Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges

Ado Adamou Abba Ari, Olga Kengni Ngangmo, Null Kolyang, Chafiq Titouna, Ousmane Thiare, Alidou Mohamadou, Abdelhak Mourad Gueroui

Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges

Received 29 August 2019
Revised 20 October 2019
Accepted 19 November 2019

Ado Adamou Abba Ari
LI-PaRAD Lab, Université Paris Saclay, University of Versailles Saint-Quentin-en-Yvelines, Versailles, France and LaRI Lab, University of Maroua, Maroua, Cameroon
Olga Kengni Ngangmo
LaRI Lab, University of Maroua, Maroua, Cameroon
Chafiq Titouna
LIPADE Lab, Université Paris Descartes, Paris, France
Ousmane Thiare
Department of Computer Science, Gaston Berger University of Saint-Louis, Saint-Louis, Senegal
Kolyang and Alidou Mohamadou
LaRI Lab, University of Maroua, Maroua, Cameroon, and
Abdelhak Mourad Gueroui
LI-PaRAD Lab, Université Paris Saclay, University of Versailles Saint-Quentin-en-Yvelines, Versailles, France

We like to thank the editor and the anonymous reviewers for their valuable remarks that helped us in better improving the content and presentation of the paper.

Declaration of Competing Interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Publishers note: The publisher wishes to inform readers that the article "Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges" was originally published by the previous publisher of *Applied Computing and Informatics* and the pagination of this article has been subsequently changed. There has been no change to the content of the article. This change was necessary for the journal to transition from the previous publisher to the new one. The publisher sincerely apologises for any inconvenience caused. To access and cite this article, please use Ari, A. A. A., Ngangmo, O. K., Titouna, C., Thiare, O., Kolyang, Mohamadou, A., Gueroiu, A. M. (2019), "Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges" *Applied Computing and Informatics*, Vol. ahead-of-print No. ahead-of-print. https://10.1016/j.aci.2019.11.005. The original publication date for this paper was 22.11.2019.

Applied Computing and Informatics
Vol. 20 No. 1/2, 2024
pp. 119-141
Emerald Publishing Limited
e-ISSN: 2210-8327
p-ISSN: 2634-1964
DOI 10.1016/j.aci.2019.11.005

Abstract

The Cloud of Things (IoT) that refers to the integration of the Cloud Computing (CC) and the Internet of Things (IoT), has dramatically changed the way treatments are done in the ubiquitous computing world. This integration has become imperative because the important amount of data generated by IoT devices needs the CC as a storage and processing infrastructure. Unfortunately, security issues in CoT remain more critical since users and IoT devices continue to share computing as well as networking resources remotely. Moreover, preserving data privacy in such an environment is also a critical concern. Therefore, the CoT is continuously growing up security and privacy issues. This paper focused on security and privacy considerations by analyzing some potential challenges and risks that need to be resolved. To achieve that, the CoT architecture and existing applications have been investigated. Furthermore, a number of security as well as privacy concerns and issues as well as open challenges, are discussed in this work.

Keywords Cloud of Things, Cloud Computing, Internet of Things, Privacy, Security

Paper type Original Article

1. Introduction

The world is undergoing major changes or technological developments with the advent of computer "things", first on the Internet and then in Cloud Computing (CC). Computer networks are no longer isolated, they are opening up to the great world of Internet, which now connects not only computers but also a number of smart and miniaturized objects of our daily life such as embedded electronic chips, sensors, actuators, and smart software, for providing pervasive information access. These objects can be mobile, wirelessly connected and dynamically reconfigurable. Moreover, the considered smart devices are capable in collecting, storing, transferring and processing data from the environment, without discontinuity between the virtual and the physical worlds [1–3]. This is known as the Internet of Things (IoT), which has been defined by the International Telecommunication Union (ITU) as a network that enables connectivity in any place and any time for any connected whatever devices. Besides, IoT puts together computer processing and real world data to reduce the costs while increasing the efficiency and accuracy [4,5].

