try to analyze data in transit so as to deduce information from communication patterns (low threat). Intruders can as well compromise a smart meter using IP spoofing, and then use MitM attacks and falsify the billing report (medium threat). Similarly, intruders can illegally install some monitoring software on a smart meter,[114] or any computer within their reach that will enable them to sniff off or steal critical information about a consumer or a utility provider, such as usernames, passwords, and so on (medium threat). Attackers can also tamper with a stored data by modifying or deleting part or all of the data, which may affect the operation of some key devices, such as transformers and circuit breakers (high threat). Additionally, intruders can logically capture a smart meter and change the firmware, which will give them the opportunity to gain control over the device. Moreover, an attacker can physically attack a smart grid installation, such as substation or transformer, and change some configurations, make wrong connections, or even vandalized it (high threat).

Smart city threat model—Smart city threats may originate from within and outside the smart city network. Smart city adversaries can include hackers, hostile governments, terrorist groups, disgruntle customers, criminal groups, disgruntled employees, spyware authors, malware authors, bot-network operators, and spammers. Attackers can disrupt communication signal of autonomous vehicles, which can pose a potential threat to public safety (high threat). Attackers can also target smart grid network in a smart city in order to cause disruption of power supply to customers (high threat). Adversaries can gain remote access to a smart waste-water treatment plant or a smart water facility and cause environmental damages, or cause water shortages, which can create public health crises (high threat). Additionally, malicious actors can target smart street lighting system and cause electrical blackouts (medium threat).

Smart transportation threat model—Threats may come from both within and outside the smart transportation network. The adversarial sources may include, but not limited to criminal groups, terrorist groups, hostile governments, disgruntled employees, hackers, bot-network operators, malware authors and spammers. An adversary can decide to compromise the Anti-lock Brake System (ABS) of a smart car by attacking the controller area networks of the car using DoS, spoofing, or any other type of cyber attacks, which may result in car accidents (high threat). An attacker can also launch DoS attacks on a critical infrastructure, spamming it with useless messages in order to exhaust the available bandwidth so as to prevent sensors on the infrastructure from obtaining important environmental information, such as data on traffic, proximity, signaling, and speed, which may have implications on safety (high threat). The adversary can equally create the same effects by infecting critical transportation networks with malicious software. Moreover, since GPS is critical to the smooth operations of autonomous cars, a malicious person can install a GPS jammer on an autonomous car or on any car that can move in close proximity to it in order to disrupt the performance of the in-car GPS receiver. This will result in misleading the autonomous car (medium threat). Furthermore, since autonomous cars can be considered to be Multi-agent System (MAS),[115] where critical tasks like negotiating corners and stopping the car are at the mercy of MAS, an attacker can take control of an autonomous car by capturing its MAS (high threat).

Smart healthcare threat model—Threats in smart healthcare may come from both within and outside the network. Adversaries may include, but not limited to hackers, disgruntled employees, spyware authors, malware authors, bot-network operators, spammers, and criminal groups. Adversaries can compromise a smart healthcare system by exploiting a vulnerability in order to gain access into the network and carry out a variety of attacks. The attackers can eavesdrop on a communication between a physician and a patient (low threat); they can also launch a DoS attack on the communication network (medium threat); or capture/hijack a critical medical device (high threat).

Smart manufacturing threat model—As all aspects of modern manufacturing are becoming smarter, moving from closed systems into Industry 4.0-based manufacturing driven by IP-based IoT and CPS, industrial plants and businesses are being exposed to numerous cyber threats. Security threats in this domain may originate from outside and within the smart manufacturing. Adversaries may include business competitors, industrial spies, disgruntled employees, innocent employees, criminal groups, hostile governments, malware authors, spyware authors and hackers. Adversaries can compromise a smart device and gain access to a critical application, they can remotely alter or corrupt a manufacturing process, maliciously manipulate machines to produce undesirable results, or they can cause disruption or denial of process controls (high threat). Adversaries can target databases for the purpose of stealing intellectual property and industrial espionage (medium threat). Additionally, Bring Your Own Device (BYOD) also offers attackers the opportunities to target smart industries through their employees (medium threat).

Smart supply chain threat model—Cyber threats in smart supply chain can come from different threat actors with varying motivations. Adversaries may include criminal groups, third-party suppliers, chip makers, business competitors, industrial spies, disgruntled or rogue employees, innocent employees, hostile governments, malware authors, and hackers. Since data is a key driver of cyber crime, persons with malicious intent may access data through third-party organizations and compromise smart supply chain and cause different levels of damages (medium threat). They can also leverage the lack of proper authorization, accountability, and authentication in the cloud to gain access to targeted networks and, ultimately, their data. The data may include sensitive information like customer contracts, credit card information and other valuable data (high threat). Adversaries can inject malware in smart supply chain applications that can steal personal information, as well as allow for complete remote control of devices (high threat). In addition, innocent employees can, unintentionally, jeopardize supply chains as a result of negligence, or simple human errors (medium threat).

Smart wearables threat model—The growth of wearable technology and the increasing number of users of smart wearable devices pose a series of security threats that open the doors for cybercriminals to target organizations and individuals via IoT devices, such as smart watches, smart headgears, fitness trackers, and smart clothing/accessories. Security threats in this domain usually originate from outside, however, disgruntled employees and innocent employees that use such devices may also constitute potential threats to an organization. Adversarial sources may include criminal groups, hackers, business competitors, industrial spies, disgruntled employees, innocent employees, and malware authors. Malicious entities can easily access sensitive data from a company if they compromise communication links between smart wearable devices and a mobile device of an employee that in turn has access to the corporate network (medium threat). They can also compromise cloud-based data centers and access sensitive financial and customer information (high threat). Adversaries can use a malware infected wearable device to infect other data sources, or create back doors for malicious purposes (high threat). They can also intercept and manipulate data transmitted to or from wearable devices (low threat).

Smart agriculture threat model—In smart farming, threats may likely originate from outside the network. Adversaries may include industrial spies, terrorist groups, criminal groups, hostile governments, hackers and spyware authors. An adversary can attack an automated fertilization system and change the percentage of chemical agents in order to produce toxic materials that will be very harmful for the crops (high threat). Additionally, attackers can create the same effects by maliciously interchanging chemical agent A for agent B. An attacker can also infiltrate a sensor network of a greenhouse and compromise the sensors so as to report false data on important information, such as temperature or soil moisture, which will have negative effects on the greenhouse (high threat). Attackers can also disrupt GPS communication using GPS jammers, which will result in disruption of the operations of satellite-guided tractors (high threat). Since smart farm-management rely on different sensor information and analysis of past crop yields to produce planting and business plans, people with malicious intention can eavesdrop data over the wireless communication channel and steal some important farming or business secrets (medium threat).

4.2.3 | Protocols and technologies

In a network, devices need to speak the same language and agree on a set of rules to be able to exchange information with each other. This set of rules is also known as protocol in the computer networking world. Protocols specify how signals are sent from one device to another, or multiple devices, in order to trigger a desired behavior.[116] In the IoT, diverse entities communicate over the network using different set of protocols and standards, some of which are depicted in Figure 1 above. Based on their transmission range, IoT communication protocols can be classified into 2 main categories, namely, short-range and long-range. Examples of protocols in each category are already given in the previous section. Although there are several application protocols for the IoT as shown in Figure 1, for the purpose of describing the protocols, we employ the CoAP in all application domains as the application protocol, as shown in Figure 5. In the same vein, we use the Datagram Transport Layer Security (DTLS) as the security protocol in all application domains.

Smart home protocols and technologies—A Home Area Network (HAN)[117] is a type of computer network that operates within a small area, such as a home or small office, and hence it is a critical enabling technology for smart homes. As a physical layer of a home-based network, HAN is used to connect devices within the close vicinity of a smart home. HAN is also used to manage communication between the smart meter and other smart devices for smart home energy management.[118] Preferred protocols and technologies for HAN have evolved over the years to provide seamless and secure communication among devices. They include ZigBee, Z-Wave,[119] Wi-Fi/Low Power, Thread, BLE[120,121] (wireless technologies), PLC (wired technology), and Ethernet. Typical examples of application and security protocols used in smart homes are CoAP[122] and DTLS, respectively, as shown in Figure 5. A brief description of each protocol or standard is given below. Table 3 also provides a comparison of some important parameters of different short-range communication technologies for IoT.[123,124]

- *ZigBee*: Is a low-power wireless technology that operates in a mesh network, meaning that it uses a device to relay a signal to other devices, thereby expanding the network. It is based on the IEEE 802.15.4 standard for Personal Area Network (PAN) and operates in the 2.4 GHz Industrial, Scientific, and Medical (ISM) band. The application focus of ZigBee includes sensor monitoring and control.[124]
- *Z-Wave*: Similar to ZigBee, Z-Wave is a low-power wireless communication protocol that can be used for remote control applications in homes and industries.[125] However, Z-Wave is about 6 times slower, but consumes less energy to cover the same distance as ZigBee.
- *Wi-Fi*: Is any wireless networking technology that is based on the IEEE 802.11 standards. It provides highspeed Internet and network connections, and operates in the 2.4 and 5 GHz bands. Additionally, Wi-Fi has less implementation complexity. The

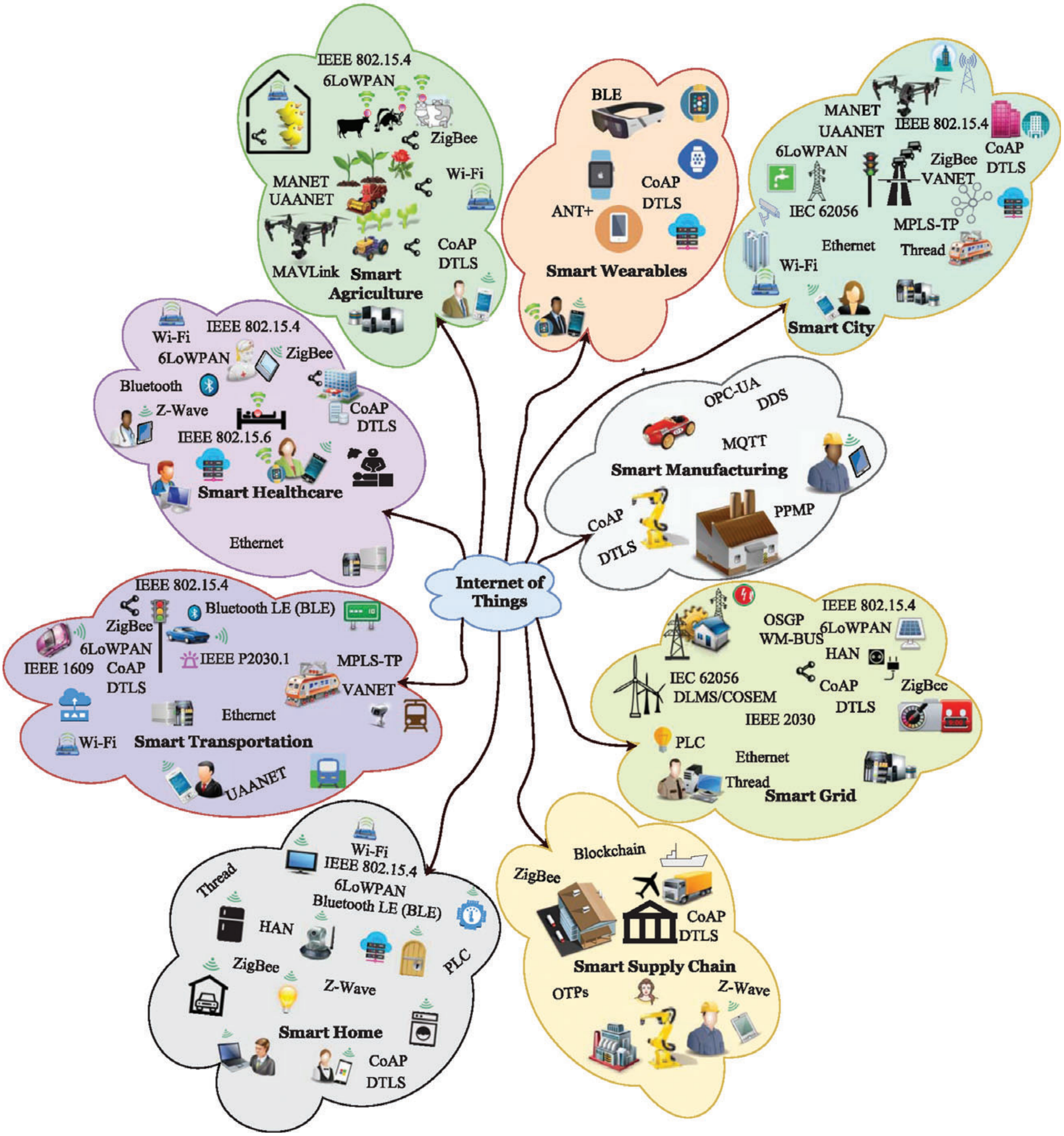


FIGURE 5 IoT protocols and technologies for 9 application domains

newer Wi-Fi technologies are the 802.11n and 802.11ac standards ratified in 2009 and 2013, respectively. While the 802.11n introduced the optional use of the 5 Gb/s, the 802.11ac enhanced the speed of data transfers, such that data rate of up to 1 Gb/s is attainable.[124]

