Systematic Review of Existing IoT Architectures Security and Privacy Issues and Concerns

Fatma Alshohoumi[1], Mohammed Sarrab[2], Abdulla AlHamadani[3], Dawood Al-Abri[4]
Communication and Information Center, Sultan Qaboos University, Muscat, Oman[1, 2]
Computer Science department, Sultan Qaboos University, Muscat, Oman[3]
Electrical & Computer Engineering Department, Sultan Qaboos University, Muscat, Oman[4]

Abstract*—Internet of things (IoT) has become one of the most prominent technologies that the world has been witnessing nowadays. It provides great solutions to humanity in many significant fields of life. IoT refers to a collection of sensors or object in the universe with the capability of communicating with each other through the internet without human intervention. Currently, there is no standard IoT architecture. As it is in its infancy, IoT is surrounded by numerous security and privacy concerns. Thus, to avoid such concerns that may hinder its deployment, an IoT architecture has to be carefully designed to incorporate security and privacy solutions. In this paper, a systematic literature review was conducted to trace the evolvement of IoT architectures from its initial development in 2008 until 2018. The Comparison among these architectures is based on terms of the architectural stack, covered issues, the technology used and considerations of security and privacy aspects. The findings of the review show that the initial IoT architectures did not provide a comprehensive meaning for IoT that describe its nature, whereas the recent IoT architectures convey a comprehensive meaning of IoT, starting from data collection, followed by data transmission and processing, and ending with data dissemination. Moreover, the findings reveal that IoT architecture has evolved gradually across the years, through improving architecture stack with new solutions to mitigate IoT challenges such as scalability, interoperability, extensibility, management, etc. with lack consideration of security solutions. The findings disclose that none of the discussed IoT architectures considers privacy concerns, which indeed considered as a critical factor of IoT sustainability and success. Therefore, there is an inevitable need to consider security and privacy solutions when designing IoT architecture.

Keywords—Internet of things; IoT architecture stack; IoT layers; IoT privacy concerns; IoT security

I. Introduction

Recently, new technology has emerged with a number of solutions to facilitate the way of interacting with any object in the world. The promising technology of the Internet of Things (IoT) offers many attractive and useful solutions to help improve communication with everything in the surrounding world. IoT assists people to interact with objects as a new paradigm of communication. This technology promises that the things around us will become smarter and more intelligent. Therefore, the technology of IoT is a recent communication paradigm that is highly integrated into our daily life, providing various applications that can change our lifestyle by making it easier, safer, and smarter [1], [2]. Although many definitions for IoT have been derived by scholars, so far, there is no standard definition for IoT [3]–[5]. The essence of IoT is that all things surrounding us can connect to the Internet and exchange data anywhere and at any time [6], [7].

The Internet of Things (IoT) will play an essential role in many aspects of our daily life. This technology was designed to tackle problems that arise because people have limited time, attention and accuracy when collecting data from things in the real world. The primary aim of IoT is to simplify our daily lives and mutate our way of accomplishing or fulfilling duties [8]–[10]. IoT can be employed to improve many important fields (e.g. healthcare, automobiles, entertainments, industrial appliances, sports, homes, transportations, smart grids, and intelligence systems) [7], [11], [12]. Furthermore, it can be used in the food industry, restaurants, logistics, tourism, travel, and library services [13], [14]. In addition, it can be useful for improving the governmental services provided for citizens, such as e-participation, e-aging, disabled people, etc. [10]. Technology reports on IoT show a dramatic change in the way we work and live due to the impact of IoT on industry and society [2]. The potential economic impact of IoT and its supporting technologies is estimated to reach a price ranging from $3.9 trillion to $11.1 trillion a year by 2025 [15]. It provides great benefits, including home monitoring, health monitoring, agriculture monitoring, energy monitoring and control, environmental monitoring, smart education, smart security, etc. [16]. The future will witness many smart applications in different fields. IoT will offer potential value to the consumers. For example, in smart automobiles, IoT can be used to detect the traffic jam on the road and notify the driver to take a decision to avoid any inconvenience that can occur due to traffic jam [17]. The most beneficial value gained from IoT is when it is used in critical fields, such as in predicting natural disasters. In this case, the sensors and autonomous simulations can predict the occurrence of earth-slides and other disasters. Furthermore, according to such detection, appropriate action can be taken in advance. Another important field that IoT can offer significant value to is an industry. For example, IoT can assist in the management of a fleet of cars for an organization, monitor their performance and detect which one needs maintenance. A significant application can be seen in monitoring water scarcity, where an IoT device can detect scarcity in different locations and can alert users if an upstream incident occurs as well, such as an unintentional release of sewage into the stream, which has dangerous implications. In addition, an appreciable advantage of IoT can be noticed when monitoring patients and saving their lives. Agriculture and other important fields can utilize IoT to perform accurate tasks

[18]. Moreover, IoT provides a benefit for waste management, which is an issue in modern cities. In these regards, an intelligent waste container can be used to detect or sense the level of load and, thus, allow for optimizing the route of the collector trucks, which can help in reducing the cost of waste collection and improving the quality of recycling [19]. Furthermore, smart cities utilize IoT to improve their infrastructure, keep people safe, engage more residents, improve public transportation, etc. Cities become smarter by means of IoT when all critical systems, including transportation systems, healthcare systems, and weather monitoring system, are connected [1]. When cities become smart, numerous benefits can be gained in the management and optimization of services, such as transport, parking, lighting, surveillance, maintenance of the public area, garbage collection, etc. [20].

Although IoT offers a range of significant and substantial solutions to the world, many challenges can stand a hindrance toward the success of IoT. These challenges, as mentioned in the surveys of [18], [21]–[24], are related to the scalability issues, data volumes, data interpretation, interoperability, fault tolerance, power supply, wireless communication, privacy, and security, etc. However, to date, security and privacy are considered the topmost challenges that need to be addressed, as they are considered a complementary requirement for IoT development [25], [26]. In 2013, the first IoT botnet was discovered, and according to a researcher at the Proof point, more than 25% of the botnet was created on IoT devices, including smart TVs, baby monitor, cameras, home appliances, etc. [27]. Security concerns may occur at any level of IoT, such as at the front-end sensors and devices, network, and at the back-end of IT systems [28]. Also, the privacy of users may be exposed as a result of serious breaches of users' sensitive information, which may occur in devices, storage, during communication and at processing [29]. Therefore, users' privacy has to be preserved using techniques, in order to protect the device privacy, as in [30], [31], during communication through using [32], at storage using [33], and at processing using [34]. To address these two challenges, the environment of IoT must be well-studied and analyzed from different aspects, like IoT architectures, consumers' needs, stakeholder's requirements, technologies used, and other aspects. In this paper, a systematic review was conducted to study the existing IoT architectures in terms of layers' classification and the considerations of security and privacy in IoT architectures.

The remaining paper is organized as follows: Section 2 presents the research methodology that is used to achieve the objectives of this research. Section 3 introduces background details related to IoT history, privacy and security concerns in IoT. Section 4 surveys the existing IoT architectures. Section 5 provides the discussion of IoT architectures in terms of the consideration of privacy and security, covered the issue in architecture with techniques used, architectural stack (the number of architectural layers). Section 6 concludes the conducted review.

II. Research Methodology

The paper provides a systematic literature review to study the existing IoT architectures. Precisely, the systematic literature review provides a comparison between sixteen of the existing IoT architectures that were developed between 2008 and 2018 [5], [18], [43], [35]–[42]. To accomplish the systematic literature review, the methodology of this study is divided into steps, as depicted in Fig. 1.

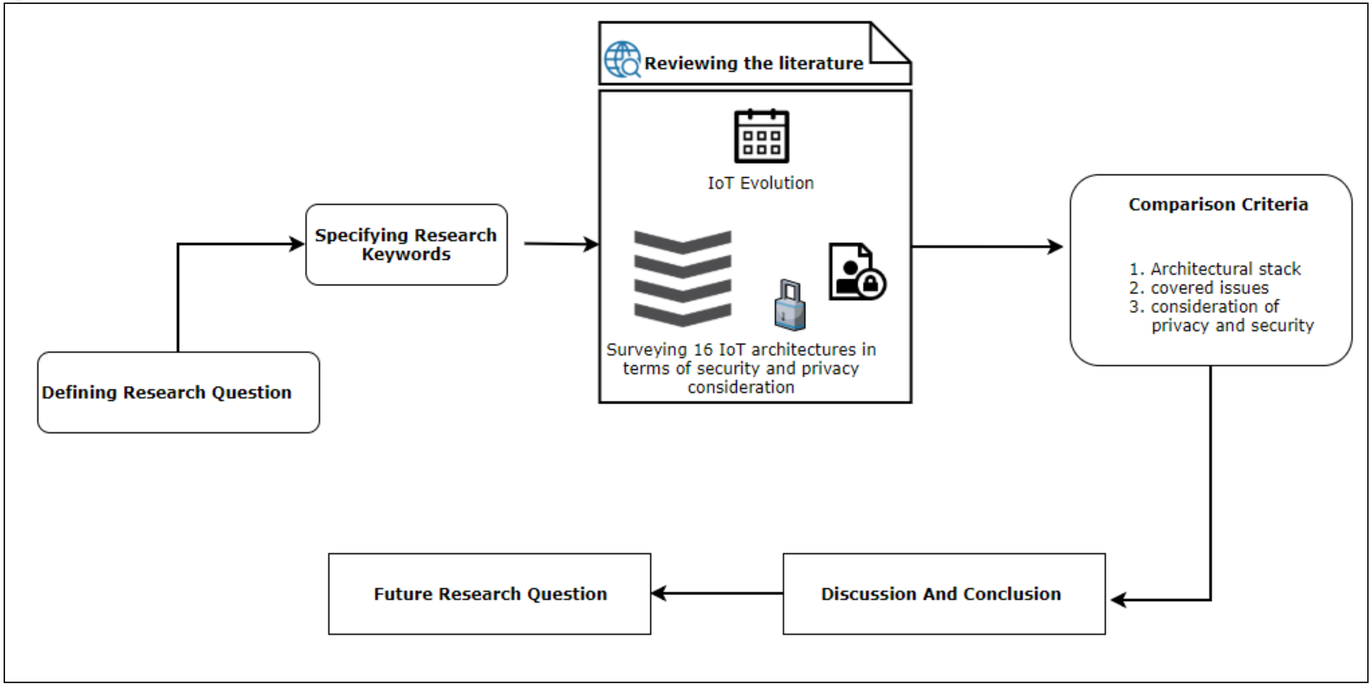
Reviewing the literature
IoT Evolution
Surveying 16 IoT architectures in terms of security and privacy consideration
Specifying Research Keywords
Defining Research Question
Comparison Criteria
1. Architectural stack
2. covered issues
3. consideration of privacy and security
Discussion And Conclusion
Future Research Question

Fig. 1. Methodology of the Systematic Review Study on the Existing IoT Architectures.

As shown in Fig. 1, the methodology of this study is divided into the following steps:

- Defining the research question.
- Specifying research keywords.
- Reviewing the literature.
- Specifying comparison criteria.
- Discussions and findings.

A. Research Questions

The aim of this research is to study and compare the existing IoT architectures in terms of the architectural stack, covered issues, and consideration of security and privacy aspects. The systematic review aims to address the following research questions:

1) Is there a standard IoT architecture? To answer this question, the researcher studied all the existing sixteen IoT architectures that were proposed during the period 2008 and 2018. This research question was divided into the following sub-questions.

- What are the IoT architecture layers or stack?
- Do all layers provide the same meaning for describing IoT?
- Do the existing IoT architectures thoroughly provide a complete meaning to IoT nature?

2) Are security and privacy considered as essential components of the IoT architecture? To answer this question, the focus was on studying the security and privacy in each of the selected IoT architectures. This question was divided into the following sub-questions:

- What are the issues that IoT architectures covered and the used techniques?
- Are security and privacy aspects implemented in IoT architectures?
- What are the open research questions related to the IoT architectures, as well as the security and privacy aspects?

B. Research Keywords

The research keywords were extracted from the research questions. Table 1 presents the research keywords, which were used for searching the resources, used in this paper.

TABLE I. RESEARCH KEYWORDS

No.	keywords
1	"IoT architecture"; "internet of things architecture"
2	"IoT layers"; "internet of things layers"
3	"IoT privacy"; "Internet of things privacy"
4	"IoT security"; "Internet of things security"

The search strings S1 and S2 are formed as a disjunction of the first two lines, and a conjunction of the disjunction of the last three lines of the specified keywords:

S1=: L1 OR L2 AND (L3 OR L4)

S2=: L1 OR L2 AND (L3 AND L4)

In addition, each line represents a disjunction of its selected keywords, e.g. L2 =: {IoT layers OR internet of things layers}.