Moreover, constant innovations in hardware development, software and wireless communication technologies over the past decade conferred to the IoT the status of an innovative concept and have led to the expansion of smart objects as the amount of connected devices increases day by day. It promises to ease our lives, save us time, relieve our brain of memorizing logistical data such as routes, times of medication, etc [6]. The constant increase in the use of these objects led to the explosion of the global amount of generated data. In this light, given to the ever increasing abilities of sensing platforms, computing and communication capabilities of smart devices, Cisco Internet Business Solutions Group predicted that, from the end of 2019, IoT smart devices will annually generate more than 500 zettabytes of unstructured and structured data. In addition, this number is expected to exponentially grow [7]. Moreover, industries' forecasts project more than 50 billion of connected devices to the Internet by 2020 [8–10].

Therefore, the ubiquitous access to different types of information would allow the sophistication of the lifestyle and a significant improvement of the quality of the services in different fields [11]. These areas include e-health, video surveillance, smart home, smart city, smart community, e-transport, environmental monitoring, street lighting, and traffic control. IoT is typically characterized by the real world and small devices or objects with limited processing capabilities and storage, as well as issues related to performance, reliability, privacy and security [12]. Moreover, the CC has non negligible capabilities in terms of processing power and storage that are the main drawbacks of IoT [12,13]. Nowadays, The cloud technology has become the one that provides a faster and smart platform for application development and hosting as well as data storage and management [14–16].

Furthermore, the recent trend of fog computing, especially the fog-to-cloud computing paradigm [17,18] that decentralizes the cloud by bringing the services closer to the end-system and end-user, changed the future of the Internet by introducing the Internet of Everything (IoE) as denominated by Cisco [19], which is meant to connect all smart objects surrounding us in our daily life [11,20]. Nowadays, the necessity to combine both technologies appears and that combination can help us in many aspects of our daily life. Besides that, the IoT can contain many things and a number of interconnected technologies like Radio Frequency and IDentification (RFID) as well as Wireless Sensor Networks (WSNs) in order to share information and large amounts of heterogeneous data are speedily generated. Unfortunately, the IoT devices have limitations in terms of storage, network, and computing. In addition to this fact, data access and scalability require technology as the CC to supplement the storage and computing resources. While the CC technology has a non negligible potential to satisfy a number of IoT requirements, the fog-to-cloud computing-based solutions are becoming a way of addressing some challenging issues including real-time processing, low latency, and data response speed. Hence, a new computing paradigm in which the CC functionalities and IoT act as two merged linked technologies is expected in order to disrupt the actual and the future Internet. Therefore, once these two technologies, i.e., IoT and CC are put together, the resulting technology called CloudIoT or Cloud of Things (CoT) become the post CC era [13,21], which enabled new perspectives including Big Data collection and processing [10,22] as well as resource constraints, scalability, security and privacy concerns [23,24].

Certainly, a number of security and privacy mechanisms that aim at securing the CoT infrastructure has been proposed [25]. However, in the CoT environment, adversaries can still perform various kinds of incursions by exploiting the vulnerabilities of the heterogeneous IoT devices. These attacks include jamming, collision, Sybil or flooding. Therefore, the best protection against these attach is to remove the technological vulnerabilities or defend against them. Furthermore, according to the fact that works in IoT tends to the underlying system, before saving data into the cloud, research has not focused enough on the privacy and security risks beyond these subsystems. This paper focuses on CoT and aims at studying open security and privacy issues. Particularly, the work proposed here aims at increasing readers' knowledge by providing a sufficient and comprehensive background. The first contribution of this paper is enabling novice readers to understand the mechanism and operation CoT. Secondly, we propose review of privacy and security issues in CoT.

This paper is organized as follows. Section 2, presents some background of CoT and the corresponding architecture. We then present some CoT applications, platforms, challenges in CoT and issues involved in Section 3.1. In Section 4, we present a number of security and privacy threats in CoT. Then, a brief literature review on security and privacy as well as some open research challenges in CoT are presented in Section 5. Finally, we conclude the paper in Section 6.

2. Cloud of Things

2.1 Background

From their emergence, the two concepts of CC and IoT have evolved separately. For many years, they have seen independent evolution in their hardware and software aspects. In its evolution, IoT faces many problems among them storage capacity, energy efficiency, computational capabilities. While looking for solutions to these problems, scientists found that CC could help to solve them. That is why they think about how to combine the two concepts. The integration of IoT and CC has generated many advantages for each of them. By visiting other network technologies, the Cloud Computing paradigm seems to be an answer in regards to its characteristics. CC could fill some gaps of the IoT which has limitations with

regard to the storage, networking and computing capabilities of different connected objects. IoT is also limited as far as energy, scalability, interoperability, flexibility, reliability, efficiency and availability are concerned [12,26–28].