- *Thread*: First introduced in July 2014, Thread is a wireless networking protocol that supports a variety of IoT devices.[124] Unlike ZigBee and Z-Wave that are not IP-based, Thread is based on the IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) wireless technology, and hence natively handles IPv6 address standard, however, it does not handles IPv4 Internet address standard. Like ZigBee, it is also based on the IEEE 802.15.4 standard.
- *BLE*: Is a short-range wireless protocol based on the IEEE 802.15.1 and used for data sharing among devices. It significantly reduces power consumption of devices, potentially allowing for longer battery life.[126]
- *PLC*: Refers to a communication technology that enables the use of existing electrical power cables for transmitting and receiving information. Over the years, PLC has proved to be a viable technology for HAN applications due its low cost installations and broad coverage. Today, it is used for remote meter reading and other home automation.[117]

TABLE 3 Comparison of different short-range communication technologies for IoT

	Technology					
Parameter	**ZigBee**	**Z-Wave**	**Wi-Fi**	**Thread**	**Bluetooth LE**	**PLC**
Nominal range	100 m	30 m	150 m	30 m	10 m	10-10,000 m
Data rate	250 kbps	40-100 kbps	54 Mbps-1 Gbps	250 kbps	1 Mbps	0.256-200 Mbps
Operating frequency	868/915 MHz, 2.4 GHz	908.47 MHz (US), 868.42 MHz (Europe)	2.4, 5 GHz	2.4 GHz	2.402-2.481 GHz	2-100 MHz
Number of nodes per network	65,000	232	250/access point	300	one-to-many	N/A
Peak current consumption	30 mA	17 mA	116 mA	12.3 mA	12.5 mA	N/A
Power consumption per bit	185.9 μW/bit	0.71 μW/bit	0.00525 μW/bit	11.7 μW/bit	0.153 μW/bit	N/A
Power consumption	3.3 μW-63 mW	∼5 mW	31.6-100 mW	∼10 mW	1-10 mW	N/A
Security	128-bit AES	128-bit AES	WPA2 - AES	128-bit AES	128-bit AES	N/A
Network topology	Star, cluster, mesh	Mesh	Star, mesh	Mesh	Point-to-point, mesh	Star, mesh
IEEE standard	802.15.4	N/A	802.11n, 802.11ac	802.15.4	802.15.1	1901-2010

- *Ethernet*: Is the most widely used Local Area Network (LAN) technology that describes how devices can be networked for data sharing using cables. Ethernet is specified in the IEEE 802.3 family of standards.
- *CoAP*: Is an application layer protocol that allows constrained devices of the IoT to interact in an IP-based HTTP-like manner with little or no overhead. CoAP is based on User Datagram Protocol (UDP)/IP in order to enable low-power devices to use RESTful services while meeting the energy constraints requirements.[127]
- *DTLS*: Is a form of Transport Layer Security (TLS) designed to provide security for applications and services that are built on top of UDP.[128] Such applications like IoT are usually delay-sensitive.

Smart grid protocols and technologies—As shown in Figure 5, a smart grid consists of a suite of technologies that improve reliability, controllability and performance of the electrical grid. There exist a variety of protocols and standards for smart grid applications, including Device Language Message Specification/Companion Specification for Energy Metering (DLMS/COSEM)[129,130]; International Electrotechnical Commission (IEC) 62056 standards[131]; the Open Smart Grid Protocol (OSGP)[132]; Wireless Metering Bus (WM-Bus)[133]; IEEE 2030; 6LoWPAN; ZigBee; Z-Wave; Thread; PLC; CoAP, DTLS and Ethernet. Below we briefly describe the smart grid protocols and standards:

- *DLMS/COSEM* is the specification that describes communication protocols and an interface model for data communication with metering equipment.
- *IEC 62056* is a set of standards for electricity metering data exchange that represents the international versions of the DLMS/COSEM standards.
- *OSGP* is a power-line communication protocol for smart meters, published by the European Telecommunications Standards Institute (ETSI). It defines a high-performance narrow band communication channel for data exchange between Smart meters and the data concentrator.
- *WM-Bus* is a wireless protocol for smart metering that specifies communication between utility meters and concentrators, smart meter gateways and data loggers. The protocol is widely used across Europe.
- *IEEE 2030* specifies how interoperability can be achieved in smart grid.
- *6LoWPAN* is a low-power adaptation layer protocol that allows wireless transmission of IPv6 packets over the IEEE 802.15.4 networks. It allows constrained wearable sensors used for health monitoring of patients to connect to the Internet using IPv6.

Smart city protocols and technologies—Smart city protocols have advanced over the years to ensure happier, efficient and safer life for citizens. They include: 6LoWPAN, Mobile Ad hoc Network (MANET),[134] Unmanned Ariel Vehicle Ad hoc Network (UAANET),[135] Vehicular Ad hoc Network (VANET), IEC 62056,[131] Multiprotocol Label Switching-Transport Profile (MPLS-TP),[136,137] Ethernet, ZigBee and other protocols within the IEEE 802.15.4 standard, CoAP, DTLS, and Wi-Fi, as depicted in Figure 5. A brief description of some of the protocols or standards are given below.

- *MANET* is a temporary and dynamic network that configures itself on the fly without the aid of any centralized administration or standard support services.
- *UAANET* is a variant of MANET for unmanned aerial vehicles (UAVs) and Ground Control Stations (GCS). Through collaboration, it enables relaying data among UAVs and between UAVs and GCS.

- *MPLS-TP* is a type of MPLS protocols (used in packet switched data networks for speeding up network traffic flow) defined by Internet Engineering Task Force (IETF). Being a simplified version for transport networks, non-relevant functions have been turned off.
- *VANET* is a form of MANET that enables vehicles to communicate with each other, vehicle-to-vehicle (V2V), and with roadside equipment over the Internet, Vehicle-to-Infrastructure (V2I).

Smart transportation protocols and technologies—As depicted in Figure 5, typical examples of smart transportation standards and protocols include IEEE P2030.1,[138] IEEE 1609,[139] VANET, UAANET, 6LoWPAN, ZigBee and other protocols within the IEEE 802.15.4 standard, Bluetooth LE (BLE), MPLS-TP, Wi-Fi,[140] CoAP, DTLS, and Ethernet. Some of the protocols are briefly described below:

- *IEEE P2030.1* is the standard that specifies the electrification of the transportation infrastructure.
- *IEEE 1609* is a set of standards for Wireless Access in Vehicular Environments (WAVE) that specifies an architecture, as well as a set of services and interfaces that will allow secure V2V and V2I wireless communications.

Smart healthcare protocols and technologies—The protocols and standards that govern smart healthcare include IEEE 802.15.6,[141] Wi-Fi, BLE,[142] 6LoWPAN, ZigBee,[143] Z-Wave,[144] Ethernet, CoAP[145] and DTLS, as shown in Figure 5. The following are brief descriptions of some of the protocols or standards:

- *IEEE 802.15.6* is a radio communication standard for WBANs. The protocol supports a wide range of applications for short-range, low-power, and reliable communication that can provide real-time diagnosing and health monitoring of patients and the elderly. WBANs operate on the surface or inside the human body.[146]

Smart manufacturing protocols and technologies—The communication protocols and standards used in smart manufacturing include the Open Platform Communications-Unified Architecture (OPC-UA), DDS, MQTT, and Production Performance Management Protocol (PPMP),[147] as shown in Figure 5.

- *OPC-UA* is a M2M communication protocol for industrial manufacturing based on client-server model, which is not limited to a specific data encoding. It provides a very good scalability in data modeling. OPC-UA has been widely implemented in various domains such as smart grids and building automation.[148]
- *DDS* is a real-time publish/subscribe M2M communication technology for efficient,[149] ubiquitous and secure data sharing introduced in 2004 by the Object Management Group (OMG). The absence of brokers and servers in this standard, also known as middleware, simplifies deployment, maximizes scalability, increases reliability, reduces complexity and cost, as well as minimizes latency. DDS has been applied in many application areas like smart grid management and air-traffic control.
- *MQTT* is a low power communication protocol for constrained devices, and arguably the most widely used protocol in the IoT application layer. It is also based on the publish/subscribe model, however, devices do not communicate directly with each other. They publish messages on a broker based on topics, and clients interested in such topics can retrieve the messages by signing in to the broker.[150]
- *PPMP* is a protocol proposed by Bosch, which specifies a format for capturing data needed for the monitoring of production process and data analytics.[147] The protocol facilitates communication between machines and sensors, and Industry 4.0 software solutions. PPMP is easy to implement in a plant by users, and it can be freely used without licence fees.

Smart supply chain protocols and technologies—A promising driving technology for smart supply chain is the Blockchain, a transparent and secure technology with decentralized operations. Blockchain has innovative possibilities that can be used to automate various business processes.[94,151] Considering the different technologies involved in smart supply chain, there will be many protocols and standards, including the tradition IPs, IoT protocols, and RFID protocols like the Ownership Transfer Protocols (OTPs), as depicted in Figure 5.

- *Blockchain* is a distributed ledger technology, an encrypted and shared database that serves as an incorruptible and irreversible repository of information, providing trust without the need for any trusted third party.[152] It is the technology underlying Bitcoin. Applications of Blockchain in smart supply chain include automating purchase processes, security, and executing smart contracts.[153]
- *OTPs* are security and privacy protocols that allow the secure and seamless transfer of ownership of RFID-tagged objects from a current owner to a new owner.[154,155] In a supply chain, change of ownership usually occurs when a distributor delivers tagged products to a retailer. Hence, 3 entities are involved, the original owner, the new owner, and the tag.[156]

Smart wearables protocols and technologies—The most common technologies that allow smart wearable devices to transfer data to other devices, and to talk to each other are BLE and ANT+, as shown in Figure 5. Although ANT+ has a longer battery life,[157] BLE is currently the protocol of choice in the smart wearable industry because of its simplicity and low energy consumption.[158] BLE is poised to continue to play an important role in the future low-power smart wearable IoT devices. In an effort to diversify its applications, the Bluetooth Special Interest Group (SIG) has recently introduced Internet Protocol Support Profiles (IPSP), and HTTP Proxy Service (HPS) to facilitate Internet accessibility for Bluetooth smart devices through a BLE gateway.[159]

- *ANT+* is a wireless protocol that allows collecting, tracking, and transferring sensor data among devices with the ANT+ technology. It uses the 2.4 GHz license-free band, which provides high-quality communication at low-power using low-cost transceivers. ANT+ networks can be configured into peer-to-peer, star, tree, and mesh topologies.[160]

Smart agriculture protocols and technologies—Wireless connectivity is usually employed in smart agriculture using the following or other protocols, as shown in Figure 5: ZigBee[161] and other protocols within the IEEE 802.15.4 standard, 6LoWPAN, CoAP, DTLS, Wi-Fi, MANET, UAANET, and Micro Air Vehicle Communication Protocol (MAVLink).