C. Reviewing the Literature

In this systematic literature review, 148 resources from different online databases were used. Most of the research papers used in this review were found on google scholar, IEEE, Future Generation Computer System, ICCCN, ICICTA, IEEE Xplore, ACM, COMNET, and other databases. The selection of the architectures was based on the year that the architecture was developed in, starting from the first IoT architecture, which was proposed in 2008, and covering all the IoT architectures that were proposed until 2018. Each of the selected IoT architecture was comprehensively studied and classified according to the number of IoT layers as:

1) Three-layer IoT architecture
2) Four-layer IoT architecture
3) Five-layer IoT architecture

D. Specifications of the Comparison Criteria

Use The selected IoT architectures have been studied, and a comparison between these architectures was conducted in terms of the number of IoT layers in each architecture, their architectural stack, and whether the architecture has considered security and privacy aspects.

1) Architecture stack (IoT layers): each architecture consists of layers that are used for describing the complete nature of IoT, starting from data collection and ending with data presentation. This criterion is used because the main components of IoT architectures are the layers that cover a subset of the required IoT functionalities or processes.

2) Covered issues and challenges: This criterion is used to show how the IoT architecture evolves over the years, and to highlight what each architecture address.

3) The technique used: This criterion is used to present the technology used for addressing the IoT challenges to improve IoT architecture.

4) Security: This criterion is very crucial because security in IoT is considered the key driver for IoT success. Thus, security should be considered in IoT architecture.

5) Privacy: This criterion has received most of the attention so far, because it touches IoT users and, thus, leads to the acceptance of IoT among users. The ways on how to preserve users' privacy must be considered in IoT architectures.

III. BACKGROUND AND OVERVIEW

A. History of the Internet of Things

The idea of connecting devices together has been around since the 1980s. Then, the concept changed to the terms of embedded computing and persuasive computing. In the early

80s, the first example of the Internet of Things appeared as a Coca-Cola machine, which was located at Carnegie Melon University. This machine had the ability to count the number of drinks left, and measure whether they are cold enough or not [44]. During the period between 1980 to 1990, many companies in America and Europe focused on manufacturing radio frequency identification (RFID) tags. Essentially, an RFID tag was used to identify an object. In the same period, this technology of object identification (RFID) was deployed for automatic toll payment application [45]. Moreover, the 1990s witnessed the great movement of shifting from machine-to-machine (M2M) to wireless technology [46]. Global Positioning Satellites (GPS) begun to be used in 1993 [47]. This technology was used to determine the location of an object. In 1998, the use of the term Internet of Things was presented by Kevin Ashton [5], [48]. The year 1999 was called the big year of this new term when the British technology pioneer Kevin Ashton (executive director of auto-ID center) coined the new term as the Internet of Things (IoT), which started gaining more popularity in academia and industry [44], [49], [50]. In 2000, the first Internet-connected refrigerator was announced by LG [44]. In the years of 2003 and 2004, the IoT-supporting technology of RFID was extensively used by Walmart and the US Department of Defense [44]. Moreover, in the same years, the IoT term had appeared in well-known publications like the Guardian, Scientific American and the Boston Globe. In 2005, ITU-T published the first article on IoT [51]. IoT was recognized by the EU in the period between 2006-2008, and accordingly, the first European IoT conference was held [52]. The statistics shown by Cisco Internet Business Solutions Group (IBSG) confirm that IoT was born between 2008 and 2009, due to the increase in the number of things or objects that were connected to the internet, which exceeded the number of people. In 2010, China considered IoT a key industry and made plans to focus its investment on it. Furthermore, IPv6 was launched in 2011 with the capability of providing 2^{128} addresses, which is sufficient to address every atom on earth [53]. The IPv6 protocol can be used in IoT. In 2012, the technology of mobile computing became popular and used in IoT development. As the number of connected IoT devices increased, many challenges emerged and many solutions were introduced such as IoT platforms. Most of Known IoT platforms were launched in 2013 [54]. Many of proprietary and open source platforms were introduced to accelerate IoT development. In the same year, an IoT group was created by Intel company, and later, in 2015, an operating system for IoT called Brillo was developed by Google [44]. Subsequently, a drastic change was noticed in the way people perceive the promising technology due to the major evolution in technologies, such as embedded systems. As a result, billions of IoT devices were connected to the Internet. In this regard; Statista (the statistics portal), which presents statistics and studies from more than 22,500 sources, expected that the number of connected IoT devices to reach 30.73 billion devices by 2020, and 75.44 billion by 2025 [55], [56]. IDC estimated that global IoT spending will reach $1.29 trillion by 2020 [57], [58]. In [59] authors predicts that the number of connected cameras to the internet will reach 100 billion in 20130 (Internet of video things). Fig. 2 illustrates the history and evolution of IoT.

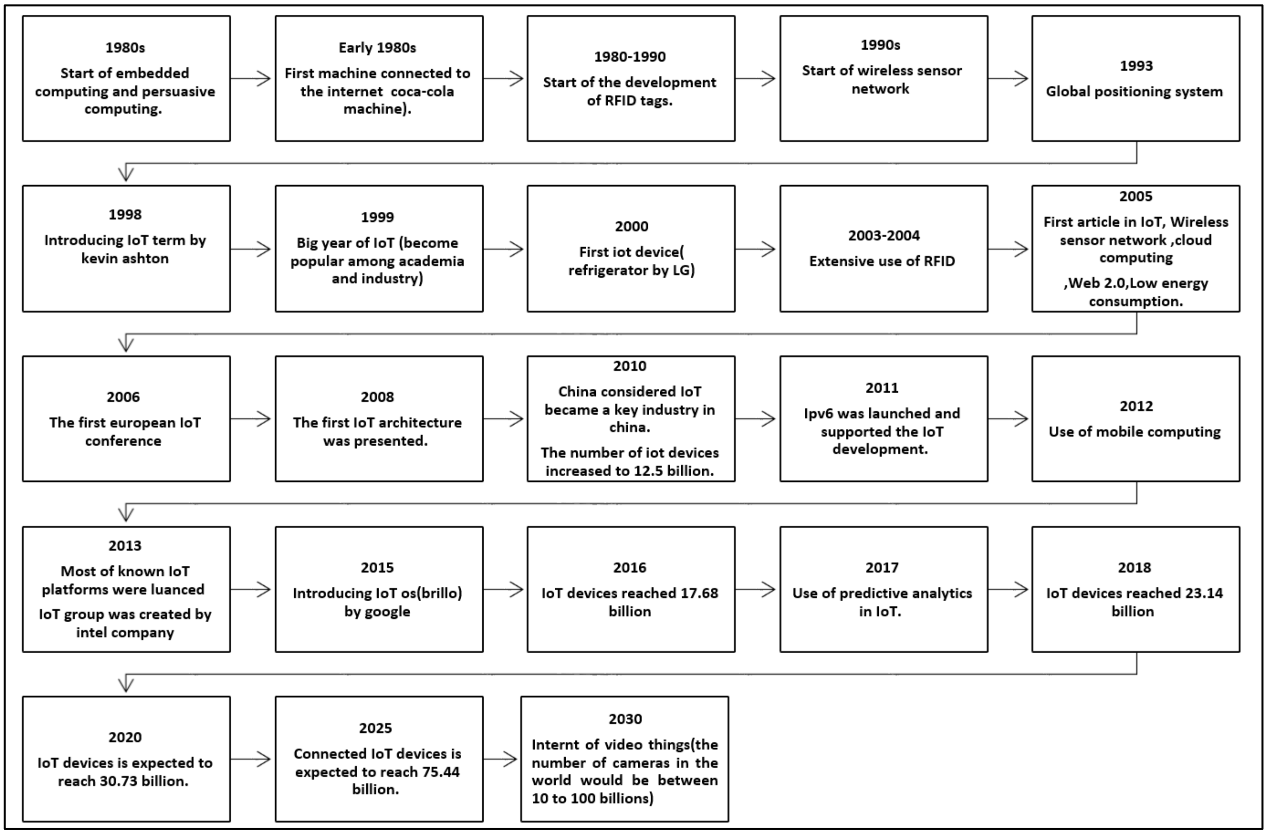
1980s
Start of embedded computing and persuasive computing.
Early 1980s
First machine connected to the internet coca-cola machine).
1980-1990
Start of the development of RFID tags.
1990s
Start of wireless sensor network
1993
Global positioning system
1998
Introducing IoT term by kevin ashton
1999
Big year of IoT (become popular among academia and industry)
2000
First iot device(refrigerator by LG)
2003-2004
Extensive use of RFID
2005
First article in IoT, Wireless sensor network ,cloud computing
,Web 2.0,Low energy consumption.
2006
The first european IoT conference
2008
The first IoT architecture was presented.
2010
China considered IoT became a key industry in china.
The number of iot devices increased to 12.5 billion.
2011
Ipv6 was launched and supported the IoT development.
2012
Use of mobile computing
2013
Most of known IoT platforms were luanced
IoT group was created by intel company
2015
Introducing IoT os(brillo) by google
2016
IoT devices reached 17.68 billion
2017
Use of predictive analytics in IoT.
2018
IoT devices reached 23.14 billion
2020
IoT devices is expected to reach 30.73 billion.
2025
Connected IoT devices is expected to reach 75.44 billion.
2030
Internt of video things(the number of cameras in the world would be between 10 to 100 billions)

Fig. 2. Summary of IoT History and Evolution.

As presented in Fig. 2. IoT has been gradually evolving due to the development of many technologies, such as RFID, wireless sensor network, global positioning system, cloud computing, web 2.0, low energy communication, IPv6, mobile computing, analytics systems, and other new technologies. The analysis of IoT history also shows that the number of IoT devices has increased in recent years, and is expected to rise sharply in the coming years, which indicates that IoT will intervene in every corner of our life.

B. Internet of Things Definition

At present, there is no standard definition accepted for IoT, as it is still in its formation process [5], [50]. A lot of communities and organizations defined IoT according to their perspectives. RFID community defined IoT as things-oriented in which tags are a thing [60]. They defined IoT as; "the worldwide network of interconnected objects uniquely addressable based on standard communication protocols" [6], [61]. Another definition was formed by the European Research Cluster of IoT (IERC), in which they defined IoT as; "The Internet of Things allows people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path/network, and any service" [6], [62]. The International Telecommunication Union (ITU) defined IoT as; "From anytime, anyplace connectivity for anyone, we will now have connectivity for anything" [6], [63].

Through the concept of the Internet of Things, things in the world can integrate and communicate with each other, in order to serve humans in their daily lives. Generally, the Internet of Things (IoT) refers to collections of various sensors, objects, and smart nodes, which have the capability to communicate with each other, without any intervention from people [11]. More specifically, it involves connecting any device that has the feature of switching off or on through the internet. To be more specific, it includes everything, such as cell phones, headphones, washing machines, lamps, wearable devices, and an electronic device that anyone can think of [17]. IoT provides devices with the capability to sense (think, see, and hear) from the environment and make a decision [64], [65]. A device can be considered as a node in the IoT, therefore, each node has the ability to transfer lightweight data, access and authorize cloud-based resources for the purpose of collecting, extracting data and making decisions through the analysis of the collected data [11].

C. Nature of the Internet of Things

The main purpose of IoT is to facilitate the process of exchanging information among things and retrieving useful knowledge from the exchanged information [5]. The great value of IoT is to improve the services of collecting, analyzing, and extracting knowledge for different purposes. To perform these services, IoT should possess three main characteristics, which are; comprehensive perception, reliable transmission, and intelligent processing [66], [67]. Comprehensive perception involves diverse devices, such as sensors and RFID, to obtain information from any object, anywhere and at any time. The reliable transmission includes a variety of wired and wireless networks that are used for data transmission. Intelligent processing is about having technologies like cloud computing, which is used for storing and processing the obtained data by sensors [67]. In order to make this new technology a reality, many related technologies support the evolution of IoT, such as wireless sensor networks, cloud computing, communication networks, mobile technologies, identification technologies, big data, security and privacy technologies, distributed computing, and fog computing [1]. Mainly, the IoT environment relays on the internet, mobile communication networks and wireless sensor networks [68]. IoT can benefit from the unlimited capabilities of cloud computing, which are mainly used for the storage and processing of data [69]. Cloud computing can also enable data collection, accelerate the setup and integration of new things, and reduce the cost of deployment [70]. Big data technology can be utilized in IoT where the collected data from sensors can be analyzed to give a better understanding of the physical world[71]. Since IoT is susceptible to attacks like Denial of Service attack(DoS), Distributed Denial of Service attack(DDOS), compromised nodes, and malicious code hacking attacks, specific security technologies, such as homomorphic and searchable encryption, can be used to make IoT secured [1], [72]. IoT is related to a distributed computing technology where the Internet can extend into the real world to connect everyday objects [73]. In addition, IoT is related to fog computing technology where computing, storage, control, and networking power can be placed anywhere, for example in data centers, cloud, edge devices, sensors, and gateways [74], [75]. Furthermore, Nanotechnology is also related to IoT, where Nano-devices can be integrated with the communication network and with the Internet to form the Internet of Nano things [76]. Fig. 3 depicts IoT and related technologies.