On the one hand, as the CC has virtually unlimited resources and capabilities, the IoT could be interested in this potential which can help in the compensation of its technological constraints such as processing, storage, and energy. For instance, CC can help to effectively implement many IoT applications. Some of them can be found among the solutions for IoT service management and composition, applications exploiting the produced data from devices. Otherwise, IoT can give to the CC the chance to deal with real-world objects in a more dynamic and distributed way for delivering new attractive services and applications in some practical scenarios. Hence, the need to merge the Cloud and IoT technologies emerge. As a result, the concept of CoT was born [29,30]. The emergence of the new concepts of CoT appears in recent years: Sensing-as-a-Service, Video-Monitoring-as-a-Service, Database-as-a-service, Identity and policy management as a service, Big Data Analytics-as-a-Service, Data-as-a-Service, Sensor-as-a-Service, etc.

2.2 Architecture of CoT

The CoT is an opportunity that represents the ongoing trend for the next generation applications of IoT smart services [30]. The IoT objects generate a big amount of data that will be processed and analyzed in the Cloud in order to produce important information. That information can be very sensitive, they are used by many smart services and/or applications. Therefore, to achieve the objective of efficiently managing the large amount of generated data, the existing cloud architecture needs to be reinforced. This enhancement is necessary to be more efficient and practical for the IoT based real-time services in terms of energy consumption, security, privacy, and end-to-end delays. To overcome these two last problems, cloud architectures are migrating to distributed architectures closer to the network edge like it is the case for Cloudlets, micro-cloud and fog nodes. The CoT networks, with these distributed architectures, can gain many facilities.

In this direction, Vasić et al. [31] give an understandable description of the CoT ecosystem. They describe it as a tiered architecture made of diverse devices interconnected. These objects can be interconnected through various and different networked environments. Moreover, Khanna [32] proposes an architecture for CoT that acts as a plan for the technology and describe its components. The author proposed an architecture with four layers. Also, Distefano et al. [33] as far as they are concerned, have introduced the approximate schema and the whole stack of the architectural modules so as to construct a CoT based on the paradigm of Things as a Service (TaaS). Therefore, the logical organization of the CoT layered architecture is given in Figure 1.

3. CoT applications, platforms and challenges

3.1 Applications of CoT

With the convergence of CoT paradigm, IT domain faces many significant changes. New set of smart applications and smart services, that can seriously impact user's daily life, appeared, Other one were significantly improved. A number of CoT applications and services can benefit from Machine-to-Machine communications (M2M) and not only send information towards the cloud. By pointing out the corresponding challenges, a number of CoT applications (see Figure 2) are presented in this section.

1. *Healthcare.* In many countries nowadays, the current trend concerning healthcare aims at reducing a number of available hospital resources by moving some healthcare services at home [12]. For instance, the medical checking is one of these services.