- *MAVLink* is a very lightweight and header-only communication protocol for controlling micro aerial vehicles. The protocol is used for communication between the control station on the vehicle, also called autopilot like Pixhawk, and the GCS.[162–164]

5 | REVIEW OF SCHEMES, TECHNOLOGIES AND MECHANISMS FOR SECURING IOT

In recent years, an increasing number of researchers have been trying to address the security and privacy issues in all layers of the IoT architecture, and many different techniques and solutions have been proposed, with more emphasis on the resource-constrained devices. One of the issues that make IoT security complex is the fact that many *things* use very simple operating systems on processors that have minimal computing capacity, and small memory, making it more difficult to fulfill basic IoT security requirements. In this Section, several proposals for addressing these issues are examined. The survey of the proposed solutions is focused on 5 different aspects, namely, cryptographic primitives, authentication protocols, hardware, specific application domains, and current security mechanisms.

5.1 | Solutions based on cryptographic primitives

Key management protocols are central in securing communication among smart devices, and many researchers are working intensively in this area. Eldefrawy et al[165] propose a key distribution protocol for constrained WSNs devices. Their key agreement algorithm is based on public key cryptography, Rivest-Shamir-Adleman (RSA) and Diffie-Hellman Elliptic Curve Cryptography (DHECC), in which pair-wise keys between nodes are only established after deployment, contrary to the idea of equipping each node with full pair-wise keys. A node shares keys only with nodes within a given routing path, thereby enhancing storing efficiency and reducing the risks of node capture. The authors claimed that their scheme enhances the re-keying property of nodes and offers better scalability.

Adiga et al[166] present their own secure M2M communication scheme as a promising solution that will ensure security and privacy in the IoT. The scheme is based on Identity-Based Encryption (IBE) using elliptic curve cryptography, which requires no use of certificates. The authors employed the use of Tate Pairing schemes for encryption and decryption, which involves 4 steps, namely setup, extract (registration), encrypt and decrypt. Only public key generation center acts in the setup mode, and a party interacts with the center once during the extract phase (generation), while only concerned parties are involved in the encrypt and decrypt processes. The encryption and decryption schemes were implemented in Java and MATLAB, and performance analysis was carried out using a machine with Microsoft Windows XP professional operating system (OS) and Pentium 4 CPU, 2.80 GHz with 2 GB RAM processor, which shows that the scheme is not suitable for constrained devices.

Another key management scheme based on IBE that allows nodes with limited resources to delegate expensive computations to non-constrained proxy nodes is proposed by Papanikolaou et al in.[167] Unlike other Publickey cryptography schemes that need Public Key Infrastructure (PKI) to map keys to identities via digitally signed certificates, which incur heavy overhead in managing the certificates, in IBE, the public-key is some arbitrary string of information associated uniquely with the user, such as e-mail address, date of birth, and so on. Nonetheless, the high computational cost of IBE cannot be borne by most resource-constrained IoT devices. To overcome this problem, the authors used IBE on elliptic curve cryptography, which is supported by embedded systems with limited resources. The proposed scheme allows a constrained node to share a secret with a remote node outside the network, which is usually non-constrained, and hence can undertake extensive computations. This scheme promises to provide more secure communications among embedded devices for IoT applications.

A different scheme, combining IBE techniques with PKI is suggested by Li and Xiong in.[168] Their scheme essentially consists of a Heterogeneous Online and Offline Signcryption (HOOSC) approach to practically secure communication between WSNs and an Internet host. The authors designate sensor nodes to be senders using IBE, while the Internet host a receiver using PKI.

The HOOSC scheme uses the following algorithms: setup, IBE-KG (key generation algorithm for IBE users), PKI-KG (key generation algorithm for PKI users), Off-Signcrypt, OnSigncrypt, and Unsigncrypt. A sensor node can send a message to the host by running the Onsigncrypt algorithm, which is a light computation like exclusive OR, and the Internet host recovers the message from the ciphertext by running Unsigncrypt. In this manner, the proposed scheme reduces the computational overhead of sensor nodes. The authors claimed that their scheme provides end-to-end confidentiality, integrity, authentication, and NR services. However, security is only guaranteed when sensor nodes send message to an Internet host, and not the other way around.

Saied et al[169] propose a lightweight collaborative approach for key establishment scheme to make the existing security protocols suitable for these devices. Instead of reducing the cost of cryptographic algorithms, the proposed collaborative scheme relieves the resource constrained devices of the computational and communication overhead incurred during key exchange by assigning these burdens to the less constrained neighboring nodes, also known as proxies, which assist in carrying out the tasks. The authors argue that using this scheme, constrained nodes can save up to 35% of their energy during key transport of TLS handshake, when compared to other schemes.

Garcia-Morchon et al[170] propose 2 different security architectures based on 2 standardized IP protocols. The first architecture is based on Host Identity Protocol (HIP), while the second uses DTLS. The authors claim that these architectures will ensure that all interactions of IP-based IoT devices, including those with limited resources, are protected from cyber attacks. The proposed architectures promise to address secure network access, secure communication and key management issues associated with these IoT devices. The authors implemented these architectures in C and tested them on Cooja simulator. They were also installed on Redbee Econotag hardware running Contiki OS 2.5 (an open source OS that is used on resource-constrained IoT devices). After comparing the 2 approaches, results show that the HIP based approach performs better than the DTLS based solution in terms of memory footprint (the HIP based mechanism uses less memory), communication cost and resilience to packet loss.

Petroulakis et al[171] present a lightweight framework for ensuring security, privacy and trustworthy life-logging in smart environments. Although there is no specific or concise definition of the proposed lightweight framework in the paper, the authors used an experimental test-bed for investigating energy consumption for the secure lifelogging to describe the framework, which consists of 2 users (represented by Digi XBee Pro 802.15.4 devices) and one adversary whose aim is to overcome the security barrier on the communication between the 2 users. A radio peripheral (USRP2) with a XCBVR2450 dual-band transceiver is used as the adversary. The experiments were conducted for 3 different scenarios: when there was no encryption, with Advanced Encryption Standard (AES) encryption and with AES encryption and there are 10 dropped packets on the devices. Results reveal that there is about 15-30% increase in energy consumption when securing the communication.

Sciancalepore et al[172] suggest a Key Management Protocol (KMP) for mobile and industrial IoT devices, which is integrated at the layer-2 of the protocol stack based on IEEE 802.15.4 technology. The authors leverage the fact that Elliptic Curve Qu-Vanstone (ECQV) can be used to generate lightweight implicit certificates. They also exploit the secret sharing mechanism of Elliptic Curve Diffie Hellman (ECDH) to develop the KMP algorithm, such that ECQV and ECDH collectively provide the needed authentication and key agreement services. The proposed scheme was implemented on a platform that is based on TelosB, and results show that the scheme provides fast re-keying, protection against replay attacks, robust key negotiation and lightweight node authentication.

5.2 | Solutions based on authentication and access control protocols

Authentication and access control play essential roles in ensuring security and privacy of IoT devices. Authentication prevents unauthorized entities from gaining access to assets by assuring that the communicating entities are the ones they claim to be, while access control prevents unauthorized use of a resource. Designing and implementing authentication and access control for constrained devices is a serious research challenge facing the IoT research community, and thus there are several works on this subject. For example, Liu et al[173] propose an authentication and access control protocol for IoT using Public Key Cryptography (PKC). The authors employed the use of Elliptic Curve Cryptography (ECC) for key establishment between 2 entities, which happens in 3 steps. They adopted Role-Based Access Control (RBAC) for access control policy. The authors suggest that handling of enormous resources can be achieved by preregistration on nearby trustworthy access point called Registration Authority (RA). Also, all users are registered using the Home Registration Authority (HRA). The proposed protocol uses a 7-step procedure for accessing a *thing*, which involves the entities: User, *thing*, RA and HRA. Since central authentication is possible using OpenID technology, where users with a single account are allowed to log on to several sites by authenticating only one identity provider, the authors used the OpenID for authenticating users. The authors carried out a security analysis, and their results show that the proposed approach can provide protection against eavesdropping, MitM, key control and replay attacks.

Some improvements to the protocol proposed by Liu et al are suggested by Ndibanje et al.[174] The authors carried out a cryptanalysis of the protocol, where they discovered that the scheme proposed by Liu et al is vulnerable to compromised device attacks and replay attacks. Additionally, they found that message exchange in that protocol incurs unnecessary overhead. In the quest to solve these problems, they propose some improvements based on 5 assumptions. They categorized the improvements into 2 phases, namely registration and authentication. Registration phase: in order for users and gateway nodes to share the secret key for authentication, initial registration with HRA server is a prerequisite for users, but the RA functions as in the scheme of Liu et al. The authentication is further divided into 2 phases, namely login phase and verification phase. The login phase is used to access IoT network, while the verification phase is used to authenticate a user. The authors also included an additional function that allows for password change or recovery. After analyzing the enhanced protocol, results show that it satisfies the primary security goals in the IoT, and also reduces the cost of communication.

Another authentication and access control scheme that is based on CoAP is presented by Pereira et al.[175] The proposed framework for CoAP-based IoT leverages the advantages of Kerberos and Remote Authentication Dial In User Service (RADIUS) schemes to come up with a new proposal that can provide fine-grained and energy efficient Authentication, Access control and Accounting (AAA) solution for resource-starved IoT devices on a per service basis. The authentication and access control process comprises 2 steps. Authentication is the first step, which involves determining the legitimacy of a user. The CoAP-Network-attached Storage (NAS) checks information about a user in terms of permissions, group, ticket time out, etc., and the CoAP-NAS sends a valid ticket if the user is successfully authenticated. Access control is the second step, in which a valid ticket accompanies every client request specifying the access rights of a user, and the server responds with an error message to any client request without a valid ticket. The proposed access control mechanism was tested on many services with diverse permission types, and results show that the scheme responds to requests according to clients permissions.

Jan et al[176] suggest an alternative approach, which is a lightweight mutual authentication scheme that verifies the identities of the devices (clients and servers) that are to take part in communication for resource observation in a CoAP-based IoT environment; the scheme also allows the verified clients to have access to various resources based on their respective requests. The authors clearly pointed out that their scheme is basically an enhancement of the security features of the CoAP protocol in order to make it more robust, efficient, and able to defend against a number of threats. Hence they suggest a robust, easy to implement and less computationally expensive authentication algorithm as an alternative to the DTLS. The proposed authentication process uses 4 handshake messages and incurs less than 1024 bits as connection cost, and it completes using the 128-bit AES. Although the proposed scheme is able to defend against eavesdropping, key fabrication, resource exhaustion and DoS attacks, the authors acknowledge that the scheme is not an effective solution against Sybil attacks. They further highlighted some other threats that have not yet been explored in an IoT domain, which include wormhole, sinkhole and selective forwarding.

Kothmayr et al[177] present a 2-way authentication architecture for IoT that is based on the DTLS protocol. Their security scheme, which is based on RSA, works on top of the UDP/IP networking technology for 6LoWPAN. In this scheme, authentication is carried out during verified DTLS handshake that is based on exchange of certificates containing RSA keys. As a proof of concept, the authors implemented the architecture on a constrained device, and results show that with minimum energy consumption, the proposed scheme provides integrity, confidentiality and authenticity.