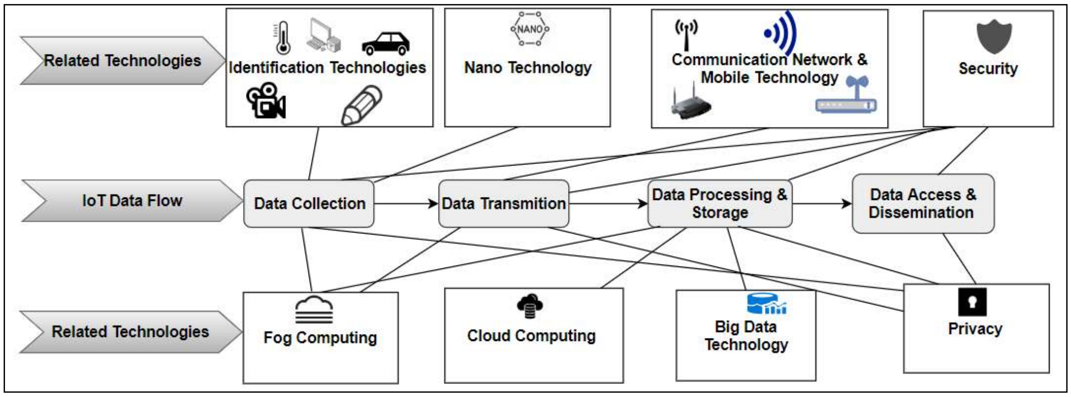

Fig. 3. IoT and Related Technologies.

As mentioned earlier, IoT provides some useful benefits, such as home monitoring, health monitoring, agriculture monitoring, energy monitoring and control, environmental monitoring, smart education, smart security, etc. [77], [78]. Regardless of the great benefits offered by IoT, many challenges and concerns hinder its development and success [24], [79]. Some surveys, such as the surveys of [18], [21]–[24], [80], were conducted to discuss the challenges of IoT. Nevertheless, to date, security and privacy concerns are the major challenges [25], [26], [81] that scholars are paying more attention to, in order to discuss and address the IoT challenges.

D. Security and Privacy in the Internet of Things

Security and privacy requirements for IoT are essential for mitigating failures and ensuring the acceptance of IoT by customers [82]. Some researchers consider privacy as part of security issues [11], [83], [84]. Indeed, there is a noticeable difference between the terms of privacy and security [85]. Security deals with securing the privacy of data, data through communication, data at storage, data at processing, and securing the access of data [11], [86]. Many security issues are threatening IoT, including vulnerabilities and attacks. For example, the first IoT worm detected in 2013 was called Linux. Darlloz, with the capability of attacking devices like home routers, CCTV, cameras, and other small Internet-enabled devices [87]. During the period from December 23rd, 2013 to January 6th, 2014, another incident attack was detected in smart devices like refrigerators and televisions. These smart devices were hacked to send more than 750,000 spam and phishing emails to individuals [43]. In 2016, the distributed denial-of-service attack took place by exploiting the unaltered default password across a large number of IoT devices [88], [89]. Therefore, the security notion aims to avoid threats that compromise IoT systems and affect the confidentiality, authority, authenticity, integrity, and availability of IoT systems [90]. Various security mechanisms exist to defend various security issues in all IoT layers, as discussed in [1], [43]. Thus, security can be defined as a structured framework composed of policies, procedures, techniques, and measures required to protect the assets of individuals and the systems against threats that may occur deliberately or unintentionally. In other words, security can be defined as a concept that attempts to protect data and devices from external attacks, spyware, and subversion [83].

Whereas security is more concerned about securing data, privacy is more related to people and their data, especially data with a high degree of sensitivity [83]. It is believed that every person should have the right to control his/her private data[62]. The term of information privacy or data privacy was known since the 1960s, due to the increase of electronic data processing [91]. Privacy was defined as "the right to be let alone", by Warren and Brandeis in 1890, in his article of 'The Right to privacy' [92]. Then, privacy was defined by Westin as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others", in his book "Privacy and Freedom" [93]. From the previously mentioned definitions, privacy can be summarized as the release of information in a controlled way. It involves the concealment of personal information and the ability to control personal data [94]. To be more specific, privacy means that the person has the right to determine the level of his/her interaction with the environment, or the amount of data that can be viewed for the public [28], [62], [83]. Weak security measures in IoT devices lead to privacy breaches and safety threats in the real world [95]. There are large overlaps and intersections between security and privacy concepts, but there is a notable difference between the terms, as Fig. 4, illustrates [83]. Generally, the manufacturers of IoT concentrate and care about hardware security more than they care about users' privacy [83].

IoT devices can leak sensitive information, as shown by recent studies [96]. For example, the data collected by smart switches, smart thermostats, and smart power meters can leak information, including information about whether a home is being occupied [97], [98]. Furthermore, IoT devices (e.g. rooftop solar panels) can reveal home location [99], [100]. In solar energy analytics, energy data can leak location information, which may cause location-based privacy attacks [96]. In critical fields (military, as an example), the privacy threat is very dangerous, because IoT devices can leak sensitive information that the enemy can exploit. For instance, Strava fitness app posts a map of its users' activity on the internet. Security researchers showed that this public activity map imposes a severe threat to the U.S national security by indirectly revealing the locations and behaviors or attitudes of the U.S military bases and personnel in Syria and Iraq [96], [101]. In healthcare, many IoT applications were developed to serve this sector, including apps used for sensing glucose level, monitoring blood pressure, monitoring ECG, etc.[102]. These applications are exposed to attacks and vulnerabilities [103]. In IoT devices, such as an insulin pump that was manufactured by Medtronic company, the system does not provide adequate security to the command sent to the pump by patients. This lack of security leads to serious privacy issues. Some of these issues are revealing patient's information by third parties, intercepting commands and replacing them, and threatening patients' lives by delivering a fatal insulin dose to the patient as well [104]. In smart cars, vulnerabilities have been found, and they can threaten people's lives. Tesla Model S was hacked by security researchers at a keen security lab, through disrupting all the car features, such as brakes, the door lock, disclosing locations and controlling computer screen from a distance of 12 miles [104]. For this reason, taking IoT privacy into consideration leads to gaining wider acceptance of IoT by customers and, thus, leads to IoT success [82]. In order to mitigate security and privacy issues in IoT, IoT architectures have to be investigated and studied. The following section surveys the existing IoT architectures in terms of considering privacy and security aspects, and the number of IoT architectural layers.

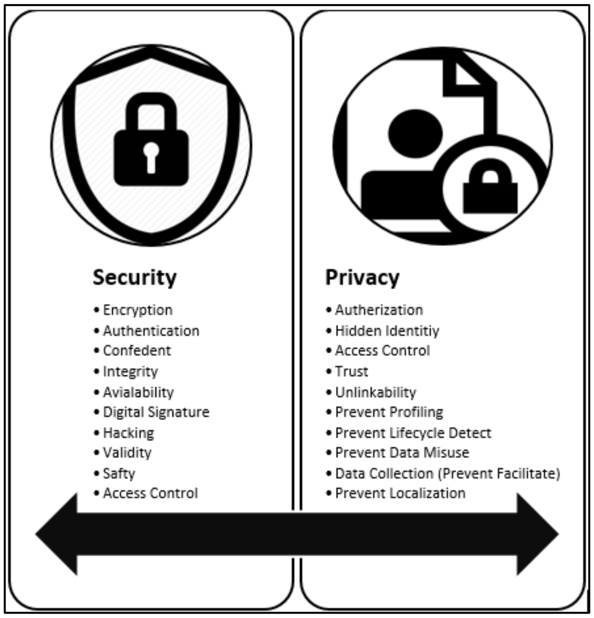

Fig. 4. Difference between Security and Privacy.

IV. Existing Internet of things Architectures

Many architectures have been proposed for IoT technology. An architecture helps to understand the nature of IoT and study all the issues that may threaten the promising technology. This section discusses the existing IoT architectures until 2018.

A. *IoT Architecture in 2008*

In 2008, Pereira [41,123] proposed a five-layer architecture for IoT, which is shown in Fig. 5.

It consists of five layers; named as the edge layer, the access gateway layer, the internet layer, the middleware layer, and the application layer. The edge layer involves all embedded systems, like RFID (Radio Frequency Identification), or sensors that are used for sensing the environment around us. The access gateway layer acts as a cross-platform communication that deals with message routing, publishing and subscribing to the layer above (middleware layer) through the internet layer. Middleware layer acts as the interface between the edge layer and the application layer, and it is responsible for managing information and devices. The topmost layer, the application layer, offers different services from the collected data in the edge layer to various consumers. These applications cover various industries including, but not limited to, food & drug, healthcare, retail, logistics, and public safety.

B. *IoT Architecture in 2010*

At this stage of IoT development, each application system worked alone, in which an object only communicates with another object in the same application system. As a result, the interoperability issues were common due to the lack of global standards. To solve such issues, Tan in [41] proposed a new layer called the coordination layer.

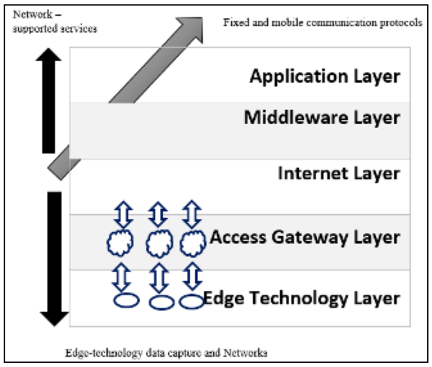

Fig. 5. Five-Layer IoT Architecture [35], [105].

The new layer performs the tasks of restructuring the packages from different application systems and reassembling them in order to form a unified structure that can be recognized and processed by the application system. Due to the nature of IoT, many objects communicate with each other and can generate massive data that leads to an exponential increase in the traffic and storage, which subsequently, creates a number of issues to be solved. To deal with traffic and storage issues, Lu et al. proposed the backbone network layer [35].

In the same year, a three-layer architecture of IoT was proposed by Miao et al. It consisted of three layers see Fig. 7, a perception layer at the bottom, an application layer at the top, and a network layer positioned between the two layers. The perception layer contains all the devices that are used for identifying objects and gathering information (e.g. RFID, 2-D barcode, etc.). Furthermore, it involves the nanotechnology devices that can be used to sense data from the objects in which microdevices are implanted within. The network layer is considered the core of IoT. It has the responsibility of assigning each object a unique address and transmitting the collected data from the perception layer to the application layer in a secure way, using different protocols, such as Wi-Fi, Bluetooth, and ZigBee. The application layer takes the responsibility of managing all applications implemented or developed in IoT. The previously mentioned architecture was the accepted three-layer structure of the new technology of IoT in 2010. It helps to understand the technical structure of IoT at the initial stage of its development.

Application Layer	
Middleware Layer	
Coordination Layer	
Backbone Network Layer	
Existed alone Application system	Access Layer
	Edge Technology Layer

Fig. 6. Five-Layer IoT Architecture [35].

However, Miao et al. [5] argued that the three-layer architecture did not provide a complete understanding of IoT features and meaning. As a result, the authors proposed a new architecture, which was derived from the analysis of the technical framework of the Internet (the core of IoT), and the logic of the layered structure of the telecommunication management network (supporting the technology of IoT). The derived IoT architecture consisted of five layers as shown in Fig. 6. Starting from the bottom, these layers are the perception layer, the transport layer, the processing layer, the application layer, and the business layer. The perception layer, as in the previous three-layer architecture, is responsible for preparing the information gathered by sensors (e.g. RFID, barcodes, etc.) as digital signals to be transmitted over the network. The transport layer performs the process of transmitting the collected data through wireless or cable network technologies. Things (objects) around us generate massive data that must be managed. Therefore, unlike the previous three-layer architecture, this architecture introduced the processing layer that has the duty of storing, analyzing, and processing the information received from the transport layer. Many advanced technologies are used in this layer, including intelligent processing, cloud computing, ubiquities computing, etc. In the application layer, the processed information is utilized in offering a variety of services. The business layer was introduced in this architecture because it can be used to consume the data obtained from the application layer to build business models, graphs and flowcharts, which are useful in evaluating the new technology of IoT. The authors suggested this layer guided by the saying; "the success of the technology relies on the innovation and reasonable of business model". Furthermore, the long-term development and effectiveness of IoT can reach a peak by conducting more research on the business model [5].

C. IoT Architecture in 2011

Until 2011, security was not considered in the IoT architecture. The world today is facing a daunting challenge to deal with many security concerns (for instance, daily virus alerts, increased number of malicious crackers, and the emergence of new cyberterrorism threats). Consequently, security threats have become common, and there is an urgent need to take security requirements into consideration [124]. As any system connected to the internet, IoT devices and applications are exposed to different types of attacks. To resolve security threats in IoT, Li et al. proposed the first IoT architecture that considered security requirements and characteristics of IoT. It was a general architecture of trusted security systems based on IoT. Fig. 9, depicts the proposed architecture.

As Fig. 9, shows the architecture was built of five main components: the trusted safety management system, the security gateway, the unified service platform of IoT, the security infrastructure, and the unified information exchange platform. The trusted user module includes a trusted user authentication system based on IoT. According to this module, identity authentication makes users legitimate. A trusted perception module was designed to address security attacks that may target devices in the perception layer, such as RFID, sensors, camera, laser scanner, etc. These attacks include copying sensed information, a counterfeit of RFIDs labels, distribution of service attack (DoS), unauthorized access of users, and stealing or modifying RFID labels. Security in this layer can be achieved by applying an authentication mechanism, an access control mechanism, an encryption mechanism, and an audit mechanism. Trusted network module basically deals with the accreditation of network users. Moreover, it is responsible for security incident management, risk and strategy management, and the control of many security-related issues. The trusted terminal module deals with securing the platform technology by using encryption techniques and through securing the operating system. Li and his colleagues suggested that this architecture can help decrease the potential risks that may occur due to the access of untrusted users and terminal devices [36].