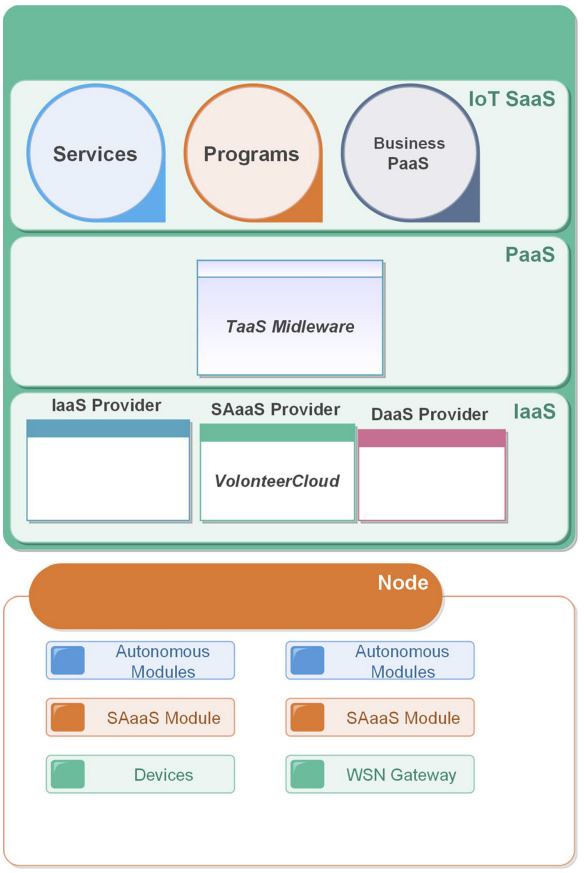

Figure 1.
CoT architecture.

With connected health, more work should be done on designing algorithms and models to use data for the decision-making activities of diagnosis and treatment. With CoT, many health applications or health services which were not executable on low capacity devices become executable with the cloud. Patients can be then remote monitored with appropriate reactions in time if necessary. In healthcare, some issues have been investigated: the lack of trust in data privacy by users, security, interoperability, streaming QoS, legal issues and how to dynamically increase the storage are commonly considered issues [34].

2. *Smart city*. Today, with the rapid growth of the population in our cities, the scarcity of natural resources and the environmental concerns, services and infrastructures should be more accessible, interactive and effective in order to tackle them. Smart cities have the ambition of improving our everyday life in many areas like public safety, tourism, transportation, urban consumption, and so on [12,35]. With the CoT, it is today possible to have a new generation of services and applications, which are capable to interact with the surrounding environment and thus creating new geo-awareness opportunities. In a number of smart cities, open data are used to organize some collected data, which requires providing a QoS level: availability, auto-scaling,

Figure 2.
Applications of CoT.

load balancing, security and privacy. Some of these requirements can be provided by the infrastructures of CC. Therefore, common issues and challenges are related to privacy and security reliability, heterogeneity, scale, resilience, and real-time interactions.

3. *Smart home.* One of the outstanding examples of CoT is Smart home. Users mainly act in home networks environment. We can find nowadays many smart objects in our homes. These smart objects are adapted to our needs. In home environments, we can found many CoT applications with the adoption of heterogeneous embedded devices integrated in CC, enabling the automation of commonly in–house activities [12,36]. A number of smart-home applications in literature involve sensor and actuators networks, and connect smart devices to the Internet in order to remotely manage, monitor or control them. Some examples are the smart metering, smart lighting, smart heating, and smart air conditioning, and intelligent management of energy consumption.

4. *Smart surveillance.* Intelligent video surveillance becomes a very important tool for several applications as far as security is concerned. Given the complexity enabled in

video analytics, it require Cloud-based solutions like Video Surveillance as a Service (VSaaS) in order to effectively satisfy the requirements of storage, management and processing of video contents obtained from video sensors. The CoT in that same context also leads to an automatic extraction of knowledge from scenes. Moreover, the proposed solutions of intelligent video surveillance are capable to deliver video streams to a non negligible number of user devices on the Internet.

5. *Smart energy and smart grid.* Smart grid and smart energy are enhanced by modern ICT (Information and Communications Technologies), monitoring and automation tools that allow a more efficient management of energy needs. The CC and IoT can be putted together to provide efficient and intelligent management of energy distribution and energy consumption in heterogeneous environments. For instance, a great economy of energy can be made by only providing lighting where and when strictly necessary. This is made possible by analyzing the information collected by various sensing nodes. Those sensing nodes have also networking and processing capabilities, but their resources are limited, so they have to be used intelligently.

6. *Smart mobility.* The automotive industry is changing with an increasingly fragmented customer base. The ownership of a car is replaced by shared mobility options for environmental sustainability and cost-effective options. Smart mobility is bringing a flexible transportation system including autonomous fleets and car electrification. So consumers should be able to adjust their transportation costs based on their individual needs. A new paradigm has emerged, Mobility as a Service (MaaS) and it can help to save a great amount of money. CoT can help in these transformations by proposing solutions to transportation systems and automobile services, which become Intelligent Transportation Systems (ITS) [37,38].