Turkanović et al[178] propose a user authentication and key agreement scheme for heterogeneous ad hoc WSNs for IoT applications. The proposed scheme allows a user to securely access a particular node of interest from a WSN without directly going through the gateway node by using a rare 4-step authentication model. There is also a provision for a user to dynamically increase the number of sensor nodes he can access. The authors use a lightweight key agreement protocol in order to ensure mutual authentication between participating entities (user, sensor node and gateway node). In order to ensure that the scheme is suitable for a resource constrained device in the IoT, the authors avoided the use of expensive computations by using simple hash and Exclusive-OR (XOR) computations instead. After 2 phases of registration, a user logs in using a smart card, and for the authentication, the user sends authentication message directly to a sensor node of interest, and a secure communication can start after a successful session key negotiation. Results of the security evaluation show that the proposed scheme can protect against replay, privileged-insider, stolen verifier, stolen smart card and smart card breach, impersonation and many logged-in users with the same login-ID attacks.

A different idea is introduced by Lee et al ,[179] who propose a lightweight authentication protocol for RFID in the IoT. Although their paper does not clearly explain their architecture, the authors argue that their method, based on XOR manipulation can replace complex encryption process based on hash functions. The authors run the operation procedure of the proposed protocol on a finite state machine they built, and based on the simulation results, they claimed that mutual authentication for RFID in IoT is achievable using their proposed protocol.

Considering the significant growth of wearable IoT devices and the new trends in electronic payments, Yohan et al[180] propose a secure BLE based authentication protocol for micropayment with IoT Wearable Devices (WD). The proposed scheme is based on mutual authentication between the WD and the Wearable Payment Counter (WP counter). Thus, communication is only between these 2 entities without the help of any intermediary device like smart phone. This protocol generates unique session key that is used for each communication process along with secret string stored in both WD and WP counter. The proposed protocol consists of 3 stages: the initialization stage, the authentication stage, and the payment stage. The authors described in 4 steps the process of authentication. They claimed that the proposed protocol can protect against 5 major attacks, namely session hijacking, bogus payment counter, passive eavesdropping, replay, and MitM attacks.

5.3 | Hardware-based solutions

Software-based security schemes remain vulnerable to certain types of attacks. For example, if a smart device can be accessed, it will not be too difficult for a malicious entity to clone or change its behavior by infecting it with rogue code. The effect is maximized if the device is infected with a bootkit malware that corrupts the boot-up sequence, which can consequently cause the device to load and run malicious code. It is difficult to prevent such attacks by using software-based security alone. Hence, many researchers argue that embedded and hardware security approaches can provide the underlying support to address the security and privacy issues related with IoT devices.

One possible approach for addressing these issues is the use of PUFs, proposed by Kanuparthi et al .[181] Essentially, PUFs are circuit primitives that can derive secrets from physical characteristics of Integrated Circuits (ICs), instead of storing secrets in digital memory. PUFs can be used to provide low cost authentication by generating secret keys that can be used for cryptographic computations. They show that by combining sensing and cryptography, sensor PUFs can provide data provenance and integrity. They describe how PUFs can be used by selecting challenge response pairs at random, to address forge identity threats. The authors also show that effective trust management can be achieved using PUFs and hardware performance counters; and finally, they describe how confidentiality and privacy of users can be guaranteed by using lightweight encryption algorithms.

Xu et al[182] discuss the use of digital PUFs for hardware security in optimizing intensive computer-aided design (CAD) for the design of more secure IoT devices. The authors observed that the analog key hardware-based security PUFs are cumbersome to integrate into digital designs, hence they advocate the use of digital PUFs also known as Public Physical Unclonable Functions (PPUFs), which enable the creation of public key protocols. The authors believe that hardware-based security solutions based on optimized CAD will show more resilience against side-channel and physical attacks, and they will also serve as good platforms for the implementation IoT protocols, because of their energy efficiency.

In the same vein, Aman et al[183] present a preliminary PUFs based mutual authentication protocol in IoT systems. The authors argue that the unique characteristics of PUFs can be exploited to provide security in IoT devices without the need to store secrets in such devices. The authentication process has 4 steps, consisting of 3 messages each. In step 1, an IoT device starts the authentication process by sending its ID to a server, and after some computations, the server verifies the message using a MAC in step 4. If the server verifies the MAC of message 3, it means the authentication is successful. However, if MAC verification fails at any step, the authentication fails. The authors claimed that the proposed protocol is secure against many attacks, including cloning or impersonation, replay, eavesdropping, MitM, spoofing, interleaving and physical attacks.

Approaching the subject matter from a different perspective, Rose[184] suggests the use of nanoelectronic hardware technologies like metal-oxide memristors for implementing security primitives and protocols in emerging IoT devices. The rationale being that nanoscale security primitives would provide the required levels of security with a very small form factor, while consuming negligible amount of energy. The author used memristive Crossbar PUF (XbarPUF) that is based on Write-Time Memristive PUF (WTMPUF) as a case example. Although XbarPUF does not depend on precise write-time, the author discovered that it performs in the same way as the WTMPUF. Moreover, the performance of XbarPUF is similar to circuits implemented using Complementary Metal-Oxide Semiconductor (CMOS) like Arbiter PUF (APUF), while decreasing transistor count. Additionally, the amount of power consumed by XbarPUF during the study was considerably smaller in comparison with WTMPUF and APUF.

Babar et al[185] propose an embedded security framework for IoT based on hardware/software methodology. The authors observed that balancing the trade-offs between cost of security and performance in the IoT is not an easy task, and hence they asserted that, in order to realize a cost effective and well established design that will meet the fundamental security goals, there is a need to combine both hardware and software implementations of security mechanisms. Therefore, the architecture consists of hardware and software levels supported at the physical and MAC layer by lightweight standardized protocols. Their security framework (which has the following features: lightweight cryptography, physical security, standardized security protocols, secure operating systems and secure storage) suggests that security should be built into the device itself. The proposed architecture promises flexible and rigorous detection, diagnosis, isolation, and quick intervention against successful breaches.

In another contribution focusing on the use of digital fingerprints for *things* authentication (similar to biometrics for human authentication), Aysu et al[186] propose the generation of digital fingerprints using popular MEMS sensors (eg, accelerometer) for low-cost platforms. In order to generate device unique electronic signatures, the authors exploited the random process variations at the time of manufacturing the ICs, and for MEMS accelerometers, the process variations produce a static offset sensor data. These unique values can be obtained by applying electrostatic impulse to the accelerometer and measuring its response. The proposed technique was demonstrated on ADXL345 accelerometer, and results reveal that it is possible to use MEMS sensors for digital fingerprints for run-time *things* authentication applications.

5.4 | Solutions for specific application domains

This subsection presents some lightweight security and privacy solutions for resource constrained devices that have been tailored for some specific application areas of the IoT.

Yan et al[187] propose an efficient Integrated Authentication and Confidentiality (IAC) security protocol for securing AMI communications in smart grid, which is based on a communication architecture that has a hop-by-hop data collection and forwarding mechanism. Their protocol consists of the following processes: initialization for authentication, meter reading collection for user data confidentiality and control message distribution for control message confidentiality. The authors used mutual authentication so as to establish secure key pairs between an authentication remote server and a smart meter for secure data communications. Security analysis reveals that the proposed protocol can offer more efficient and secure data collection as well as better message delivery between smart meters and a local collector.

For solutions in smart healthcare, Lee et al[188] propose a secure key management scheme based on ECC for protecting medical information of patients, which consists of 3 phases: setup, registration and verification and key exchange. The authors employed ECC due to its small key size and low computational cost, they also used SIM card numbers of the smart phone of patients as the identification code, while patients are allowed to compute their full private keys instead of depending on a third party. The proposed scheme also uses hashed counter number in the process of authenticated message exchange so as to protect against replay attacks. However, the authors did not present any experimental results.

In the same vein, Picazo-Sanchez et al[189] propose an architecture based on Publish-Subscribe protocols for heterogeneous medical WBANs that are used as wearable and implantable sensors and devices. Due to the possibility that medical sensors may coexist with other sensors and devices, the authors used these 2 protocols that are based on the Ciphertext Policy Attribute-Based Encryption (CP-ABE) scheme, a lightweight paradigm proposed recently, since the CP-ABE primitives allow sensors to subscribe to the data published by different devices and sensors using a constant size decryption key. The proposed scheme provides a fine-grained access control by using Lattice-Based Access Control (LBAC) policies that utilizes only AND operations; and experimental results show that the proposed scheme can be used on most of the sensors in use today.

Liu et al[190] present a scalable, regular and highly optimized ECC library that achieves high performance for scalar multiplications on both AVR-based and MSP430-based sensor nodes, such as MICAz and Tmote Sky with different levels of security. The authors also define a new family of lightweight elliptic curves (MoTe curve) for resource-constrained sensor nodes. Their parametrized implementation of elliptic curve group arithmetic, which has 2 different versions of designs, supports pseudo-Mersenne prime fields. First, the high-speed version (which aims at setting a new speed record) achieves high performance, while the memory-efficient version (aims at saving memory space) requires only half of the code size of current best implementation. The authors also developed a model for evaluating the energy consumption of cryptographic schemes. Both versions can defend against timing and Simple Power Analysis (SPA) attacks.

5.5 | Current IoT security mechanisms

Although addressing IoT security issues from a holistic point of view remains a bottleneck, there are quite a few lightweight security mechanisms currently in use, which are based on a number of security techniques and cryptographic algorithms, including hash functions, XOR encryption, access control, and lightweight public-key cryptographic schemes based on ECC.

1. In IoT, *hash functions* and Cryptographically Secure Pseudo Random Number Generators (CSPRNGs) can be used to implement security solutions for IoT devices and embedded systems. For example, a hash function and a pseudo random number generator (PRNG) based on AES (in this specific case) have been used to implement a security for embedded microprocessors that uses less memory and consumes less energy.[191] Similarly, a hash algorithm is used to ensure integrity in smart home systems.[192]
2. XOR *encryption* is lightweight, and hence it is employed in many IoT security mechanisms.[193] For instance, a lightweight authentication protocol for IoT was developed based on XOR manipulation.[179] In the same vein, a secure tag search scheme based on XOR and PRNGs for RFID that protects against tracking of tags was proposed in.[194]
3. *Access control*: A robust IoT security policy should specify who or what has access to what, and to which extent. This is particularly important for accessing information contained in or generated by edge devices in the perception layer of the IoT. Access control is the technology that is currently being used to achieve this objective. A number of lightweight security mechanisms have been proposed over the years to efficiently inhibit improper access to information in the IoT while considering the inherent restrictions imposed by IoT edge devices. A few security solutions based on authentication and access control have been examined in section 5.2, however, 2 solutions mainly based on access control are considered herein. Fotiou et al[195] proposed a lightweight solution aimed at addressing the access control problem in the IoT. In this scheme, complex access control decisions are delegated to trusted third parties, which impose minimal overhead on the resource-constrained devices. Their results show that the solution is secure and enhances end-user privacy. Beltran et al[196]

presented *SMARTIE*, a user-centric access control integrating platform for efficient security in smart cities. The authors claimed that their platform can ensure security, access control and user privacy for citizens sensitive information.

4. *ECC* is a type of public-key cryptography based on manipulation of points on elliptic curves as well as number theory. Today, ECC is one of the most widely used public-key cryptosystems to achieve security objectives, such as confidentiality, integrity, nonrepudiation, and availability. The primary advantages of ECC over the earlier cryptosystems like RSA are smaller key size and speed. With reduced key size, ECC based algorithms can provide the same cryptographic strength as their RSA-based counterparts. For example, a 384-bit ECC key is equivalent to 7680 bit RSA key. Consequently, ECC is emerging as an attractive cryptosystem for constrained environments such as IoT and embedded systems. For instance, Haripriya and Kulothungan[197] proposed a mutual authentication scheme based on ECC self-certified key management, where the public key of the highly constrained nodes in the IoT system is generated by the less constrained systems. A lightweight ECC for the Contiki OS was also implementation by Pinol et al,[198] and it is released under the Berkeley Software Distribution license.