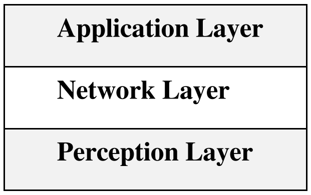

Fig. 7. Three-Layer IoT Architecture [5].

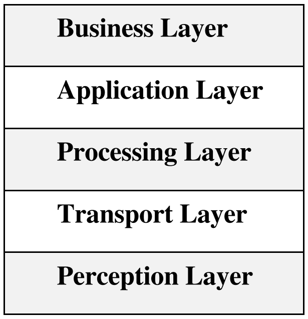

Fig. 8. Five-Layer IoT Architecture [5].

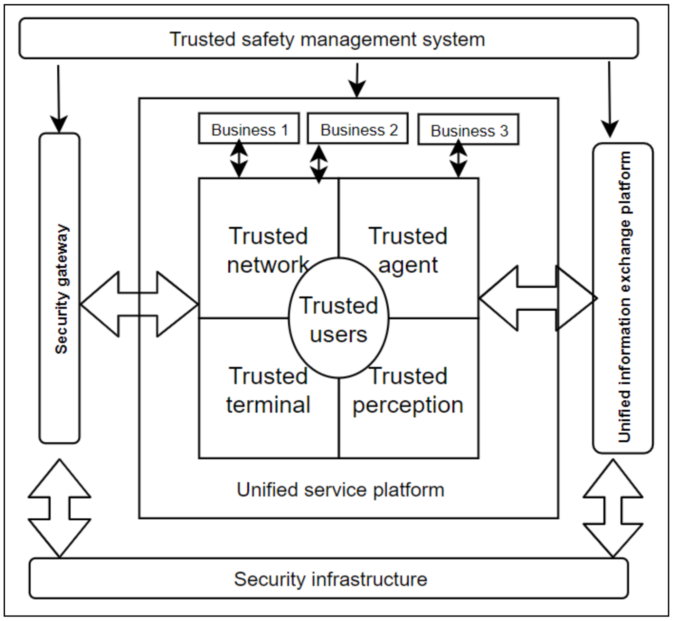

Fig. 9. A General Architecture of Trusted Security Systems based on IoT [36].

In the same year, scalability issues in IoT were considered. In this regard, a 3G-PLC architecture was proposed based on integrating power line communication (PLC) with 3G networks. As shown in Fig. 8, this architecture consists of the three well-known layers of IoT (the perception layer, the network layer, and the application layer), in addition to a newly added layer called the aggregation layer. As discussed earlier, the perception layer includes all of the devices that can sense and collect data from objects. Once data had been collected, the aggregation layer acts as a middleware layer to coordinate information processing, and to translate the data into a standard format. Thus, the formatted data will be transmitted to the network layer. The focus of the 3G-PLC architecture was on the network layer, which combines all types of communication systems, including a 3G mobile network and the technology of Long Term Evolution (LTE). Fig. 10, illustrates 3G-PLC architecture.

As stated before, the 3G-PLC architecture focuses on addressing the scalability issue in IoT, by combining two complex communication networks, which are PLC and 3G. PLC and 3G offer low cost, convenience, and more reliable services. Moreover, PLC can be operated through the existing power line in buildings, which saves significant costs compared to an optical fiber line. The advantage of the 3G node is that it can provide things with useful services such as classification, storage, signal processing, and power saving of the back-end network. 3G-PLC architecture can help in the development of the promising technology of IoT [37].

D. IoT Architecture in 2012

In 2012, a five-layer IoT architecture was proposed by Khan et al. in [27]. The five layers are the perception layer, the network layer, the middleware layer, the application layer, and the business layer, as shown in Fig. 11. The authors discussed that the perception layer can be called a device layer because it includes all the physical things and sensor devices, which mainly deal with identifying things and collecting their specific information. The sensed data from these devices will be transmitted to the network layer. The network layer includes all communication networks, including 3G, UMTS, WIFI, Bluetooth, ZigBee, infrared, etc.

It can be called the transmission layer, and it performs the functionality of transferring or transmitting the collected data from the lower layer to the middleware layer for further processing. In the middleware layer, the collected data received from the network layer will be managed and stored in databases and processed for different purposes. This layer includes techniques or mechanisms used for information processing. Furthermore, ubiquities computation can be performed in this layer for the purpose of making decisions based on the computed data. In the application layer, the processed data from the middleware layer can be utilized by IoT applications and, thus, the application layer will provide global management for similar applications, such as smart health, smart homes, smart buildings, smart or intelligent transportation, etc. In the business layer, the data used in IoT applications can be exploited to build a business model, charts and graphs that may assist in developing or supporting the IoT technology [18].

E. IoT Architecture in 2013

In 2013, an IoT architecture that integrated IoT with cloud computing was proposed by Zhou et al. in [44]. It was called CloudThings architecture, which is an online platform that assists system integrators and solution providers to create a complete infrastructure of things application for developing, deploying, operating, and combining things applications and services. The CloudThings architecture consists of three modules: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service(SaaS), as depicted in Fig. 12.

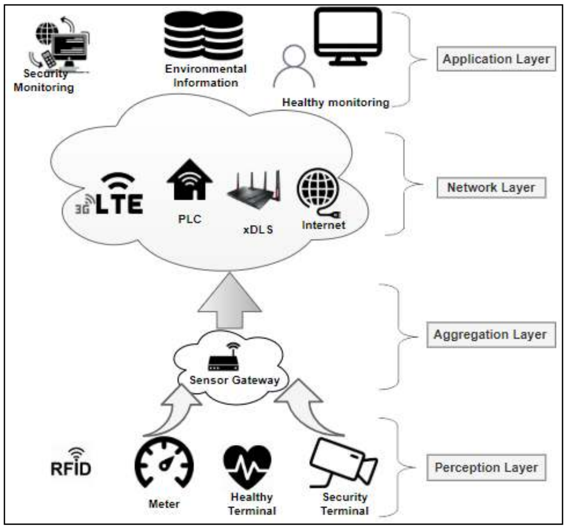

Fig. 10. IoT Architecture based on 3G-PLC[37].

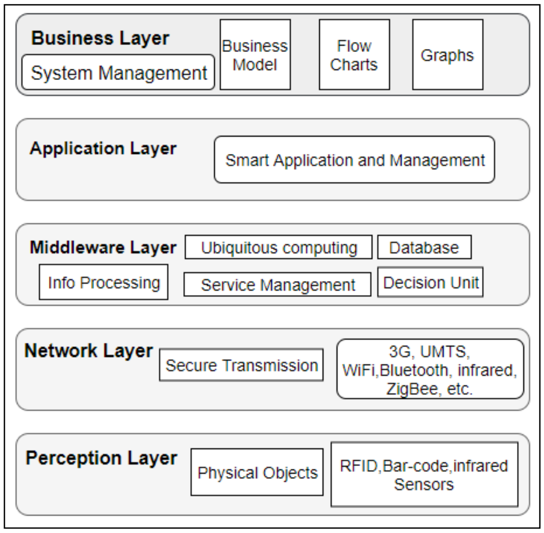

Fig. 11. Five-Layer IoT Architecture [18].

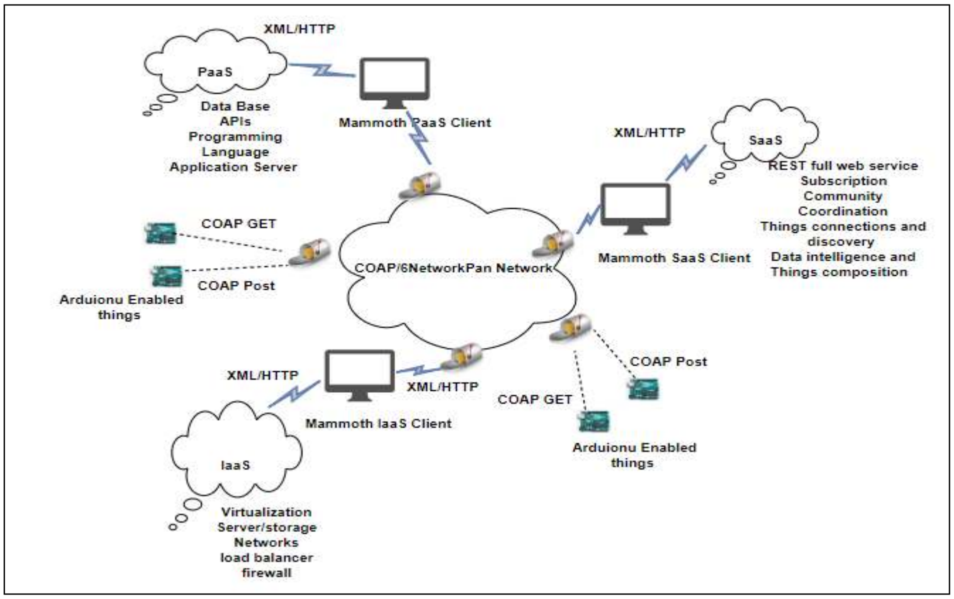

Fig. 12. CloudThings IoT Architecture [38].

CloudThings service platform (IaaS) helps users to run or operate any application on cloud hardware. This module offers users with distinctive management capabilities. It helps direct communication with deceives and offers storage or spaces to collect data on things and helps transmit event of things. The collected mass data can be exposed to an analysis by utilizing cloud computing and storage resources. CloudThings developer suite (PaaS) provides a set of tools for cloud services that can be used for things application development. CloudThings Operating Portal (SaaS) is a set of services provided by the cloud for the purpose of supporting the deployment and handling the special processing services, such as data intelligence and data discovery. The integration of cloud computing in IoT helps to develop things application. Using a cloud-based IoT offers a great advantage compared to traditional or conventional IoT development since the cloud provides services to develop, deploy, run, and manage data online. In other words, the cloud facilitates the development of IoT [38].

F. *IoT Architecture in 2015*

The nature of IoT imposes the heterogeneity in things that are connected to the Internet. Due to the heterogeneity, interoperability among heterogeneous devices is a challenge. To address such a challenge, Service-Oriented Architecture (SOA) is one solution that may help to ensure interoperability among different IoT devices in many ways. In 2015, SOA of IoT was proposed by Li et al. in [5]., which consists of four main layers, known as the sensing layer, the network layer, the service layer, and the interface layer as illustrated in Fig. 13.

Fig. 13, shows that the layers are displayed horizontally starting from the sensing layer, and ending with the interface layer. Like the previously mentioned IoT architectures, the sensing layer acts as the perception layer, which includes all devices that can sense the status of hardware objects and acquisition protocol in order to transmit the sensed data. The network layer helps to support the connections among IoT devices over the different types of networks, such as wireless sensor network and mobile network. The service layer accomplishes the functionality of creating and managing services required by users and provides applications with ready-made services that are available upon request. The interface layer involves interaction techniques or methods, which users and applications can use to interact with the provided services of the service layer. Applying SOA in IoT ensures the availability of the features of extensibility, scalability, modularity, and interoperability among different IoT things [50].

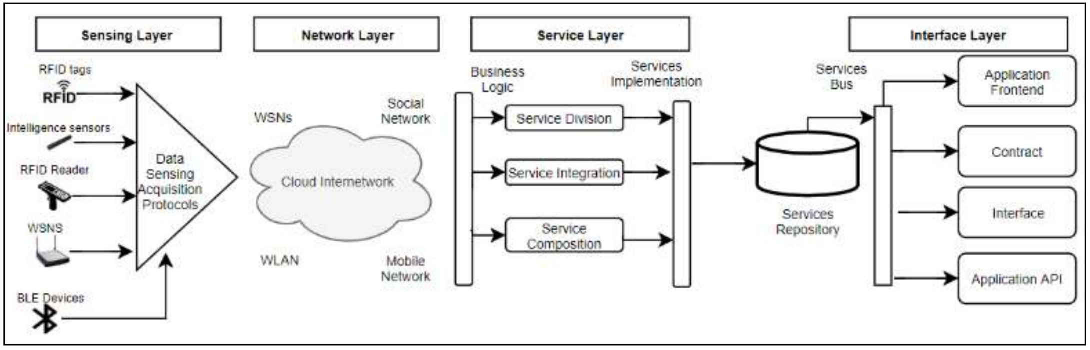

Fig. 13. Service-Oriented IoT Architecture Proposed in 2015[50].

G. IoT Architecture in 2016

In 2016, the focus of IoT architecture was on considering the existence of security. In [46], Salman et al. proposed an IoT architecture with features of data decentralization and control centralization. This architecture, shown in Fig. 14, is formed of four layers: the device layer, the network layer, the control layer, and the application layer.