7. *Smart logistic.* With the introduction of CoT in logistics, business paradigms change radically because of the promotion of new modes of service. It is thenceforth more easy to automatically manage flows of goods from a departure point to an arrival point, while tracking these goods simultaneously in transit [39,40]. With CoT, conventional logistics systems are evolving into more sophisticated systems able to automatically deal with complexity and changes.

8. *Environmental monitoring.* In the domain of environmental monitoring, the CoT can help in the deployment of a high-speed information system that link the sensors and actuators deployed in the considered environment and the entity in charge of monitoring [39,41]. Some applications can be related to the water quality/level monitoring, pollution source monitoring, air quality and gas concentration in air monitoring, soil humidity monitoring, lighting conditions. Those monitoring can be continuous and long-term.

Certainly, the integration of IoT and CC can help to achieve a number of Internet goals in the future. It is nonetheless a process that has some difficulties. It generates several challenges and concerns such as security and privacy, standardization, power and energy efficiency, storage and manipulation of the large amount of data generated, management of network communications, scalability and flexibility, etc. In particular, privacy and security issues are of paramount importance. If a system can not assure both challenges of privacy and security, several consequences could be inquired. It is easy to imagine the danger if CoT devices spy on us and reveal our personal data with the real identity. The situation would be even worse if the critical applications of the IoT, for example, the nuclear reactor control system, the vehicle safety system or the medical devices were compromised. To ensure privacy and security in the CoT, viable and robust solutions must be considered.

3.2 CoT platforms

Designing CoT platforms can lead to the development of smart infrastructures, which enable intelligent applications. Many authors in the literature try to propose various architectures for CoT platforms in order to deal with the new concept of CoT. These platforms can be open source or proprietary. Unfortunately, they are concerned on addressing heterogeneity issues related to both IoT and the CC by implementing a middleware towards the Cloud and another one on the things' side, in addition to offering an API to ease the interaction with applications. We present in Table 1, the most common of these CoT platforms by reporting their main characteristics.

3.3 Challenges faced by CoT and issues involved

We discussed in the previous section how CoT provides many benefits and how its implementation could ease many processes in our lives. CoT encourages the improvement of some interesting applications in a considerable number of domains. Moreover, CoT scenario imposes many challenges (see Figure 3). In this section, the analysis of such challenges and issues involved. The prominent challenges raised by the application scenarios of CoT are listed hereinafter. (see Figure 4).

Platform	Integration	Data collection	Security	Analytic type	Energy efficient	Open source
OpenIoT [42]	REST	XGSN	oAUTH 2.0	-	Yes	Yes
Xively [43]	REST	MQTT, Sockets, Websockets HTTP(S)	SSL/TLS, Keys oAUTH 2.0 Password	RA	No	No
Nimbits [44]	REST	REST	oAUTH 2.0, Keys	RA	No	Yes
ThingSpeak [45]	REST	HTTP, ZigBee	Keys	Yes	No	Yes
CloudPlugs [46]	REST	PlugNet, MQTT, Websockets	PlugNet, SSL	RA	Yes	No
EvryThng [47]	REST	MQTT, CoAP, Websockets	TLS, oAUTH 2.0	RA	Yes	No
ThingWrox [48]	REST	REST, MQTT Websockets	E-t-E, R	RA, PA	–	No
AWS IoT [49]	REST	HTTP, MQTT, Websockets	TSL	BA, PA	Yes	No
MS Azure IoT hub [50]	REST	AMQP, HTTP	oAUTH 2.0, SAS	BA, PA	Yes	No
		MQTT Websockets	X.509			
KAA IoT [51]	REST	MQTT, HTTP, XMPP, REST CoAP	TLS, DTLS	BA	Yes	Yes
Oracle IoT [52]	REST	MQTT	E-t-E	RA, PA	Yes	No
SENSEi [53]	REST	COAP Sockets USB, REP	TA, R	RA	Yes	–
Paraimpu [54]	REST	–	TA	RA	–	No
Particle [55]	REST	COAP	Password oAUTH 2.0	–	–	Yes

Table 1. Selected CoT platforms and their main characteristics.

REST API: REpresentational State Transfer API; XGSN: An Open-source Middleware for the Web of Things; MQTT: Message Queuing Telemetry Transport; TA: Token-based Authentication; X.509: X.509 Certificate; Password: User/Password Authentication; E-t-E: End-to-End security; R: Roles for permissions.
RA: Real-time Analytics; BA: Batch Analytics; PA: Predictive Analytics.