Researchers are still working on different aspects of IoT security and privacy. The most recently proposed IoT security mechanisms include the work of Zhu et al,[199] who proposed an automatic identity framework for the IoT. The authors used Blockchain-based Identity Framework to achieve identity self-management by end users for a smart home scenario. The proposed framework can autonomously extract appliances signatures, and then create blockchain-based identities for their appliance owners.

Another framework for enabling risk management for smart infrastructures with an anomaly behavior analysis intrusion detection system was presented by Pacheco et al.[200] Their work is based on an anomaly behavior analysis method that allows the autonomic computing paradigm and an intrusion detection system to detect any threat capable of compromising IoT infrastructures.

In order to protect physical IoT devices from intruders, Nakagawa and Shimojo[201] also proposed an IoT agent platform mechanism with transparent cloud computing framework for improving IoT security. Their mechanism is based on a transparent programming framework for IoT devices called Dripcast, which allows vendors to easily develop physical IoT devices.

6 | OPEN ISSUES

Although significant research efforts have been made toward securing IoT devices, there are still many challenges ahead. Considering the basic security requirements of many IoT devices, most of the existing cryptographic techniques that are currently available have some issues, and hence require further study and analysis to determine applicability in the context of the IoT. This is because most of the cryptographic suites were designed for systems with sufficient resources, such as memory and processor speed. Even some of the newly schemes proposed for the 3 layers of the IoT, some of which are lightweight, need to be further investigated and enhanced before they can be fully applicable in the IoT.

The near-universal acceptance of IoT will largely depend upon trust and confidence of people that the new technology will provide some level of security and privacy to their sensitive personal data.[202] The review of existing solutions in section 5 reveals several important research challenges pertaining to addressing security and privacy issues in the IoT. In this section, we outline some of the important open research challenges that need to be addressed in this active area of research as follows:

- some authentication schemes designed for specific IoT scenarios are not able to protect against all possible threats associated with such ecosystems. For example, the scheme proposed in[176] is not effective against Sybil attacks, and hence the need for more studies in that direction;
- authentication schemes for IoT applications must be lightweight, efficient and flexible, while ensuring that security and privacy are not compromised;
- there is need to design appropriate cryptographic schemes for each IoT application domain;
- lightweight cryptography for the resource constrained devices of IoT still needs further studies;
- there is need to investigate some existing lightweight authentication solutions like the one in[179] in order to ascertain the claims of authors about the viability of the schemes;
- holistic approach to ensuring security and privacy in the IoT devices is needed, unlike the approach in[168] where security is only guaranteed when transmission is in one direction (ie, from sensor nodes to Internet host);
- there is need to investigate the fate of existing lightweight cryptographic schemes for securing IoT devices in quantum computing, since it is believed that quantum computers will break most of the existing standard public-key cryptographic systems.[203–205] Also, there is need to design new lightweight cryptographic schemes that can survive quantum computing;
- there is need to develop a more robust model for evaluating the energy consumption of cryptographic schemes[190];
- there in need to develop more reliable and resource efficient nanoelectronic security primitives[184];

- there is need for efficient key management schemes that can be used in different application domains;
- key management schemes need to be verified through simulations and experimental test beds. For instance, the authors of[165,173,188] did not verify their claims using experimental testbeds or simulations. As such, it is difficult to ascertain their findings;
- some of the existing key management schemes are not suitable for resource constrained devices of the IoT. For instance, considering the type and resources of the machine used in the experimental testbed in,[166] it can be concluded that the proposed scheme is not suitable for severely constrained devices of the IoT, hence the need for more research on lightweight schemes;
- there is need for efficient key revocation schemes that can be used to annul or cancel keys when adversaries successfully compromised smart devices;
- the key management schemes where resource constrained nodes delegate most of the computation tasks to non-constrained remote party proxy nodes, usually outside the network, need further studies.

7 | CONCLUSIONS

In the last few years there has been considerable interest in the study of IoT among researchers. The security and privacy aspects have particularly been attracting a significant research attention, and this would continue for years to come due to the numerous security and privacy challenges posed by IoT connected devices, especially those with limited resources. Consequently, several researchers have made considerable progress in developing lightweight protocols, schemes and frameworks aimed at addressing security and privacy-related concerns in the IoT. We have surveyed a number of such approaches that have been proposed in the literature.

In this survey article, we have compared this survey with the previous works on the same subject and showed how it differs from the previous surveys. We presented an overview of the IoT, defined 9 application domains, as well as identified cyber assets per domain. We also defined security requirements and presented typical security requirements for the IoT application domains within the scope of this paper. In addition, we discussed system model, threat model and protocols/technologies, all within the context of IoT. Furthermore, we presented a review of the existing approaches for securing resource-constrained devices of the IoT, and discussed current IoT security mechanisms. Finally, we highlighted some open issues and research challenges that need to be addressed in the near future.

ACKNOWLEDGEMENTS

The authors wish to thank the Centre for Geodesy and Geodynamics, National Space Research and Development Agency, Toro, Bauchi State, Nigeria for supporting this work. This work is partially supported by the Portuguese Fundação para a Ciência e a Tecnologia (FCT) under the UID/EEA/50008/2013 Project.

ORCID

Musa G. Samaila http://orcid.org/0000-0003-2913-9447

REFERENCES

1. Li S, Xu L, Zhao S. The internet of things: a survey. *Inf Syst Frontiers*. 2015;17(2):243-259.
2. Breivold HP, Sandstrãűm K. *Internet of Things for industrial automation—challenges and technical solutions. IEEE International Conference on Data Science and Data Intensive Systems, December*; 2015:532-539.
3. Bello O, Zeadally S. Intelligent device-to-device communication in the Internet of Things. *IEEE Syst J*. 2014;PP(99):1-11.
4. Jara Antonio J, Ladid L, Skarmeta A. The internet of everything through IPv6: an analysis of challenges, solutions and opportunities. *J Wireless Mobile Netw, Ubiquitous Comput, Dependable Appl (JoWUA)*. 2013;4(3):97-118.
5. Hasan M, Hossain E, Niyato D. Random access for machine-to-machine communication in LTE-advanced networks: issues and approaches. *IEEE Commun Mag*. 2013;51(6):86-93.
6. Zhang M, Sun F, Cheng X. *Architecture of Internet of Things and its key technology integration based-on RFID. 5th IEEE International Symposium on Computational Intelligence and Design (ISCID), October*; 2012:294-297.
7. Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of things (IoT): a vision, architectural elements, and future directions. *J Future Gener Comput Syst*. 2013;29(7):1645-1660.
8. Forsythe EW, Leever B, Gordon M, et al. *Flexible electronics for commercial and defense applications. 2015 IEEE International Electron Devices Meeting (IEDM), December*; 2015:19.1.1–19.1.4. https://doi.org/10.1109/IEDM.2015.7409731.
9. Raza S, Misra P, He Z, Voigt T. *Bluetooth smart: an enabling technology for the Internet of Things. 11th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), October*; 2015:155-162.
10. Fortino G, Guerrieri A, Russo W. *Agent-oriented smart objects development. 16th IEEE International Conference on Computer Supported Cooperative Work in Design (CSCWD), May*; 2012:907-912.
11. Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M. Internet of things for smart cities. *IEEE IoT J*. 2014;1(1):22-32.

12. Xu LD, He W, Li S. Internet of things in industries: a survey. *IEEE Trans Ind Informat*. 2014;10(4):2233-2243.
13. Chandrakanth S, Venkatesh K, Mahesh JU, Naganjaneyulu KV. Internet of Things. *Int J Innov Adv Comput Sci*. 2014;3(8):1-20.
14. Lio MD, Biral F, Bertolazzi E, et al. Artificial co-drivers as a universal enabling technology for future intelligent vehicles and transportation systems. *IEEE Trans Intell Transp Syst*. 2015;16(1):244-263.
15. Nastic S, Sehic S, Le D-H, Truong H-L, Dustdar S. *Provisioning software-defined IoT cloud systems. IEEE International Conference on Future Internet of Things and Cloud (FiCloud), August*; 2014:288-295.
16. Rao Prahlada BB, Saluja P, Sharma N, Mittal A, Sharma SV. *Cloud computing for Internet of Things and sensing based applications. 6th IEEE International Conference on Sensing Technology (ICST), December*; 2012:374-380.
17. Botta A, de Donato W, Persico V, Pescape A. *On the integration of cloud computing and internet of things. IEEE International Conference on Future Internet of Things and Cloud (FiCloud), August*; 2014:23-30.
18. Keoh Sye L, Kumar Sandeep S, Tschofenig H. Securing the Internet of Things: a standardization perspective. *IEEE IoT J*. 2014;1(3):265-275.
19. Want R, Schilit BN, Jenson S. Enabling the internet of things. *IEEE Comput*. 2015;48(1):28-35.
20. Singh D, Tripathi G, Jara AJ. *A survey of internet-of-things: future vision, architecture, challenges and services. IEEE World Forum on Internet of Things (WF-IoT), March*; 2014:287-292.
21. Perera C, Zaslavsky A, Christen P, Georgakopoulos D. Context aware computing for the Internet of Things: a survey. *IEEE Commun Surv Tuts: First Quarter*. 2014;16(1):414-454.
22. Weiser M. The computer for the 21st century. *SIGMOBILE Mob Comput Commun Rev*. 1999;3(3):3-11.
23. Liu Y, Zhou G. *Key technologies and applications of Internet of Things. 5th IEEE International Conference on Intelligent Computation Technology and Automation (ICICTA), January*; 2012:197-200.
24. Vermesan O, Friess P. In: Ruggieri M, Nikookar H, eds. *Internet of Things: converging technologies for smart environments and integrated ecosystems*. Aalborg, Denmark: River Publishers Denmark; 2013.
25. Stankovic JA. Research directions for the internet of things. *IEEE IoT J*. 2014;1(1):3-9.
26. Axelrod CW. *Enforcing security, safety and privacy for the Internet of Things. IEEE Long Island Conference on Systems, Applications and Technology (LISAT), May*; 2015:1-6.
27. Clarke S. The Internet of Things: Cybersecurity Threat or Massive Hype?: nuix; 2015. https://www.nuix.com/blog/internet-things-cybersecurity-threat-or-massive-hype. Accessed April 5 2015.
28. Zahra A, Shah MA. *IoT based Ransomware growth rate evaluation and detection using command and control blacklisting. IEEE 23rd International Conference on Automation and Computing (ICAC), September*; 2017:1-6.
29. Skarmeta AF, HernaÌĄndez-Ramos JL, Moreno MV. *A decentralized approach for security and privacy challenges in the internet of things. IEEE World Forum on Internet of Things (WF-IoT), March*; 2014:67-72.
30. Anderson M. Vulnerable “Smart” Devices Make an Internet of Insecure Things: IEEE Spectrum; 2004. https://spectrum.ieee.org/riskfactor/computing/networks/vulnerable-smart-devices-make-an-internet-of-insecure-things. Accessed December 2, 2015.
31. Niu J, Jin Y, Lee AJ, Sandhu R, Xu W, Zhang X. *Panel security and privacy in the age of Internet of Things: opportunities and challenges. Proceedings of the 21st ACM on Symposium on Access Control Models and Technologies*. New York, NY: ACM; 2016:49-50.
32. Roman R, Najera P, Lopez J. Securing the internet of things. *IEEE Comput*. 2011;44(9):51-58.
33. Scott D, Ketel M. *Internet of things: a useful innovation or security nightmare? Southeastcon 2016, March*; 2016:1-6.
34. HP. *Internet of Things Research Study*. HP; 2014. http://d-russia.ru/wp-content/uploads/2015/10/4AA5-4759ENW.pdf. Accessed March 10.
35. ISACA. *Risks and Rewards of the Internet of Things*. ISACA; 2013. https://www.isaca.org/SiteCollectionDocuments/2013-Risk-Reward-Survey/2013-Global-Survey-Report.pdf. Accessed Febrruary 07, 15.
36. Kumar JS, Patel Dhiren R. A survey on internet of things: security and privacy issues. *Int J Comput Appl*. 2014;90(11):20-26.
37. Zhao K, Ge L. *A survey on the Internet of Things security. 9th IEEE International Conference on Computational Intelligence and Security (CIS), December*; 2013:663-667.
38. Granjal J, Monteiro E, Sa Jorge S. Security for the internet of things: a survey of existing protocols and open research issues. *IEEE Commun Surv Tuts*. 2015;17(3):1294-1312.
39. Sicari S, Rizzardi A, Grieco LA, Porisini AC. Security, privacy and Trust in Internet of things: the road ahead. *Comput Netw*. 2015;76:146-164.
40. Grabovica M, Popic S, Pezer D, Knezevic V. *Provided security measures of enabling technologies in Internet of things (IoT): a survey. IEEE International Conference on Zooming Innovation in Consumer Electronics (ZINC), June*; 2016:28-31.
41. Granjal J, Monteiro E, Sa Jorge S. Security in the integration of low-power wireless sensor networks with the internet: a survey. *J Ad Hoc Netw*. 2015;24(Pt A):264-287.
42. Benabdessalem R, Hamdi M, Kim TH. *A survey on security models, techniques, and tools for the Internet of Things. 7th IEEE International Conference on Advanced Software Engineering and Its Applications (ASEA), December*; 2014:44-48.
43. Suo H, Wan J, Zou C, Liu J. *Security in the internet of things: a review. IEEE International Conference on Computer Science and Electronics Engineering (ICCSEE), March*; 2012:648-651.
44. Oracevic A, Dilek S, Ozdemir S. *Security in Internet of Things: a survey. IEEE International Symposium on Networks, Computers and Communications (ISNCC), May*; 2017:1-6.
45. Yang K, Blaauw D, Sylvester D. Hardware designs for security in ultra-low-power IoT systems: an overview and survey. *IEEE Micro*. 2017;37(6):72-89.
46. Chen L, Thombre S, Jarvinen K, et al. Robustness, security and privacy in location-based services for future IoT: a survey. *IEEE Access*. 2017;5:8956-8977.
47. Qiu T, Chen N, Li K, Atiquzzaman M, Zhao W. How can heterogeneous Internet of Things build our future: a survey. *IEEE Commun Surv Tuts*. 2018;PP(99):1-1.
48. Sezer OB, Dogdu E, Ozbayoglu AM. Context-aware computing, learning, and big data in Internet of Things: a survey. *IEEE IoT J*. 2018;5(1):1-27.
49. Miorandi D, Sicari S, Pellegrini FD, Chlamtac I. Internet of things: vision, applications and research challenges. *Ad Hoc Netw*. 2012;10(7):1497-1516.
50. Yan Z, Zhang P, Vasilakos AV. A survey on trust management for internet of things. *J Netw Comput Appl*. 2014;42:120-134.
51. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of things: a survey on enabling technologies, protocols, and applications. *IEEE Commun Surv Tutor: Fourth Quarter*. 2015;17(4):2347-2376.
52. Atzori L, Iera A, Morabito G. The Internet of Things: a survey. *Comput Netw*. 2010;54(15):2787-2805.
53. Kraijak S, Tuwanut P. *A survey on Internet of Things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends. 16th IEEE International Conference on Communication Technology (ICCT), October*; 2015:26-31.
54. Razzaque MA, Milojevic-Jevric M, Palade A, Clarke S. Middleware for internet of things: a survey. *IEEE IoT J*. 2016;3(1):70-95.
55. Moness M, Moustafa AM. A survey of cyber-physical advances and challenges of wind energy conversion systems: prospects for internet of energy. *IEEE IoT J*. 2016;3(2):134-145.
56. Whitmore A, Agarwal A, Da XL. The internet of things: a survey of topics and trends. *Inf Syst Frontiers*. 2015;17(2):261-274.