Starting from the bottom, the device layer includes different types of identification device of things, such as RFID and sensors. In addition, it includes communication technologies like Bluetooth. Network layer performs data transmission that was received from the device layer. Many network types can be used in this layer, including wireless sensor network (WSN), Vehicle area network (VANET), legacy network, and mobile networks, such as second-generation (2G), third-generation (3G), and Long-Term Evolution (LTE). Software-defined gateway (SD-Gateway) is the most useful component of the network layer of this architecture because it facilitates the interoperability among the different types of communication protocol, plus the communication between different networks.

Moreover, SD-Gateway provides many important functions such as firewall, packet encapsulation, and decapsulation, network address translation (NAT), enabling data storage through fog computing, and packet forwarding. The idea of this architecture was to distribute the computing power between cloud and fog nodes, which are located on the edge of SD-Gateway. This kind of distribution will tackle power consumption issues that arise when all data computation is done in SD-Gateway, and network unavailability when data computation is done in the central server (cloud). An intelligent algorithm is needed to decide which kind of data must be stored or saved locally in fog nodes, which sort of data has to be transmitted to cloud, and which type of data need to be deleted. The control layer performs all the computation and involves routing algorithms, scheduling algorithm, and defining the security rules. The central control will lead to scalability limitation and can affect the security enhancement of this architecture. In the application layer, a different IoT application can be implemented. The control layer offers the benefit where the same applications can be deployed on a different SD-Gateway. Different types of management can be performed by this layer, for example, quality of service (QoS), security, privacy, and data analysis [40].

H. IoT Architecture in 2017

In 2017, a four-layer of secured IoT architecture was discussed by Adat and Gupta in [49]. It is mainly composed of four layers: the perceptual layer, the network layer, the support layer, and the application layer, as depicted in Fig. 15.

Fig. 15 illustrates that the perceptual layer is used to collect a different kind of data through physical devices and sensors. The network layer achieves information or data transmission from the perceptual layer to the processing unit. In the support layer, intelligent data operations and processing are executed. The top-most layer (the application layer) deals with end-users. This layer caters for consumers' needs by incorporating users' need in the applications. In this architecture, the analysis of security features in each level or layer was discussed, along with the security requirements, which are necessary to meet the security concerns at each layer. As Adat and Gupta discussed, the main challenges in the perceptual level are devices resource constraints, devices can be exposed to different Denial of service attack (DoS), interferences among devices, issues of confidentiality, integrity, availability (C-I-A) of sensed data at this layer. They suggested that, in order to avoid such challenges in the perceptual layer, the mechanisms of lightweight encryptions, protection of sensed data, and key agreement have to be implemented and applied. In the network layer, Adat and Gupta point out that the main challenges are congestion in the network, eavesdropping, and counterfeiting of the transmitted data, junk emails, and viruses, distributed denial of service attack (DDoS). The key defensive mechanisms for such threats are encryption techniques, anti-DDoS, and communication security. In the control layer, the major issues are intelligent massive processing of data and the filtration of suspicious information. The key solutions for these issues are using techniques to secure multiparty communication and secure computing. The main challenges in the application layer are data privacy and information leakage, application-dependent challenges, and control of access. To address such issues, the privacy protection and security education and management have to be considered [106].

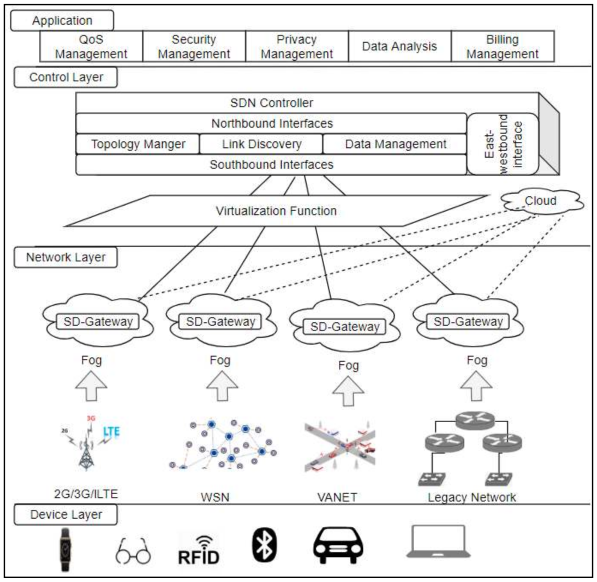

Fig. 14. Centralized Data and Decentralized Control IoT Architecture [40].

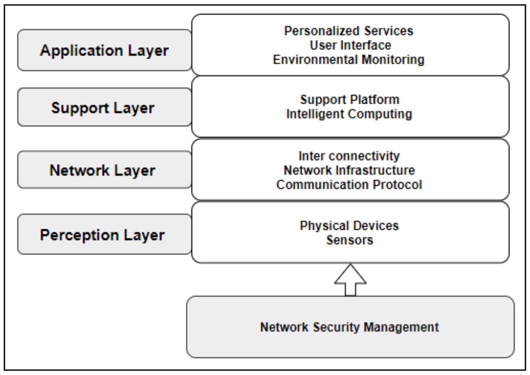

Fig. 15. Four-Layer of Secure IoT Architecture [43].

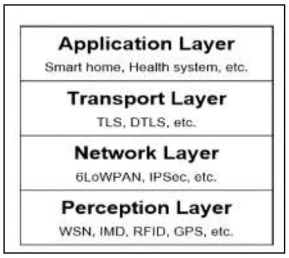

Fig. 16. Four-Layer IoT Architecture [107].

Concurrent with this layer, another four-layer IoT architecture was proposed in [107] by Yuchen et al. The security issues and solutions in each layer were also discussed. The four layers of this architecture are illustrated in Fig. 16.

At the perception layer, various devices are used to collect data, including sensors used to sense temperature, sounds, vibrations, movements, pressure, etc. According to this architecture, this layer is divided into two parts: the perception node and the perception network. The perception node is used for data acquisition, and includes things such as sensors, controllers, etc., while the perception network can be a node that has the ability to communicate and send the obtained data to the gateway [108]. This layer includes technologies such as WSN, implantable medical devices (IMDs), RFID, Global Positioning System (GPS), etc. Several issues were discussed in this layer, as the physical attack on sensor nodes that may lead to destroying or disabling the node. To avoid such attack, QoS should be ensured by having the capability to detect the faulty node and to take actions to minimize the degradation of the service. In the network layer, Yuchen et al suggested using lightweight mobile IPv6 and IPsec as mentioned in [109], since they are the best IoT solution in terms of security and efficiency. In the transport layer, Yuchen et al suggested implementing the two-way communications between IoT devices, such as Datagram Transport Layer Security (DTLS) protocol as discussed in [110]–[112], which provides full authentication DTLS handshake based on the exchange of X.509 certificates that include RSA keys. In the application layer, a variety of applications can be developed, such as smart homes, real-time health monitoring, energy management, environmental monitoring, smart parking, and many other applications. Through these applications, several threats can be noticed and there is an inevitable need to develop standards and security policies for IoT products [107].

Addressing scalability and management issues in IoT is crucial. A new architecture was proposed in 2017 for the purpose of addressing the scalability and management issues based on transparent computing in [42] by Hui et al. This architecture is composed of five layers, as shown in Fig. 17.

As is shown in Fig. 17, the first layer is the end-user layer, which consists of many IoT devices such as PC, Pad, Phones, Vehicle, Sensors, etc. These devices install MetaOS to support the cross-platform and execution of dynamic services. The installed MetaOS can assist them to boot many OSes from the upper layer (edge network layer), by network protocol through different lightweight terminals, which lead to scalability in IoT. Edge network layer has devices, such as a high-performance router and small-scale server that are used to collect and process the data of users, which are collected from the end-user layer. In this layer, the data will be sent to the upper layer (service and storage layer) through the core network layer that forms a bridge between the network layer and the service and storage layer. The service and storage layer has many servers, such as data server, software server, and control server. The main function of the data server is to store the data collected from the lower layer of analytical processing. The software server is responsible for storing the applications and program files of the OSes of the IoT devices and edge devices. The control server is used for managing the two servers (software and data). The management layer manages the servers in the service and storage layer and gives the control server tasks or duties that include adding or updating software. Transparent computing in this architecture is useful for improving the scalability of IoT apps, by logically splitting the hardware and software of IoT devices. This architecture is effective and efficient as the conducted experiment showed [42].

I. IoT Architecture in 2018

Recently, Blockchain was integrated into IoT to solve the challenges related to IoT device management. New IoT architecture was proposed in 2018 to provide a decentralized access control system connected to a distributed sensor network. The architecture was composed of six components which are wireless sensor network, managers, agent node, smart contract, Blockchain management, and management hub [132] as illustrated in Fig. 18.

In this architecture, a wireless sensor network includes IoT devices. As seen in Fig .16, IoT devices do not belong to the blockchain network. The manager has the responsibility to manage the access control permission of a set of IoT devices. The agent node is a specific Blockchain used to deploy smart contact in the system. The access management system is governed by the operations defined in a single smart contract, which is unique and cannot be deleted. The Blockchain network proposed in this architecture is a private network. Management hub is used to translate the information encoded by in CoAP messages by the IoT devices into JSON- RPC messages to be understood by Blockchain node. The proposed architecture addressed the issue of scalability problem of managing billions of IoT devices [113].

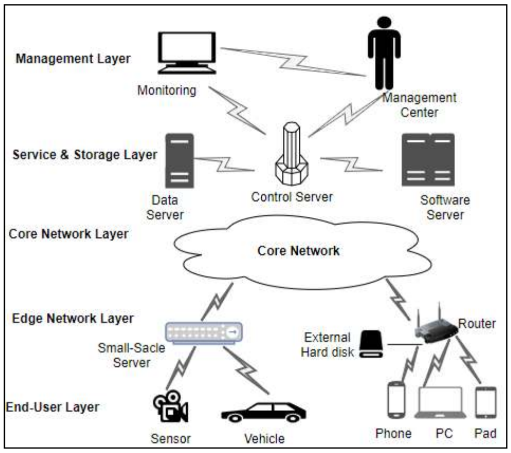

Fig. 17. A Scalable and Manageable IoT Architecture based on Transparent Computing [42].

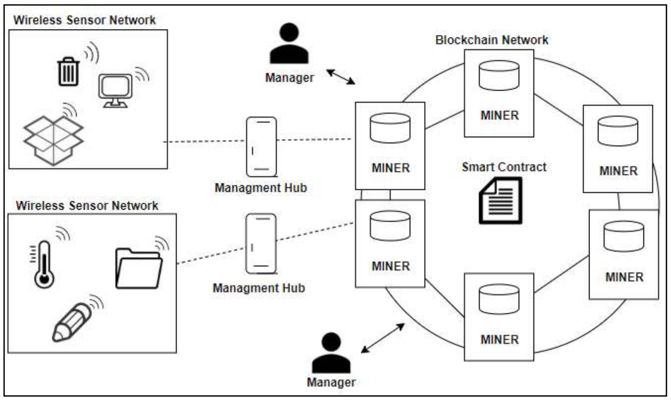

Fig. 18. Blockchain Meets IoT: the Architecture for Scalable Access Management in IoT [113].

In 2018, new IoT architecture was proposed to solve issues such as scalability, efficacy, security, etc. This architecture was based on new technologies such as device-to-device communication, 5G-IoT, Machine-Type Communication (MTC), Wireless Network Function virtualization (WNFV), Wireless Software Defined Networks (WSDN), Mobile Edge Computing (MEC), and Mobile Cloud Computing (MCC). It composed of 8 interconnected layers including Physical device layer that consists of wireless sensors, actuators, and controllers, data communication layer which includes two sublayers (device to device communication, connectivity layer). Fog computing layer, which processes data by edge node to make decisions on data. Data storage layer which stores and protect the obtained information from the edge layer. Management service layer which deals with handling the communication between devices and data centers and it consist of (network management layer, cloud computing layer, and data analytic layer). Application layer that allows software to interact with previous layers and data. Security layer which protects all layers through data encryption, user authentication, network access control, and cloud security [114]. The following Fig. 19. illustrated layers of this architecture.

Another new architecture was proposed in 2018 to tackle challenges of IoT such as scalability, extensibility, interoperability, and integration of heterogeneous devices and protocols. This architecture was based on microservices in the cloud. The architecture uses microelements that involve microservices, which are specific IoT functionalities that can be migrated across various virtualized infrastructure and microdata to exchange across services and devices. In this architecture as depicted in Fig. 20., the microservices is integrated into both edge servers and cloud. Microservices in edge servers supports computation in sensors locally which can save bandwidth for cloud communication. Microservices in cloud server performs Cloudification, virtualization and softwarization, and security of IoT.