Figure 3.
CoT challenges.

1. *Security and privacy.* Among the main concerns of CoT, privacy and data integrity have a great place. The main part of the exchanged data is about the user's personal information. Many issues as the protection of user's privacy and manufacturer's IP; the detection of malicious activity and how to block them, come under CoT security threats [32]. With CoT, the data transfer from the real world towards the Cloud is made possible. One particularly important issue that has not yet been addressed is how to provide appropriate authorization policies and rules while ensuring that only authorized users have access to the sensitive data.
2. *Heterogeneity.* The wide heterogeneity of devices as well as operating systems, cloud platforms and their available services, are important challenge in CoT. Due to the fact cloud services are typically embedded with proprietary interfaces, integration of resources becomes a not easy task given the customization and specificity of CoT service providers. This issue can become worse when services depend on a number of different providers.
3. *Big data.* With the huge amount of upcoming connected devices that are estimated to 50 billion by 2020, more specific attention must be paid to data transfer, storage,

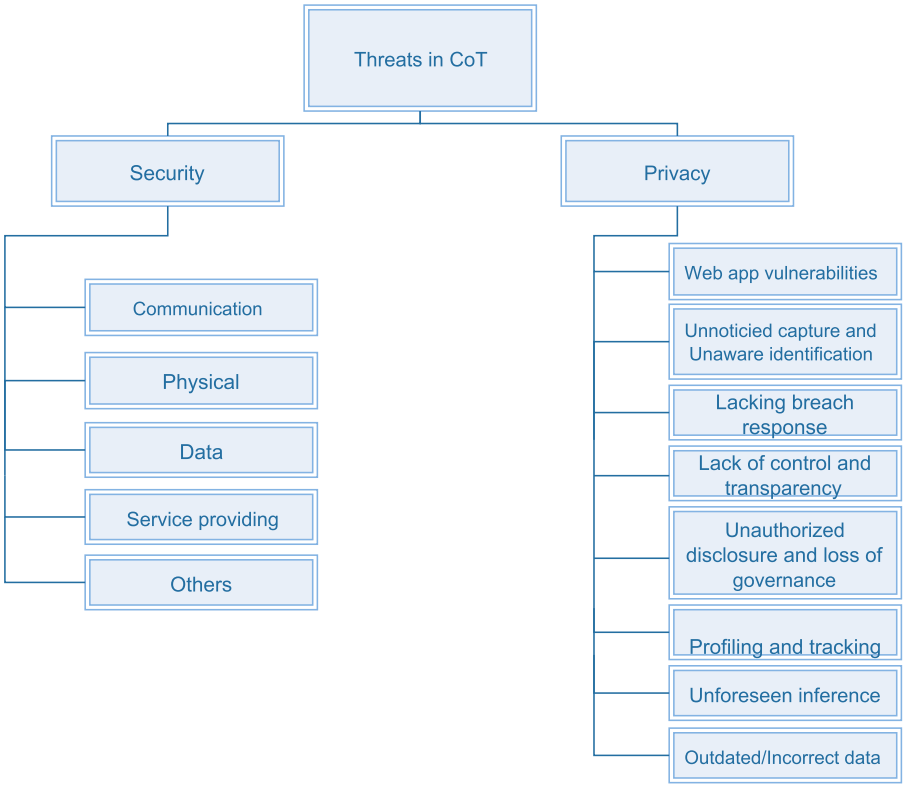

Figure 4.
Security and privacy threats.

processing and access of the enormous quantity of produced data. Therefore, IoT is among the main sources to big data, and the CC has the role of processing and storing these data. The need for scalable computing cloud platforms is real because mobile devices are ubiquitousness and sensor are pervasive and every day 2.5 quintillion bytes of data are generated [10,56]. Moreover, data integrity is an important aspect because of its impact on the QoS and also because of outsourced data privacy and security [57].

4. *Performance.* CoT applications require specific performances and QoS at many levels like for data transfer, communication, computation, and storage aspects. Particularly, obtaining good network performance towards the Cloud is a great challenge because bandwidth increase does not follow computation and storage evolution [39].