57. Landwehr C, Boneh D, Mitchell JC, Bellovin SM, Landau S, Lesk ME. Privacy and cybersecurity: the next 100 years. *Proc IEEE*. 2012;100(Special Centennial Issue):1659-1673.
58. Liu J, Li X, Chen X, Zhen Y, Zeng L. *Applications of Internet of Things on smart grid in China. 13th IEEE International Conference on Advanced Communication Technology (ICACT), February*; 2011:13-17.
59. Gang G, Zeyong L, Jun J. *Internet of Things security analysis. IEEE International Conference on Internet Technology and Applications (iTAP), August*; 2011:1-4.
60. Qi J, Vasilakos Athanasios V, Wan J, Lu J, Qiu D. Security of the internet of things: perspectives and challenges. *Wireless Netw*. 2014;20(8):2481-2501.
61. Ou Q, Zhen Y, Li X, Zhang Y, Zeng L. *Application of Internet of Things in smart grid power transmission. 3th IEEE FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing (MUSIC), June*; 2012:96-100.
62. Cui K, Zhou K, Song H, Li M. Automated software testing based on hierarchical state transition matrix for smart home. *IEEE Access*. 2017;PP(99):1-1.
63. Saputro N, Akkaya K. Investigation of smart meter data reporting strategies for optimized performance in smart grid AMI networks. *IEEE IoT J*. 2017;PP(99):1-1.
64. Ejaz W, Naeem M, Shahid A, Anpalagan A, Jo M. Efficient energy Management for the Internet of things in smart cities. *IEEE Commun Mag*. 2017;55(1):84-91.
65. Guerrero-ibanez JA, Zeadally S, Contreras-Castillo J. Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies. *IEEE Wirel Commun*. 2015;22(6):122-128.
66. Choden P, Seesaard T, Eamsa-ard T, Sriphrapradang C, Kerdcharoen T. *Volatile urine biomarkers detection in type II diabetes towards use as smart healthcare application. 9th IEEE International Conference on Knowledge and Smart Technology (KST), February*; 2017:178-181.
67. Alexakos C, Anagnostopoulos C, Fournaris A, Kalogeras A, Koulamas C. *Production process adaptation to IoT triggered manufacturing resource failure events. 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), September*. IEEE; 2017:1-8.
68. Fore V, Khanna A, Tomar R, Mishra A. *Intelligent supply chain management system. IEEE International Conference on Advances in Computing and Communication Engineering (ICACCE), November*; 2016:296-302.
69. KozioÅĆ D, Moya FS, Yu L, Van PV, Xu S. *QoS and service continuity in 3GPP D2D for IoT and wearables. IEEE Conference on Standards for Communications and Networking (CSCN), September*; 2017:233-239.
70. Nugroho LE, Pratama AGH, Mustika IW, Ferdiana R. *Development of monitoring system for smart farming using progressive web app. 9th IEEE International Conference on Information Technology and Electrical Engineering (ICITEE), October*; 2017:1-5.
71. Bing K, Fu L, Zhuo Y, Yanlei L. *Design of an Internet of Things-based smart home system. 2nd IEEE International Conference on Intelligent Control and Information Processing (ICICIP), July*; 2011:921-924.
72. Kumar GEP, Baskaran K, Blessing RE, Lydia M. *Securing the smart grid network: a review. IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), December*; 2016:1-6.
73. Wind River. *Internet of Things: Energy Use Case*. Wind River Systems, Inc.; 2014.
74. Ding D, Conti M, Solanas A. *A smart health application and its related privacy issues. 2016 Smart City Security and Privacy Workshop (SCSP-W), April*; 2016:1-5.
75. UCL Centre For Advanced Spatial Analysis. *Smart Cities of the Future*. London, UK: Centre for Advanced Spatial Analysis, University College; 2012.
76. Casale A, Spadafina L, Porcelli A, Matrino D, Sarcina V. *A water meter reading middleware for smart consumption monitoring. IEEE Workshop on Environmental, Energy, and Structural Monitoring Systems (EESMS), June*; 2016:1-6.
77. Brizzi P, Bonino D, Musetti A, Krylovskiy A, Patti E, Axling M. *Towards an ontology driven approach for systems interoperability and energy management in the smart city. International Multidisciplinary Conference on Computer and Energy Science (SpliTech), July*; 2016:1-7.
78. Djahel S, Doolan R, Muntean G-M, Murphy J. A communications-oriented perspective on traffic management systems for smart cities: challenges and innovative approaches. *IEEE Commun Surv Tutor*. 2015;17(1):125-151.
79. Konig M, Jacob J, Kaddoura T, Farid AM. *The role of resource efficient decentralized wastewater treatment in smart cities. Smart Cities Conference (ISC2), 2015 IEEE First International, October*; 2015:1-5.
80. Yuan W, Li Y, Liu C. *Integrated intelligence of long bridge disaster prevention and mitigation by focusing on bearing performance. IEEE International Conference on Smart City and Systems Engineering (ICSCSE), November*; 2016:54-58.
81. Khekare GS. *Design of emergency system for intelligent traffic system using VANET. IEEE International Conference on Information Communication and Embedded Systems (ICICES2014), February*; 2014:1-7.
82. Yongjun Z, Xueli Z, Shuxian Z, Shenghui G. *Intelligent transportation system based on internet of things. IEEE World Automation Congress (WAC), June*; 2012:1-3.
83. Chunli L. *Intelligent transportation based on the Internet of Things. 2nd IEEE International Conference on Consumer Electronics, Communications and Networks (CECNet), April*; 2012:360-362.
84. Turner SW, Uludag S. *Intelligent transportation as the key enabler of smart cities. IEEE/IFIP Network Operations and Management Symposium, April*; 2016:1261-1264.
85. Cheng J, Wu W, Cao J, Li K. Fuzzy group-based intersection control via vehicular networks for smart transportations. *IEEE Trans Ind Inform*. 2017;13(2):751-758.
86. Lu C. *Smart grid, smart transportation, and smart city: where we are? Keynote address. IEEE/ACIS 16th International Conference on Computer and Information Science (ICIS), May*; 2017:1-1.
87. Moller DPF, Vakilzadian H. *Cyber-physical systems in smart transportation. IEEE International Conference on Electro Information Technology (EIT), May*; 2016:0776-0781.
88. Kiran MPRS, Rajalakshmi P, Bharadwaj K, Acharyya A. *Adaptive rule engine based IoT enabled remote health care data acquisition and smart transmission system. IEEE World Forum on Internet of Things (WF-IoT), March*; 2014:253-258.
89. DELL. *Digital Technologies are Driving a New Generation of Telehealth*. DELL; 2014. http://i.dell.com/sites/doccontent/business/solutions/whitepapers/en/Documents/D391_Telehealth_Whitepaper.pdf. Accessed March 20, 2015.
90. Kavitha KC, Perumalraja R. *Smart wireless healthcare monitoring for drivers community. IEEE International Conference on Communications and Signal Processing (ICCSP), April*; 2014:1105-1108.
91. Suryajaya B, Chen CC, Hung MH, Liu YY, Liu JX, Lin YC. *A fast large-size production data transformation scheme for supporting smart manufacturing in semiconductor industry. 13th IEEE Conference on Automation Science and Engineering (CASE), August*; 2017:275-281.
92. Qi Q, Tao F. Digital twin and big data towards smart manufacturing and industry 4.0: 360 degree comparison. *IEEE Access*. 2018;PP(99):1-1.
93. Yuvaraj S, Sangeetha M. *Smart supply chain management using Internet of Things(IoT) and low power wireless communication systems. IEEE International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), March*; 2016:555-558.
94. Chen S, Shi R, Ren Z, Yan J, Shi Y, Zhang J. *A blockchain-based supply chain quality management framework. 14th IEEE International Conference on e-Business Engineering (ICEBE), November*; 2017:172-176.
95. Sharma A, Pande T, Aroul P, Soundarapandian K, Lee W. *Circuits and systems for energy efficient smart wearables. IEEE International Electron Devices Meeting (IEDM), December*; 2016:6.2.1-6.2.4.
96. Sun W, Liu J, Zhang H. When smart wearables meet intelligent vehicles: challenges and future directions. *IEEE Wirel Commun*. 2017;24(3):58-65.
97. Mekala MS, Viswanathan P. *A Survey: Smart Agriculture IoT with Cloud Computing. IEEE International conference on Microelectronic Devices, Circuits and Systems (ICMDCS), August*; 2017; 1-7.
98. Gartner. *How Does IoT Impact Your Information Management Strategy?* . Egham, UK: Gartner; 2015.