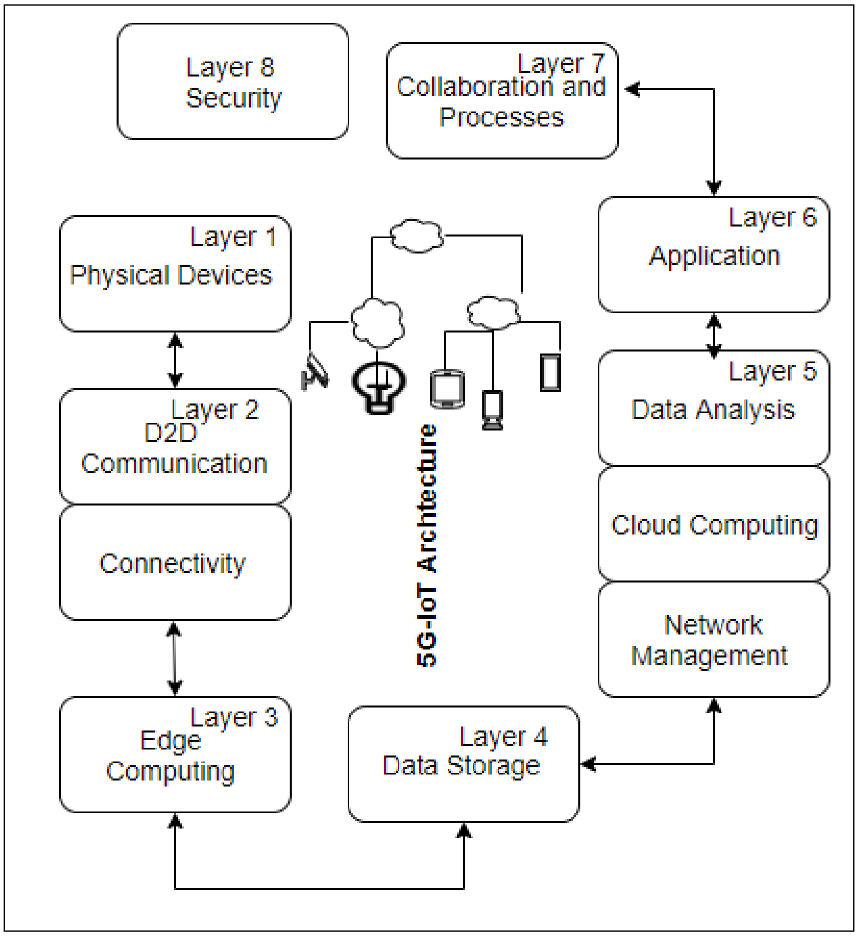

Fig. 19. 5G-IoT Architecture [114].

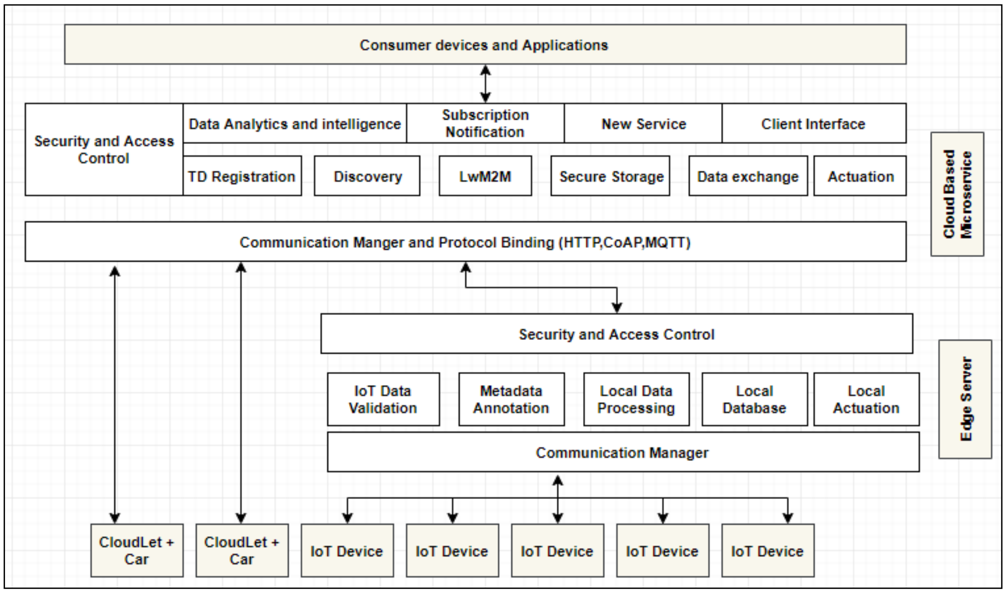

Fig. 20. IoT Architecture based on Microservices [115].

V. Discussion

Table II summarized different IoT architectures that were proposed with the aim of capturing the general essence of IoT technology. All the existing IoT architectures describe the IoT layers. Some architectures are very generic, in which they only describe the IoT layers in an abstract way (e.g. architectures proposed in 2008 and 2010), whereas architectures proposed after 2010 give more details of each layer. However, by comparing all these architectures, it became clear that the earliest architectures, which were proposed at the initial stage of IoT development, have some limitations. For example, the IoT architecture proposed in 2008 in [35], [105], did not consider the storage and processing in their layers. It is well known that data collection is the main functionality of IoT devices. Thus, the collected data need to be processed and stored, in order to be presented or disseminated to the users. In other words, the flow of the data collected by IoT devices was not depicted in this architecture. The architecture that was proposed in 2010 added more description to the previous IoT architecture, in which the storage and the processing layers were introduced. The architectures proposed after 2010 described the comprehensive meaning of IoT, starting from the data collection layer, followed by the network layer, then the processing layer, and ending with the application layer. As shown in Table 2, until 2011, none of the IoT architectures considered security. Table 2 shows the number of IoT devices that reached 12.5 billion in 2010, which resulted in increased concerns related to security issues that threaten IoT. Accordingly, the IoT architecture proposed in 2011 started considering security in IoT layers. It discussed security techniques that can help to decrease the potential risks of the network that may occur due to the access of untrusted users. This architecture was based on a summary of former scholars' research that combined security requirements and IoT characteristics. Scalability and interoperability issues of IoT were considered by the IoT architectures that were proposed in 2014 and 2105. Cloud computing was integrated into IoT architecture to provide a solution for scalability challenge in IoT. Whereas, service originated architecture (SOA) was integrated into IoT architecture to avoid interoperability issues that may occur due to the heterogeneous IoT devices. From 2016 onward, scholars paid more attention to the security issues in IoT. Architectures proposed during this period discussed all the security issues and challenges in each IoT layer, and some recent architectures proposed in 2017 include more details regarding the threats and requirements, and how to deal with such threats. As noticed in architectures which were proposed recently in 2018, different technologies such as Blockchain, 5G, and microservices in the cloud were used to mitigate the challenge of scalability in IoT.

Regarding the consideration of security and privacy aspects in IoT architectures, the findings showed that the existing IoT architectures lack security and privacy aspects. As presented in Table II, none of these architectures considered privacy preservation in IoT. Similar to other technologies, data is the main component of IoT. The data collected by sensors is stored, processed, and presented to users at the end. Therefore, in each IoT layer, there is an inevitable need to secure data and preserve users' privacy. Security in IoT can be achieved by applying security mechanisms, such as encryption and authentications, as pointed out recently by many scholars in [7], [7], [11], [43], [107]. The pervasive nature of IoT imposes many threats that affect individuals' privacy [116]. In IoT, data collection, data storage, data processing, and data representation increase privacy concerns[117]. Many privacy preservation techniques were used for preserving data generated by many technologies, including data mining, data publishing, and wireless sensor network, which were discussed in [118], [119], [128]–[130], [120]–[127]. Recently, scholars have started paying more attention to privacy issues in IoT, as discussed in [131]–[133]. Considering privacy in IoT architecture layers is necessary to preserve users' privacy, which contributes to the sustainability of IoT technology.

TABLE II. COMPARISONS BETWEEN THE EXISTING IOT ARCHITECTURES

IoT Architecture Evolution			**Comparison Criteria**		**Consideration of critical issues**	
Architecture Reference	Year	Architecture Stack	Covered issues(IoT challenges)	Used Technique	Security	Privacy
IoT Five-layer Architectures [105][35]	2008	1. Application Layer 2. Middleware Layer 3. Internet Layer 4. Gateway Layer 5. Edge technology	Didn't consider any IoT challenges. It only describes the main IoT architecture's components.	-	✗	✗
IoT Five-layer Architectures [35]	2010	1. Application Layer 2. Middleware Layer 3. Coordination Layer 4. Backbone Network 5. Edge Technology Layer	It considered the issue of packet recognition from different apps and traffic and storage.	Perform tasks in the coordination layer and network layer for restructuring packages and reassembling them to form a unified structure.	✗	✗
IoT Three-layer Architectures [5]		1. Application Layer 2. Network Layer 3. Perception Layer	It was the accepted three-layer structure of IoT. But it cannot express all of the features and connotation of IoT.	-	✗	✗
IoT Five-layer Architectures [5]		1. Business Layer 2. Application Layer 3. Processing Layer 4. Transport Layer 5. Perception Layer	It considered data storage and processing issue and it added processing and business layer.	Many advanced technologies are used in the processing layer such as: Intelligent processing Cloud computing Ubiquities computing	✗	✗
General Architecture Of Trusted Security System Based on IoT [36]	2011	1. Trusted user module 2. Trusted perception module 3. Trusted network module 4. Trusted terminal module 5. Trusted Agent Module	It considered important features such as integration, management, supervision of many resources of information security.	To achieve security; authentication mechanism, access control mechanism, encryption mechanism, and audit mechanism were used.	✓	✗
IoT Architecture Based on Integrated PLC and 3G Communication Networks [37]		1. Application Layer 2. Network Layer 3. Aggregation Layer 4. Perception Layer	It considered scalability issues.	Combining two types of complex communication networks: PLC and 3G, which offers low cost, convenience, and more reliable services.	✗	✗
IoT Five-layer Architectures [18]	2012	1. Business Layer 2. Application Layer 3. Middleware Layer 4. Network Layer 5. Perception Layer	It considered the larger traffic and storage needed for data generated by IoT where it focuses on network layer and middleware layer.	Techniques of ubiquities computing, database, information processing, service management, and decision unit are used in the middleware layer.	✗	✗
Common Architecture for Integrating the Internet of Things with Cloud Computing [38]	2013	1. CloudThings service platform(IaaS) 2. CloudThings developer suite(PaaS) 3. CloudThings operating Portal(SaaS)	It considered integration issue through integrating cloud computing into IoT assist in developing IoT application; it helps to develop, run and deploy Things app online.	Three modules of cloud computing were used: IaaS, PaaS, and SaaS with a set of tools in each module.	✗	✗

Service-oriented Architecture of IoT [50]	2014	1. Sensing Layer 2. Network Layer 3. Service Layer 4. Interface Layer	It considered heterogeneity, interoperability among heterogeneous IoT devices.	Service Oriented Architecture (SOA)	✗	✗
Decentralized Data and Centralized Control IoT architecture [40]	2105	1. Application Layer 2. Control Layer 3. Network Layer 4. Device Layer	It considered security through SD-Gateway.	SD-Gateway used techniques of: ▪ Firewall ▪ packet encapsulation ▪ Decapsulation ▪ Network Address Translation (NAT). ▪ Fog computing, ▪ Packet forwarding. In the application layer, they introduced privacy management and security management.	✓	✗
Four-layer of secured IoT architecture [107]	2017	1. Application Layer 2. Support Layer 3. Network Layer 4. Perception Layer	It theoretically discussed security challenges in all IoT layers.	The author suggested using lightweight encryption and protection of sensed data.	✓	✗
Four-layer IoT architecture [43]		1. Application Layer 2. Transport Layer 3. Network Layer 4. Perception Layer	It theoretically discussed security issues and solutions in each layer.	The author suggested using Lightweight mobile IPv6 and IPsec to provide security in the network layer. And to use DTLS protocol in the transport layer.	✓	✗
A scalable and manageable IoT architecture based on transparent computing [42]		1. Management Layer 2. Server & Storage Layer 3. Core Network Layer 4. Edge Network Layer 5. End-User Layer	It considered scalability and management issues.	It used transparent computing by logically splitting the hardware and software of IoT devices.	✗	✗
Blockchain meets IoT: an architecture for scalable access management in IoT [113]	2018	1. Wireless Sensor Network 2. Managers 3. Agent Node 4. Smart Contract 5. Blockchain Network 6. Management Hubs	It considered the scalability issue.	Integrating Blockchain in IoT for managing billions of IoT devices through decentralized access control system.	✓	✗
5G-IoT architecture [114]		1. Physical Devices Layer 2. Communication Layer 3. Edge Computing 4. Data Storage Layer 5. Management Service Layer 6. Application Layer 7. Collaboration and Processes Layer 8. Security Layer	It considered issues such as scalability, efficacy, security, etc.	New technologies were used such as a device to device communication, 5G-IoT, Machine-Type Communication(MTC), Wireless Network Function virtualization (WNFV), Wireless Software Defined Networks (WSDN), Mobile Edge Computing (MEC), and Mobile Cloud Computing (MCC)	✓	✗
IoT Architecture Based on Microservices [115]		1. Consumer devices and application 2. Cloudbased microservices 3. Edge server microservices	It solved issues such as scalability, efficacy, security, etc.	The technology of microservices in the cloud was used in edge server to support computation in sensors and in the cloud to perform services such as security, virtualization, etc.	✓	✗

VI. Conclusion

As technology evolves, new concepts emerge in the technology world that adds new advanced features to serve the world with influential solutions. This paper presented a systematic literature review to study the existing IoT architectures in terms of architecture classification (the number of layers), limitations in each architecture, and considerations of different aspects or features in each layer such as storage, processing techniques, security, and privacy. The findings show that the improvement of IoT architectures occurred gradually as technology evolved. In addition, the initial IoT architectures were very abstract and did not provide a comprehensive meaning of IoT nature. On the other hand, late architectures focused more on the essence of IoT and concentrated on how the data can be transferred, stored, and transmitted to the consumer. Different supporting technologies were considered in each layer of the different IoT architectures. The consideration of the security aspect in IoT architecture started in 2011. Overall, it was clearly noticed that none of these architectures has considered privacy preservation in IoT. Considering privacy in IoT architectures is very important for users to accept the IoT technology. Thus, there is an inevitable need to address privacy issues in IoT, which is considered a key factor in the sustainability of IoT development. The research will be extended to consider user privacy in all IoT architecture layers, by integrating privacy mechanisms in IoT architecture layers.