5. *Legal and social aspects.* With the CoT application, legal aspects are very important and actual in recent research concerns. For example, service providers must adapt the international regulations because cloud databases, providers and clients can be situated in different countries or continents. Social aspects are also an important challenge that interests the research community.

6. *Monitoring.* This is the mainly documented issue in the literature. Monitoring is an essential activity in the CC environments when it comes to security, performance, capacity planning, managing resources, and troubleshooting. Thus, CoT inherits the

same monitoring requirements from the CC, despite the fact that there are still some related challenges that are affected by velocity, volume, variety, and some characteristics of IoT.

7. *Scaling.* The CoT makes possible the design of new applications that aim at integrating and analyzing data that originated from IoT devices. Some depicted scenarios require interacting with a non negligible number of these devices, usually distributed throughout a number of areas [12,39]. The large scale behavior of the resulting systems raises new challenges harder to overcome.
8. *Fog computing.* It is a model that extends classic CC services to the edge of the network. The fog computing has been designed to support IoT applications which are latency constraints and require mobility as well as geo-distribution [58].
9. *Energy conservation.* Recent CoT applications need frequent data transmissions from smart devices towards the cloud, which quickly drains battery capacity of devices, thus limiting their continuous operation. Thus, energy saving as well as energy efficient management are very important challenges.
10. *Pricing and billing.* Pricing and billing in CoT is a major concern. Many different entities in CoT have their own systems of customers and services management, as well as their own payments and pricing methods [21]. Furthermore, the cost of keeping devices connected to the Cloud is quickly increasing while the cost of deploying them is decreasing.
11. *Standardization.* The confusion problem of unavailable standards is actually considered by researchers as a big issue in the CoT. Even if there are a number of contributions in the deployment and standardization of the CoT, there exists a necessity of standardizing architectures, protocols, and frameworks. This will facilitate the interconnection among heterogeneous devices and thus, the creation of smart services for the CoT [59].

4. Security and privacy threats on CoT

At large, preserving privacy has always been a fundamental human right. In the business context, privacy implies the protection and mostly an appropriate use of the customers' personal information. This use should meet expectations of customers. As weel, in business entities information systems, privacy refers to the application of laws, standards, policies and processes by which personal information is managed. In order to be in the same focus, in this paper, the notion of security refers to information security, which is defined by the ISO 27001 standard as the preservation of confidentiality, integrity, availability as well as accountability, authenticity, reliability and non-repudiation can also be involved [60–62]. Commonly, some security practitioners consider confidentiality equated with privacy. But it is an error. For the standard ISO 27001 of 2005, Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities or processes [63]. In this section, after comparing conventional security and security in IoT paradigm, we make an overview on security challenges in CoT. We also present the privacy and security threats as well as feasible solutions are discussed.

4.1 Conventional and IoT security

In this context, IoT refers to the interconnection of large heterogeneous networks of things in different communication models including human-to-human (H2H), human-to-machine (H2M), and object-to-object or machine-to-machine (M2M). Its specific end goal is to provide

advanced and intelligent services to users. Connected objects such as sensors, actuators and mobile devices, monitor the environment and collect all kinds of data in real time. In an IoT model, devices equipped with sensors know how to deliver lightweight data gathered around them, allowing cloud resources to extract data from actuators, which improve communication between the nodes. As a major gathering platform for the development of constrained devices in IoT, WSNs have been widely studied a number of methods and algorithms for securing WSNs have been proposed in the literature. In another hand, communication between the Internet and sensor nodes should satisfy the following criteria in order to be well secured: reliability, secrecy, verification, and non-revocation.

However, the IoT security and privacy issues are distinct from those of conventional wireless networks and others; this in terms of deployment and technology. Therefore, IoT networks are commonly deployed on environments constrained by energy, processing and storage [64]. These constraints make sensors impossible for public key encryption to secure the devices. Because of these characteristics of IoT devices, it is a necessity to use a lightweight encryption technology for security and privacy of devices and data. This technology implies a lightweight cryptographic algorithm. Data loss here is due to node spoofing. erroneous control messages can be sent by an attacker.