99. Savvas A. *Farming Industry must Embrace the Internet of Things to 'Grow Enough Food'*. IDG, UK: Techworld; 2015.
100. Varga P, Plosz S, Soos G, Hegedus C. *Security threats and issues in automation IoT*. *13th IEEE International Workshop on Factory Communication Systems (WFCS), May*; 2017:1-6.
101. Islam S, Falcarin P. *Measuring security requirements for software security*. *10th IEEE International Conference on Cybernetic Intelligent Systems (CIS), September*; 2011:70-75.
102. Cybenko G, Hughes J. *No free lunch in cyber security*. *Proceedings of the First ACM Workshop on Moving Target Defense*. New York, NY: ACM; 2014:1-12.
103. Raza S. *Lightweight Security Solutions for the Internet of Things*. Kista Stockholm: Swedish Inst. Comput. Sci. (SICS), Swedish ICT; 2013.
104. Lin CH, Hsieh WS, Mo F, Chang MH. *A PTC scheme for Internet of Things: private-trust-confidentiality*. *30th IEEE International Conference on Advanced Information Networking and Applications Workshops (WAINA), March*; 2016:969-974.
105. Mukherjee A. Physical-layer security in the internet of things: sensing and communication confidentiality under resource constraints. *Proc IEEE*. 2015;103(10):1747-1761.
106. D'Orazio CJ, Choo KKR, Yang LT. Data exfiltration from internet of things devices: iOS devices as case studies. *IEEE IoT J*. 2017;4(2):524-535.
107. Ali M, Reaz R, Gouda Mohamed G. *Nonrepudiation protocols without a trusted party*. In: Abdulla PA, Delporte Gallet C, eds. *Networked Systems: 4th International Conference, NETYS 2016, Marrakech, Morocco, May 18–20, 2016, Revised Selected Papers*. Springer International Publishing; 2016:1-15.
108. Perera C, Ranjan R, Wang L, Khan SU, Zomaya AY. Big data privacy in the internet of things era. *IT Prof*. 2015;17(3):32-39.
109. Porambage P, Ylianttila M, Schmitt C, Kumar P, Gurtov A, Vasilakos AV. The quest for privacy in the internet of things. *IEEE Cloud Comput*. 2016;3(2):36-45.
110. Madakam S, Date H. *Security mechanisms for connectivity of smart devices in the Internet of Things*. In: Mahmood Z, ed. *Connectivity Frameworks for Smart Devices, Computer Communications and Networks Switzerland*. Springer International Publishing; 2016:23-41.
111. Sabaliauskaite G, Adepu S. *Integrating six-step model with information flow diagrams for comprehensive analysis of cyberphysical system safety and security*. *18th IEEE International Symposium on High Assurance Systems Engineering (HASE), January*; 2017:41-48.
112. Tyagi H. *Distributed computing with privacy*. *IEEE International Symposium on Information Theory Proceedings, July*; 2012:1157-1161.
113. Rapoza J. *Your TV is Listening to You, as is Most of the Internet of Things*. TechPro Essentials; 2015. http://www.aberdeenessentials.com/techpro-essentials/your-tv-is-listening-to-you-as-is-most-of-the-internet-of-things/. Accessed September 8, 2015.
114. Wang Y, Lin W, Zhang T. *Study on security of wireless sensor networks in smart grid*. *IEEE International Conference on Power System Technology (POWERCON), October*; 2010:1-7.
115. Mukisa SS, Rashid A. *Cyber-security challenges of agent technology in intelligent transportation systems*. *Proceedings of the 1st International Workshop on Agents and CyberSecurity*. New York, NY, ACM; 2014:9:1-9:4.
116. Kumar S, Poddar S, Marimuthu R, Balamurugan S, Balaji S. *A review on communication protocols using Internet of Things*. *IEEE International conference on Microelectronic Devices, Circuits and Systems (ICMDCS), August*; 2017:1-6.
117. Ayar M, Latchman HA. *A delay and throughput study of adaptive contention window based HomePlug MAC with prioritized traffic classes*. *International Symposium on Power Line Communications and its Applications (ISPLC), March*; 2016:126-131.
118. Aouini I, Azzouz LB, Jebali M, Saidane LA. *Improvements to the smart energy profile security*. *13th International Wireless Communications and Mobile Computing Conference (IWCMC), June*; 2017:1356-1361.
119. Yassein MB, Mardini W, Khalil A. *Smart homes automation using Z-wave protocol*. *International Conference on Engineering MIS (ICEMIS), September*; 2016:1-6.
120. Garrido C, Lopez V, Olivares T, Ruiz MC. *Poster abstract: architecture proposal for heterogeneous, BLE-based sensor and actuator networks for easy management of smart homes*. *15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN), April*; 2016:1-2.
121. Yufeng Z, Ruqiao J. *Design and realization of the smart home control system based on the Bluetooth*. *IEEE International Conference on Intelligent Transportation, Big Data and Smart City, Decmber*; 2015:286-289.
122. Sahana MN, Anjana S, Ankith S, Natarajan K, Shobha KR, Paventhan A. *Home energy management leveraging open IoT protocol stack*. *IEEE Recent Advances in Intelligent Computational Systems (RAICS), December*; 2015:370-375.
123. Baviskar A, Baviskar J, Wagh S, Mulla A, Dave P. *Comparative study of communication technologies for power optimized automation systems: a review and implementation*. *5th International Conference on Communication Systems and Network Technologies, April*. IEEE; 2015:375-380.
124. Samuel SSI. *A review of connectivity challenges in IoT-smart home*. *3rd MEC International Conference on Big Data and Smart City (ICBDSC), March*; 2016:1-4.
125. Landa I, Blazquez A, Velez M, Arrinda A. *Indoor measurements of IoT wireless systems interfered by impulsive noise from fluorescent lamps*. *11th European Conference on Antennas and Propagation (EUCAP), March*; 2017:2080-2083.
126. ElSaadany Y, AJA M, Ucci DR. *A wireless early prediction system of cardiac arrest through IoT*. *41st IEEE Annual Computer Software and Applications Conference (COMPSAC), July*; 2017:690-695.
127. Esquiagola J, Costa L, Calcina P, Zuffo M. *Enabling CoAP into the swarm: a transparent interception CoAP-HTTP proxy for the Internet of Things*. *2017 Global Internet of Things Summit (GIoTS), June*; 2017:1-6.
128. Tiburski RT, Amaral LA, de Matos E, de Azevedo DFG, Hessel F. *Evaluating the use of TLS and DTLS protocols in IoT middleware systems applied to E-health*. *14th IEEE Annual Consumer Communications Networking Conference (CCNC), January*; 2017:480-485.
129. Kheaksong A, Prayote A, Lee W. *Performance evaluation of smart grid communications via network simulation version 3*. *13th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), June*; 2016:1-5.
130. Mohammadali A, Tadayon MH, Asadian M. *A new key management for AMI systems based on DLMS/COSEM standard*. *2014 7th International Symposium on Telecommunications (IST), September*; 2014:849-856.
131. Jaloudi S. *Open source software of smart city protocols current status and challenges*. *International Conference on Open Source Software Computing (OSSCOM)*; 2015:1-6.
132. Kursawe K, Peters C. *Structural weaknesses in the open smart grid protocol*. *10th International Conference on Availability, Reliability and Security, August*; 2015:1-10.
133. Squartini S, Gabrielli L, Mencarelli M, Pizzichini M, Spinsante S, Piazza F. *Wireless M-bus sensor nodes in smart water grids: the energy issue*. *Fourth International Conference on Intelligent Control and Information Processing (ICICIP), June*; 2013:614-619.
134. Bellavista P, Cardone G, Corradi A, Foschini L. Convergence of manet and wsn in iot urban scenarios. *IEEE Sens J*. 2013;13(10):3558-3567.
135. Maxa JA, Mahmoud MSB, Larrieu N. *Joint model-driven design and real experiment-based validation for a secure UAV ad hoc network routing protocol*. *Integrated Communications Navigation and Surveillance (ICNS), April*; 2016:1E2-1-1E2-16.
136. Choi JS. Design and implementation of a stateful PCE-based unified control and management framework for carrier-grade MPLS-TP networks. *J Lightw Technol*. 2016;34(3):836-844.
137. Murakami M, Koike Y. Highly reliable and large-capacity packet transport networks: technologies, perspectives, and standardization. *J Lightw Technol*. 2014;32(4):805-816.
138. *IEEE Std 2030.1.1-2015. IEEE Standard Technical Specifications of a DC Quick Charger for Use with Electric Vehicles*. IEEE; 2016:1-97.
139. Hall J, Lee J, Benin J, Armstrong C, Owen H. *IEEE 1609 Influenced automatic identification system (AIS)*. *IEEE 81st Vehicular Technology Conference (VTC Spring), May*; 2015:1-5.