VII. Research Direction

Efforts must be devoted to integrating privacy preservation mechanisms when designing an IoT architecture, with the aim of preserving the privacy of users on one side and providing quality services on the other side. Privacy issues should be addressed at every IoT stage or level to avoid any attack that may compromise the data and, thus, influence the trust of users which could impact IoT sustainability.

Acknowledgment

This work was supported by Omental as a part of the project [code: EG/SQU-OT /18/02] under the title of "Internet of Things (IoT) security and privacy aspects related to architecture, connectivity and collected data.

References

[1] Z. K. Aldein Mohammeda and E. S. Ali Ahmed, “Internet of Things Applications, Challenges and Related Future Technologies,” no. February, 2017.

[2] A. Kott and I. Linkov, “Cyber Resilience of Systems and Networks,” pp. 381–401, 2019.

[3] T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang, “A medical healthcare system for privacy protection based on IoT,” in 2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), 2015, pp. 217–222.

[4] A. Whitmore, A. Agarwal, and L. Da Xu, “The Internet of Things—A survey of topics and trends,” Inf. Syst. Front., vol. 17, no. 2, pp. 261–274, 2015.

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

[6] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Cla, “Middleware for internet of things: A survey,” IEEE Internet Things J., vol. 3, no. 1, pp. 70–95, 2016.

[7] M. Ammar, G. Russello, and B. Crispo, “Internet of Things: A survey on the security of IoT frameworks,” J. Inf. Secur. Appl., vol. 38, pp. 8–27, 2018.

[8] A. Tewari and B. B. Gupta, “Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags,” J. Supercomput., vol. 73, no. 3, pp. 1085–1102, Mar. 2017.

[9] V. A. Memos, K. E. Psannis, Y. Ishibashi, B.-G. Kim, and B. B. Gupta, “An Efficient Algorithm for Media-based Surveillance System (EAMSuS) in IoT Smart City Framework,” Futur. Gener. Comput. Syst., vol. 83, pp. 619–628, Jun. 2018.

[10] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, “Vision and Challenges for Realising the Internet of Things The meaning of things lies not in the things themselves, but in our attitude towards them. Antoine de Saint-Exupéry,” 2010.

[11] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, “Internet of Things security and forensics: Challenges and opportunities,” Futur. Gener. Comput. Syst., vol. 78, pp. 544–546, 2018.

[12] B. C. Chifor, I. Bica, V. V. Patriciu, and F. Pop, “A security authorization scheme for smart home Internet of Things devices,” Futur. Gener. Comput. Syst., 2017.

[13] B. Xu, L. Da Xu, H. Cai, C. Xie, … J. H.-I. T. on, and U. 2014, “Ubiquitous data accessing method in IoT-based information system for emergency medical services,” ieeexplore.ieee.org, 2014.

[14] S. Fang, L. Da Xu, Y. Zhu, J. Ahati, … H. P.-I. T. on, and U. 2014, “An integrated system for regional environmental monitoring and management based on internet of things,” ieeexplore.ieee.org, vol. 10, no. 2, 2014.

[15] J. Manyika et al., “Unlocking the potential of the Internet of Things | McKinsey,” 2015. [Online]. Available: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world. [Accessed: 06-Nov-2018].

[16] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for IoT security and privacy: The case study of a smart home,” 2017 IEEE Int. Conf. Pervasive Comput. Commun. Work. (PerCom Work., pp. 618–623, 2017.

[17] J. Morgan, “A Simple Explanation Of ‘The Internet Of Things,’” Forbeds, 2014. [Online]. Available: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#105f158b1d09. [Accessed: 16-Jul-2018].

[18] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, “Future internet: The internet of things architecture, possible applications and key challenges,” Proc. - 10th Int. Conf. Front. Inf. Technol. FIT 2012, pp. 257–260, 2012.

[19] A Zanella, N. Bui, a Castellani, L. Vangelista, and M. Zorzi, “Internet of Things for Smart Cities,” IEEE Internet Things J., vol. 1, no. 1, pp. 22–32, 2014.

[20] D. Cuff, M. Hansen, and J. Kang, “Urban sensing: out of the woods,” Commun. ACM, vol. 51, no. 3, pp. 24–33, 2008.

[21] R. Davies, “The Internet of Things opportunities and challenges,” Eur. Parliam. Res. Serv., 2015.

[22] E. T. Chen, “The Internet of Things: Opportunities, Issues, and Challenges,” in The Internet of Things in the Modern Business Environment, IGI Global, 2017, pp. 167–187.

[23] B. L. R. Stojkoska and K. V Trivodaliev, “A review of Internet of Things for smart home: Challenges and solutions,” J. Clean. Prod., vol. 140, pp. 1454–1464, 2017.

[24] A. Al-Fuqaha et al., “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” vol. 17, no. 4, 2015.

[25] H. Wang, Z. Zhang, and T. Taleb, “Editorial: Special Issue on Security and Privacy of IoT,” 2017.

[26] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, “A survey on security and privacy issues in internet-of-things,” IEEE Internet Things J., vol. 4, no. 5, pp. 1250–1258, 2017.

[27] B. Lam and C. Larose, "How did the internet of things allow the latest attack on the internet?" 2016.

[28] J. S. Kumar, "A Survey on Internet of Things : Security and Privacy Issues," vol. 90, no. 11, pp. 20–26, 2014.

[29] Y. Cheng, M. Naslund, G. Selander, and E. Fogelstrom, "Privacy in machine-to-machine communications a state-of-the-art survey," in Communication Systems (ICCS), 2012 IEEE International Conference on, 2012, pp. 75–79.

[30] L. Zhou, Q. Wen, and H. Zhang, "Preserving sensor location privacy in internet of things," in Computational and Information Sciences (ICCIS), 2012 Fourth International Conference on, 2012, pp. 856–859.

[31] B. Tepekule, U. Yavuz, and A. E. Pusane, "On the use of modern coding techniques in QR applications," in Signal Processing and Communications Applications Conference (SIU), 2013 21st, 2013, pp. 1–4.

[32] M. Giannikos, K. Kokoli, N. Fotiou, G. F. Marias, and G. C. Polyzos, "Towards secure and context-aware information lookup for the Internet of Things," in Computing, Networking and Communications (ICNC), 2013 International Conference on, 2013, pp. 632–636.

[33] R. Hall, A. Rinaldo, and L. Wasserman, "Differential privacy for functions and functional data," J. Mach. Learn. Res., vol. 14, no. Feb, pp. 703–727, 2013.

[34] E. Liu, Z. Liu, and F. Shao, "Digital rights management and access control in multimedia social networks," in Genetic and Evolutionary Computing, Springer, 2014, pp. 257–266.

[35] L. Tan, "Future internet: The Internet of Things," 2010 3rd Int. Conf. Adv. Comput. Theory Eng., pp. V5-376-V5-380, 2010.

[36] X. Li, Z. Xuan, and L. Wen, "Research on the architecture of trusted security system based on the internet of things," Proc. - 4th Int. Conf. Intell. Comput. Technol. Autom. ICICTA 2011, vol. 2, pp. 1172–1175, 2011.

[37] H. C. Hsieh and C. H. Lai, "Internet of things architecture based on integrated PLC and 3G communication networks," Proc. Int. Conf. Parallel Distrib. Syst. - ICPADS, pp. 853–856, 2011.

[38] J. Zhou et al., "CloudThings: A common architecture for integrating the Internet of Things with Cloud Computing," Proc. 2013 IEEE 17th Int. Conf. Comput. Support. Coop. Work Des. CSCWD 2013, pp. 651–657, 2013.

[39] P. Fremantle, "A reference architecture for the internet of things," vol. 0, p. 21, 2015.

[40] O. Salman, I. Elhajj, A. Kayssi, and A. Chehab, "An architecture for the Internet of Things with decentralized data and centralized control," Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl. AICCSA, vol. 2016-July, 2016.

[41] J. Suarez, J. Quevedo, I. Vidal, D. Corujo, J. Garcia-Reinoso, and R. L. Aguiar, "A secure IoT management architecture based on Information-Centric Networking," J. Netw. Comput. Appl., vol. 63, pp. 190–204, 2016.

[42] H. Guo, J. Ren, D. Zhang, Y. Zhang, and J. Hu, "A scalable and manageable IoT architecture based on transparent computing," J. Parallel Distrib. Comput., 2017.

[43] V. Adat and B. B. Gupta, "Security in Internet of Things: issues, challenges, taxonomy, and architecture," Telecommun. Syst., vol. 67, no. 3, pp. 423–441, 2018.

[44] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," Futur. Gener. Comput. Syst., 2018.

[45] L. Castro and S. F. Wamba, "AN INSIDE LOOK AT RFID TECHNOLOGY," vol. 2, no. 1, 2007.

[46] M. Zennaro, "Intro to Internet of Things ITU ASP COE TRAINING ON &quot; Developing the ICT ecosystem to harness IoTs &quot;," 2016.

[47] K. D. Foot, "A Brief History of the Internet of Things - DATAVERSITY," dataversity.net, 2016. [Online]. Available: http://www.dataversity.net/brief-history-internet-things/. [Accessed: 30-Mar-2018].

[48] P. T. Venkat, N. Rao, A. Mandala, and S. Sangam, "Internet of Things-Architecture and Enabling Technologies," vol. 7, no. 6, pp. 798–804, 2016.

[49] K. Lueth, "Why it is called Internet of Things: Definition, history, disambiguation," iot-analytics, 2014. [Online]. Available: https://iot-analytics.com/internet-of-things-definition/. [Accessed: 12-Apr-2018].

[50] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," Inf. Syst. Front., vol. 17, no. 2, pp. 243–259, 2015.

[51] J. Gubbi, R. Buyya, S. Marusic, M. P.-F. generation computer, and undefined 2013, "Internet of Things (IoT): A vision, architectural elements, and future directions," Elsevier.

[52] "Internet of Things (IoT) History | Postscapes," 2018. [Online]. Available: https://www.postscapes.com/internet-of-things-history/. [Accessed: 30-Oct-2018].

[53] "History of IoT | Background Information and Timeline of the Trending Topic," postscapes.com, 2016. [Online]. Available: https://www.postscapes.com/internet-of-things-history/. [Accessed: 15-Mar-2018].

[54] K. Lasse, "Current state of the 360+ IoT Platforms," 2016. [Online]. Available: https://iot-analytics.com/current-state-of-iot-platforms-2016/. [Accessed: 12-Apr-2019].

[55] B. Insider, "IoT and IIoT are not a fad ; these technology," 2018.

[56] "IoT: number of connected devices worldwide 2012-2025 | Statista," statista.com, 2018. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. [Accessed: 25-Mar-2018].

[57] M. Shirer, "IDC Forecasts Worldwide Spending on the Internet of Things to Reach $772 Billion in 2018," 2018. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS43295217. [Accessed: 14-Oct-2018].

[58] IANS, "internet of things: Global Internet of Things market to hit $1.29 trillion by 2020: Report, Telecom News, ET Telecom," 2017. [Online]. Available: https://telecom.economictimes.indiatimes.com/news/global-internet-of-things-market-to-hit-1-29-trillion-by-2020-report/61053782. [Accessed: 14-Oct-2018].

[59] A. Mohan, K. Gauen, Y. H. Lu, W. W. Li, and X. Chen, "Internet of video things in 2030: A world with many cameras," Proc. - IEEE Int. Symp. Circuits Syst., pp. 2–5, 2017.

[60] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Comput. networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[61] H. Duce, "Internet of Things in 2020." Academic Press, 2008.

[62] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, "Vision and challenges for realising the Internet of Things," Clust. Eur. Res. Proj. Internet Things, Eur. Commision, vol. 3, no. 3, pp. 34–36, 2010.

[63] I. Peña-López and others, "ITU Internet report 2005: the internet of things," 2005.

[64] H. Chen, R. Chiang, V. S.-M. Quarterly, and U. 2012, "Business intelligence and analytics: from big data to big impact," JSTOR, 2012.

[65] M. Zorzi, A. Gluhak, … S. L.-I. W., and U. 2010, "From today's intranet of things to a future internet of things: a wireless-and mobility-related view," ieeexplore.ieee.org, 2010.

[66] T. Liu and D. Lu, "The application and development of IoT," in Information Technology in Medicine and Education (ITME), 2012 International Symposium on, 2012, vol. 2, pp. 991–994.