140. Shlayan N, Kurkcu A, Ozbay K. *Exploring pedestrian Bluetooth and WiFi detection at public transportation terminals. 19th IEEE International Conference on Intelligent Transportation Systems (ITSC), November*; 2016:229-234.
141. Huang X, Liu D, Zhang J. *An improved IEEE 802.15.6 password authenticated association protocol. IEEE/CIC International Conference on Communications in China (ICCC), November*; 2015:1-5.
142. Singh M, Jain N. Performance and evaluation of smartphone based wireless blood pressure monitoring system using Bluetooth. *IEEE Sens J*. 2016;16(23):8322-8328.
143. Spano E, Pascoli S. Di, Iannaccone G. Low-power wearable ECG monitoring system for multiple-patient remote monitoring. *IEEE Sens J*. 2016;16(13):5452-5462.
144. Burns NB, Sassaman P, Daniel K, Huber M, Zaruba G. *PESTO: data integration for visualization and device control in the smartcare project. IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), March*; 2016:1-6.
145. Khoi Ngo M, Saguna S, Mitra K, Ahlund C. *IReHMo: an efficient IoT-based remote health monitoring system for smart regions. 17th International Conference on E-health Networking, Application Services (HealthCom), October*; 2015:563-568.
146. Thamilarasu G, Odesile A. *Securing wireless body area networks: challenges, review and recommendations. IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), December*; 2016:1-7.
147. Marcon P, Zezulka F, Vesely I, et al. *Communication technology for Industry 4.0. IEEE Progress In Electromagnetics Research Symposium—Spring (PIERS), May*; 2017:1694-1697.
148. Luo Z, Hong S, Lu R, et al. *OPC UA-based smart manufacturing: system architecture, implementation, and execution. IEEE 5th International Conference on Enterprise Systems (ES), September*; 2017:281-286.
149. Beckmann K, Dedi O. *sDDS: a portable data distribution service implementation for WSN and IoT platforms. IEEE 12th International Workshop on Intelligent Solutions in Embedded Systems (WISES), October*. IEEE; 2015:115-120.
150. Houimli M, Kahloul L, Benaoun S. *Formal specification, verification and evaluation of the MQTT protocol in the internet of things. IEEE International Conference on Mathematics and Information Technology (ICMIT), December*; 2017:214-221.
151. Bocek T, Rodrigues BB, Strasser T, Stiller B. *Blockchains everywhere—a use-case of blockchains in the pharma supply-chain. IFIP/IEEE Symposium on Integrated Network and Service Management (IM), May*; 2017:772-777.
152. Sharma PK, Chen MY, Park JH. A software defined fog node based distributed Blockchain cloud architecture for IoT. *IEEE Access*. 2018;6:115-124.
153. Cha SC, Chen JF, Su C, Yeh KH. A blockchain connected gateway for BLE-based devices in the Internet of Things. *IEEE Access*. 2018;PP(99):1-1.
154. Burmester M, Munilla J, Ortiz A, Caballero-Gil P. An RFID-based smart structure for the supply chain: resilient scanning proofs and ownership transfer with positive secrecy capacity channels. *Sens J*. 2017;7(17):1-20.
155. Ray BR, Abawajy J, Chowdhury M, Alelaiwi A. Universal and secure object ownership transfer protocol for the Internet of Things. *Future Gener Comput Syst*. 2018;78:838-849.
156. Onishi H. *Paradigm change of vehicle cyber security. 4th IEEE International Conference on Cyber Conflict Torrance, CA, USA, June*; 2012:381-391. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6243987. Accessed September 27, 2015.
157. Mehmood NQ, Culmone R. *A data acquisition and document oriented storage methodology for ANT+ protocol sensors in realtime web. 30th IEEE International Conference on Advanced Information Networking and Applications Workshops (WAINA), March*; 2016:312-318.
158. Rheinländer CC, Wehn N. *Precise synchronization time stamp generation for Bluetooth low energy. 2016 IEEE SENSORS*. 2016;1-3, *October*; https://doi.org/10.1109/ICSENS.2016.7808812.
159. Lee T, Han J, Lee MS, Kim HS, Bahk S. *CABLE: connection interval adaptation for BLE in dynamic wireless environments. 14th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), June*; 2017:1-9.
160. Mehmood NQ, Culmone R, Mostarda L. *An ontology driven software framework for the healthcare applications based on ANT+ protocol. 28th IEEE International Conference on Advanced Information Networking and Applications Workshops, May*; 2014:245-250.
161. Zaier R, Zekri S, Jayasuriya H, Teirab A, Hamza N, Al-Busaidi H. *Design and implementation of smart irrigation system for groundwater use at farm scale. 7th International Conference on Modelling, Identification and Control (ICMIC), December*; 2015:1-6.
162. Atoev S, Kwon KR, Lee SH, Moon KS. *Data analysis of the MAVLink communication protocol. IEEE International Conference on Information Science and Communications Technologies (ICISCT), November*; 2017:1-3.
163. Rodrigues AV, Carapau RS, Marques MM, Lobo V, Coito F. *Unmanned systems interoperability in military maritime operations: MAVLink to STANAG 4586 Bridge. IEEE OCEANS 2017—Aberdeen, June*; 2017:1-5.
164. Smigielski P, Raczynski M, Gosek L. *Visual simulator for MavLink-protocol-based UAV, applied for search and analyze task. IEEE Federated Conference on Computer Science and Information Systems (FedCSIS), September*; 2017:1177-1185.
165. Eldefrawy MH, Khan MK, Alghathbar K. *A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography. IEEE International Conference on Anti-Counterfeiting, Security and Identification, July*; 2010:1-6.
166. Adiga BS, Balamuralidhar P, Rajan MA, Shastry R, Shivraj VL. *An identity based encryption using elliptic curve cryptography for secure M2M communication. Proceedings of the First International Conference on Security of Internet of Things*. New York, NY: ACM; 2012:68-74.
167. Papanikolaou A, Rantos K, Androulidakis I. *Proxied IBE-based key establishment for LLNs. 10th IEEE International Conference on Digital Technologies (DT), July*; 2014:275-280.
168. Li F, Xiong P. Practical secure communication for integrating wireless sensor networks into the internet of things. *IEEE Sens J*. 2013;13(10):3677-3684.
169. Saied YB, Olivereau A, Zeghlache D, Laurent M. Lightweight collaborative key establishment scheme for the internet of things. *Comput Netw*. 2014;64:273-295.
170. Garcia-Morchon O, Keoh SL, Kumar S, Moreno-Sanchez P, Vidal-Meca F, Ziegeldorf JH. *Securing the IP-based Internet of Things with HIP and DTLS. Proceedings of the 6th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. New York, NY: ACM; 2013:119-124.
171. Petroulakis NE, Tragos EZ, Fragkiadakis AG, Spanoudakis G. A lightweight framework for secure life-logging in smart environments. *Inf Secur Techn Rep*. 2013;17(3):58-70.
172. Sciancalepore S, Capossele A, Piro G, Boggia G, Bianchi G. *Key management protocol with implicit certificates for IoT systems. Proceedings of the 2015 Workshop on IoT Challenges in Mobile and Industrial Systems*. New York, NY: ACM; 2015:37-42.
173. Liu J, Xiao Y, Chen CLP. *Authentication and access control in the Internet of Things. 32nd IEEE International Conference on Distributed Computing Systems Workshops, June*; 2012:588-592.
174. Ndibanje B, Lee H-J, S-G L. Security analysis and improvements of authentication and access control in the internet of things. *Sensors*. 2014;14(8):14786.
175. Pereira PP, Eliasson J, Delsing J. *An authentication and access control framework for CoAP-based Internet of Things. 40th IEEE Annual Conference of the IEEE Industrial Electronics Society (IECON), October*; 2014:5293-5299.
176. Jan Mian A, Nanda P, He X, Tan Z, Liu RP. *A Robust Authentication Scheme for Observing Resources in the Internet of Things Environment. 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), September*; 2014:205-211.
177. Kothmayr T, Schmitt C, Hu W, Brunig M, G C. DTLS based security and two-way authentication for the internet of things. *Ad Hoc Netw*. 2013;11(8):2710-2723.
178. Turkanović M, Brumen B, Holbl M. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion. *Ad Hoc Netw*. 2014;20:96-112.

179. Lee JY, Lin WC, Huang YH. *A lightweight authentication protocol for Internet of Things*. *IEEE International Symposium on Next-Generation Electronics (ISNE), May*; 2014:1-2.
180. Yohan A, Lo N-W, Randy V, Chen S-J, Hsu M-Y. *A novel authentication protocol for micropayment with wearable devices*. *Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication*. New York, NY: ACM; 2016:18:1-18:7.
181. Kanuparthi A, Karri R, Addepalli S. *Hardware and embedded security in the context of Internet of Things*. *Proceedings of the ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles*. New York, NY: ACM; 2013:61-64.
182. Xu T, Wendt JB, Potkonjak M. *Security of IoT systems: design challenges and opportunities*. *IEEE/ACM International Conference on Computer-Aided Design (ICCAD), November*; 2014:417-423.
183. Aman MN, Chua KC, Sikdar B. *Position paper: Physical unclonable functions for IoT security*. *Proceedings of the Second ACM International Workshop on IoT Privacy, Trust, and Security*. New York, NY: ACM; 2016:10-13.
184. Rose GS. *Security meets nanoelectronics for Internet of Things applications*. *Proceedings of the 26th Edition on Great Lakes Symposium on VLSI*. New York, NY: ACM; 2016:181-183.
185. Babar S, Stango A, Prasad N, Sen J, Prasad R. *Proposed embedded security framework for Internet of Things (IoT)*. *2nd IEEE International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology, February*. IEEE; 2011:1-5.
186. Aysu A, Ghalaty NF, Franklin Z, Yali MP, Schaumont P. *Digital fingerprints for low-cost platforms using MEMS sensors*. *Proceedings of the Workshop on Embedded Systems Security*. New York, NY: ACM; 2013:2:1-2:6.
187. Yan Y, Hu RQ, Das SK, Sharif H, Qian Y. An efficient security protocol for advanced metering infrastructure in smart grid. *IEEE Netw*. 2013;27(4):64-71.
188. Lee YS, Alasaarela E, Lee H. *Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system*. *IEEE International Conference on Information Networking (ICOIN), February*; 2014:453-457.
189. Picazo-Sanchez P, Tapiador JE, Peris-Lopez P, Suarez-Tangil G. Secure publish-subscribe protocols for heterogeneous medical wireless body area networks. *Sensors*. 2014;14(12):22619.
190. Liu Z, Huang X, Hu Z, Khan MK, Seo H, Zhou L. On emerging family of elliptic curves to secure Internet of Things: ECC comes of age. *IEEE Trans Depend Secure Comput*. 2016;PP(99):1-1.
191. Seo H, Choi J, Kim H, Park T, Kim H. *Pseudo random number generator and hash function for embedded microprocessors*. *IEEE World Forum on Internet of Things (WF-IoT), March*; 2014:37-40.
192. Vinayaga SB, Ramnath M, Prasanth M, Sundaram V. *Encryption and Hash based security in Internet of Things*. *3rd International Conference on Signal Processing, Communication and Networking (ICSCN), March*; 2015:1-6.
193. Yu W, Kose S. A lightweight masked AES implementation for securing IoT against CPA attacks. *IEEE Trans Circ Syst I*. 2017;PP(99):1-11.
194. Sundaresan S, Doss R, Piramuthu S, Zhou W. Secure tag search in RFID systems using mobile readers. *IEEE Trans Depend Secure Comput*. 2015;12(2):230-242.
195. Fotiou N, Kotsonis T, Marias GF, Polyzos GC. *Access control for the Internet of Things*. *IEEE International Workshop on Secure Internet of Things (SIoT), September*; 2016:29-38.
196. Beltran V, Martinez JA, Skarmeta AF. *User-centric access control for efficient security in smart cities*. *IEEE Global Internet of Things Summit (GIoTS), June*; 2017:1-6.
197. Haripriya AP, Kulothungan K. *ECC based self-certified key management scheme for mutual authentication in Internet of Things*. *IEEE International Conference on Emerging Technological Trends (ICETT), October*; 2016:1-6.
198. Pinol OP, Raza S, Eriksson J, Voigt T. *BSD-based elliptic curve cryptography for the open Internet of Things*. *7th IEEE International Conference on New Technologies, Mobility and Security (NTMS), July*; 2015:1-5.
199. Zhu X, Badr Y, Pacheco J, Hariri S. *Autonomic identity framework for the internet of things*. *International Conference on Cloud and Autonomic Computing (ICCAC), September*; 2017:69-79.
200. Pacheco J, Zhu X, Badr Y, Hariri S. *Enabling risk management for smart infrastructures with an anomaly behavior analysis intrusion detection system*. *2nd IEEE International Workshops on Foundations and Applications of Self* Systems (FAS*W), September*; 2017:324-328.
201. Nakagawa I, Shimojo S. *IoT agent platform mechanism with transparent cloud computing framework for improving IoT security*. 41st IEEE Annual Computer Software and Applications Conference (COMPSAC), July. ; 2017:684-689.
202. Kobayashi G, Broens MC, Gonzalez MEQ, Quilici-Gonzalez JA. *The Internet of Things and its impact on social relationships involving mutual trust*. *IEEE International Symposium on Technology and Society (ISTAS), November*; 2015:1-6.
203. Chang Y-A, Chen M-S, Wu J-S, Yang B-Y. *Postquantum SSL/TLS for embedded systems*. *7th IEEE International Conference on Service-Oriented Computing and Applications, November*; 2014:266-270.
204. El Zouka Heshem A, Hosni Mustafa M. *On the power of quantum cryptography and computers*. *3rd IEEE International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), April*; 2014:58-63.
205. Shaowu M, Huanguo Z, Wanqing W, Jinhui L, Shuanbao L, Houzhen W. A resistant quantum key exchange protocol and its corresponding encryption scheme. *Commun China*. 2014;11(9):124-134.

How to cite this article: Samaila MG, Neto M, Fernandes DAB, Freire MM, Inácio PRM. Challenges of securing Internet of Things devices: A survey. *Security and Privacy* 2018;1:e20. https://doi.org/10.1002/spy2.20