[67] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of IoT: Applications, challenges, and opportunities with China Perspective," IEEE Internet Things J., vol. 1, no. 4, pp. 349–359, 2014.

[68] H.-D. Ma, "Internet of things: Objectives and scientific challenges," J. Comput. Sci. Technol., vol. 26, no. 6, pp. 919–924, 2011.

[69] A. Botta, W. De Donato, V. Persico, and A. Pescapé, "On the integration of cloud computing and internet of things," in Future internet of things and cloud (FiCloud), 2014 international conference on, 2014, pp. 23–30.

[70] Khan and P. S. D. Sawant, "A review on integration of cloud computing and Internet of Things," Int. J. Adv. Res. Comput. Commun. Eng., vol. 5, no. 4, pp. 1046–1050, 2016.

[71] D. N. Preethi, "Performance evaluation of IoT result for machine learning," Trans. Eng. Sci., vol. 2, no. 11, 2014.

[72] P. Fraga-Lamas, T. M. Fernández-Caramés, M. Suárez-Albela, L. Castedo, and M. González-López, "A review on internet of things for defense and public safety," Sensors, vol. 16, no. 10, p. 1644, 2016.

[73] V. D. Thoke, “Theory of distributed computing and parallel processing with applications, advantages and disadvantages,” Int. J. Innov. Eng. Res. Technol. http//www. ijiert. org/admin/papers/1452798652_ICITDCEME% E2, vol. 80, p. 9915.

[74] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, “Fog computing and its role in the internet of things,” in Proceedings of the first edition of the MCC workshop on Mobile cloud computing, 2012, pp. 13–16.

[75] B. T. STUDENT and S. SVNIT, “FOG COMPUTING IN IOT.”

[76] S. S. Kulkarni, S. G. Kulkarni, and V. P. Datar, “Current Trends in Internet of Things: A Survey,” 2018.

[77] J. Kim and J. W. Lee, “OpenIoT: An open service framework for the Internet of Things,” 2014 IEEE World Forum Internet Things, WF-IoT 2014, pp. 89–93, 2014.

[78] I. Ali, E. Khan, and S. Sabir, “Privacy-Preserving Data Aggregation in Resource-Constrained Sensor Nodes in Internet of Things: A Review,” Futur. Comput. Informatics J., 2017.

[79] I. Yaqoob et al., “Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges,” IEEE Wirel. Commun., vol. 24, no. 3, pp. 10–16, 2017.

[80] F. Mattern and C. Floerkemeier, “From the Internet of Computers to the Internet of Things,” in From active data management to event-based systems and more, Springer, 2010, pp. 242–259.

[81] E. Commission, “Internet of Things Factsheet Privacy & Security,” Eur. Comm., pp. 1–9, 2013.

[82] I. Alqassem and D. Svetinovic, “A taxonomy of security and privacy requirements for the Internet of Things (IoT),” IEEE Int. Conf. Ind. Eng. Eng. Manag., vol. 2015-Janua, pp. 1244–1248, 2014.

[83] A. A. Abi Sen, F. A. Eassa, K. Jambi, and M. Yamin, “Preserving privacy in internet of things: a survey,” Int. J. Inf. Technol., vol. 10, no. 2, pp. 189–200, 2018.

[84] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, “Internet of things: Vision, applications and research challenges,” Ad hoc networks, vol. 10, no. 7, pp. 1497–1516, 2012.

[85] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” Comput. networks, vol. 76, pp. 146–164, 2015.

[86] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, “A survey of intrusion detection in Internet of Things,” J. Netw. Comput. Appl., vol. 84, pp. 25–37, 2017.

[87] K. Hayashi, “IoT worm used to mine cryptocurrency,” Symantec Secur. Response, 2017.

[88] E. Bertino, “Botnets and Internet,” Comput. by IEEE Comput. Soc. Soc., vol. February, pp. 76–79, 2017.

[89] M. Siegel, M. S. Jalali, J. P. Kaiser, M. Siegel, and S. Madnick, “The Internet of Things (IoT) Promises New Benefits – and Risks : A Systematic Analysis of Adoption Dynamics of IoT Products The Internet of Things (IoT) Promises New Benefits — and Risks : A Systematic Analysis of Adoption Dynamics of IoT Products,” no. August, 2017.

[90] A. Jacobsson, “IoT, Security and Privacy,” 2018 1st Int. Conf. Comput. Appl. Inf. Secur., pp. 1–14, 2017.

[91] C. Li and B. Palanisamy, “Privacy in Internet of Things: from Principles to Technologies,” IEEE Internet Things J., vol. PP, no. c, pp. 1–1, 2018.

[92] S. D. Warren and L. D. Brandeis, “The Harvard Law Review Association,” Harv. Law Rev., vol. 4, no. 5, pp. 193–220, 1890.

[93] A. F. Westin, “Privacy and freedom,” Wash. Lee Law Rev., vol. 25, no. 1, p. 166, 1968.

[94] R. H. Weber, “Internet of Things - New security and privacy challenges,” Comput. Law Secur. Rev., vol. 26, no. 1, pp. 23–30, 2010.

[95] D. He, R. Ye, S. Chan, M. Guizani, and Y. Xu, “Privacy in the Internet of Things for Smart Healthcare,” IEEE Commun. Mag., vol. 56, no. 4, pp. 38–44, 2018.

[96] D. Chen, P. Bovornkeeratiroj, D. Irwin, and P. Shenoy, “Private memoirs of IoT devices: Safeguarding user privacy in the IoT Era,” Proc. - Int. Conf. Distrib. Comput. Syst., vol. 2018-July, pp. 1327–1336, 2018.

[97] D. Chen, S. Kalra, D. Irwin, P. Shenoy, and J. Albrecht, “Preventing occupancy detection from smart meters,” IEEE Trans. Smart Grid, vol. 6, no. 5, pp. 2426–2434, 2015.

[98] S. Barker, S. Kalra, D. Irwin, and P. Shenoy, “Powerplay: creating virtual power meters through online load tracking,” in Proceedings of the 1st ACM Conference on Embedded Systems for Energy-Efficient Buildings, 2014, pp. 60–69.

[99] D. Chen and D. Irwin, “Weatherman: Exposing weather-based privacy threats in big energy data,” in Big Data (Big Data), 2017 IEEE International Conference on, 2017, pp. 1079–1086.

[100] D. Chen, S. Iyengar, D. Irwin, and P. Shenoy, “SunSpot: Exposing the Location of Anonymous Solar-powered Homes,” in Proceedings of the 3rd ACM International Conference on Systems for Energy-Efficient Built Environments, 2016, pp. 85–94.

[101] R. Perez-Pena and M. Rosenberg, “Strava fitness app can reveal US military sites, analysts say,” New York Times, vol. 29, 2018.

[102] A. B. Pawar and S. Ghumbre, “A survey on IoT applications, security challenges and counter measures,” Int. Conf. Comput. Anal. Secur. Trends, CAST 2016, pp. 294–299, 2017.

[103] S. M. R. Islam, D. Kwak, M. D. H. Kabir, M. Hossain, and K.-S. Kwak, “The internet of things for health care: a comprehensive survey,” IEEE Access, vol. 3, pp. 678–708, 2015.

[104] N. Dragoni, A. Giaretta, and M. Mazzara, “The Internet of Hackable Things,” in Proceedings of 5th International Conference in Software Engineering for Defence Applications, 2018, pp. 129–140.

[105] J. Pereira, “From autonomous to cooperative distributed monitoring and control: Towards the Internet of smart things,” in ERCIM Workshop on eMobility, 2008.

[106] V. Adat and B. B. Gupta, “Security in Internet of Things: issues, challenges, taxonomy, and architecture,” Telecommun. Syst., vol. 67, no. 3, pp. 1–19, 2017.

[107] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, “A Survey on Security and Privacy Issues in Internet-of-Things,” IEEE Internet Things J., vol. 4, no. 5, pp. 1250–1258, 2017.

[108] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, “Security of the Internet of Things: perspectives and challenges,” Wirel. Networks, vol. 20, no. 8, pp. 2481–2501, 2014.

[109] A. J. Jara, D. Fernandez, P. Lopez, M. A. Zamora, and A. F. Skarmeta, “Lightweight MIPv6 with IPSec support,” Mob. Inf. Syst., vol. 10, no. 1, pp. 37–77, 2014.

[110] S. Raza, D. Trabalza, and T. Voigt, “6LoWPAN compressed DTLS for CoAP,” Proc. - IEEE Int. Conf. Distrib. Comput. Sens. Syst. DCOSS 2012, pp. 287–289, 2012.

[111] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, “Lithe: Lightweight secure CoAP for the internet of things,” IEEE Sens. J., vol. 13, no. 10, pp. 3711–3720, 2013.

[112] M. Brachmann, S. L. Keoh, O. G. Morchon, and S. S. Kumar, “End-to-end transport security in the IP-based internet of things,” 2012 21st Int. Conf. Comput. Commun. Networks, ICCCN 2012 - Proc., 2012.

[113] O. Novo, “Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT,” IEEE Internet Things J., vol. 5, no. 2, pp. 1184–1195, 2018.

[114] H. Rahimi, A. Zibaeenejad, and A. A. Safavi, “A Novel IoT Architecture based on 5G-IoT and Next Generation Technologies,” 2018 IEEE 9th Annu. Inf. Technol. Electron. Mob. Commun. Conf., pp. 81–88, 2018.

[115] S. K. Datta and C. Bonnet, “Next-Generation, Data Centric and End-to-End IoT Architecture Based on Microservices,” 2018 IEEE Int. Conf. Consum. Electron. - Asia, ICCE-Asia 2018, pp. 206–212, 2018.

[116] N. Madaan, M. A. Ahad, and S. M. Sastry, “Data integration in IoT ecosystem: Information linkage as a privacy threat,” Comput. Law Secur. Rev., vol. 34, no. 1, pp. 125–133, 2018.

[117] S. Al-Fedaghi, “Engineering privacy revisited,” J. Comput. Sci., vol. 8, no. 1, pp. 107–120, 2012.

[118] V. S. Verykios, E. Bertino, I. N. Fovino, L. Parasiliti Provenza, Y. Saygin, and Y. Theodoridis, “State-of-the-art in Privacy Preserving Data Mining *.”

[119] Y. Abdul, A. S. Aldeen, M. Salleh, and M. A. Razzaque, “A comprehensive review on privacy preserving data mining,” Springerplus.

[120] Z. Batmaz and H. Polat, “Randomization-based Privacy-preserving Frameworks for Collaborative Filtering,” Procedia Comput. Sci., vol. 96, pp. 33–42, 2016.

[121] A. Diyanat, A. Khonsari, and H. Shafiei, “Preservation of temporal privacy in body sensor networks,” J. Netw. Comput. Appl., vol. 96, no. October 2016, pp. 62–71, 2017.

[122] Y. Xu, T. Ma, M. Tang, and W. Tian, “A Survey of Privacy Preserving Data Publishing using Generalization and Suppression,” Appl. Math. Inf. Sci, vol. 8, no. 3, pp. 1103–1116, 2014.

[123] S. Matwin, “Privacy-Preserving Data Mining Techniques: Survey and Challenges,” Springer, Berlin, Heidelberg, 2013, pp. 209–221.

[124] B. C. M. Fung, K. Wang, R. Chen, and P. S. Yu, “Privacy-preserving data publishing,” ACM Comput. Surv., vol. 42, no. 4, pp. 1–53, 2010.

[125] Z. Zhan and W. Du, “Privacy-Preserving Data Mining Using Multi-Group Randomized Response Techniques,” Group, vol. 1, pp. 1–18, 2010.

[126] B.-C. Chen, D. Kifer, K. LeFevre, and A. Machanavajjhala, Privacy-Preserving Data Publishing, vol. 2, no. 1–2. 2009.

[127] J. Wang, Y. Luo, Y. Zhao, and J. Le, “A Survey on Privacy Preserving Data Mining,” in 2009 First International Workshop on Database Technology and Applications, 2009, pp. 111–114.

[128] N. Li, N. Zhang, S. K. Das, and B. Thuraisingham, “Privacy preservation in wireless sensor networks: A state-of-the-art survey,” Ad Hoc Networks, vol. 7, no. 8, pp. 1501–1514, 2009.

[129] W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher, “PDA: Privacy-preserving data aggregation in wireless sensor networks,” Infocom ’07, 2007.

[130] P. Samarati and L. Sweeney, “Protecting Privacy when Disclosing Information: k-Anonymity and its Enforcement Through Generalization and Suppresion.,” Proc IEEE Symp. Res. Secur. Priv., pp. 384–393, 1998.

[131] D. Zheng, A. Wu, Y. Zhang, and Q. Zhao, “Efficient and privacy-preserving medical data sharing in Internet of Things with limited computing power,” vol. 3536, no. c, 2018.

[132] J. Luis, C. Sanchez, J. B. Bernabe, and A. F. Skarmeta, “Towards Privacy Preserving Data Provenance for the Internet of Things,” pp. 41–46, 2018.

[133] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, “Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system,” Inf. Sci. (Ny)., vol. 0, pp. 1–26, 2018.