Furthermore, in the network layer, security issues can be man-in-the-middle attacks and counterfeiting. During these two attacks, false information can be captured and sent to the nodes involved in communication. Unallowed nodes are blocked by the mechanisms of identity authentication and data privacy. For instance, a lightweight and robust certificateless signature mechanism has been proposed by Zhang et al. [65] in CoT. Moreover, at the application layer, data sharing is the main feature. Security issues here are in data privacy, access control, and disclosure of information. Therefore, the security architectural design for conventional networks is not applicable for machine-to-machine communication. It is more for users.

4.2 Security threats

despite the fact that the research on the security in the CoT is still in progress, there is some existing works that analyzes the outlined challenges and some possible protection schemes. Hence, a number of existing threats can strongly compromise the security of CoT system. Security threats in CoT are in different forms including communication threats, physical threats, data threats, service provisioning threats and other threats.

4.2.1 Communication threats. Here the communication channel within a CoT system can be abused by an attacker to initiate various threats.

1. *Denial of Service (DoS).* A non negligible number of DoS attacks can be launched against the CoT. This attack can reduce or remove a the capacity of a network to execute its expected function through hardware failures, resource exhaustion, software bugs and malicious broadcasting of high-energy signals. Due to the limitations of devices, CoT is especially vulnerable to the DoS attack [24,66].

2. *Eavesdropping.* It refers to a real-time unauthorized interception of a private communication. Attacker gain access to communication channels and exploit them to extract the data during interactions between diverse entities within a system [66].

3. *Spoofing attack.* In this attack, a malicious party try to mimic another device on the network or impersonate a user on a network in order to launch attacks against network nodes, spread malware, steal data and bypassing access control mechanisms. A number of kinds of spoofing attacks exist, among which, IP spoofing and ARP spoofing [60,67].

4. *Man-in-the-middle (MITM) attack.* It is a common type of cybersecurity attack that allows attacker to eavesdrop on the communication between a legitimate sender and a legitimate receiver without their knowledge. He can then intercept the sensitive data packet during data transmission and replace them with fraudulent ones [68,60].

5. *Replay attack.* The scenario of this attack relies on an unsecured network in which an attacker can capture the data traffic and then resend the captured packets later in order to obtain unauthorized access to the targeted network resources. The resources of the node or the system can also be wasted by this attack, thereby inducing a mild DoS.

4.2.2 Physical threats. Physical threats refer to causes of physical incidents that may lead to loss and physical damage on devices. Physical threats can be classified into three main categories: internal (fire, humidity, unstable power supply, etc), external (lightning, earthquakes, floods, etc) and human (theft, errors which can be accidental or intentional, vandalism of the infrastructures, etc). Below is another description of the identified threats.

1. *Device capture.* An attacker can capture the devices and extract information before they are transmitted and securely stored in the system. Device and network security are two of the major challenges to be considered in the design of a secure architecture of constrained devices [69,70].

2. *Node damaging.* With physical access to the IoT devices, an attacker can physically damage one of them. A damaged device is unsuitable to sense and transmit any data. A DoS attack can be launched if many devices are damaged. So, the system will be unusable for providing any services that rely on such data [71,60].

3. *Side channel attack.* This security violation refers to is any attack based on information gained on the implementation of the system. It relies on the fact that logical functionalities may exhibit some deterministic physical characteristics depending on the input data. Inference can be made from these characteristics. Those inferences can be exploited to compromise the system security.

4.2.3 Data threats. For common Internet users, data threats are one of the most common threats to cybersecurity. Spams can be sent, security settings can be disabled, data can be corrupted and stolen. We present here the threats and their corresponding attacks that rely on data generated by a CoT system.

1. *Threats during data retrieval from devices, transfer, and storage.* If an attacker can get physical access to an IoT device, he could retrieve raw sensed data by tampering the device via reverse engineering or micro-probing. Normally, collected data need to be transferred to the cloud system for storage and further analysis. So, there is a high risk of data tampering during the transfer or during the storage [72].

2. *Deployment of unauthorized device.* Unauthorized devices may be deployed to the CoT environment by an attacker. If the authenticity of a device is not established, his data must not be accepted. The system must accept just the data gathered by only properly authenticated and authorized devices, if not, the trustworthiness of the CoT system can not be guaranteed [73].

3. *Key compromization and the breakage of cryptographic protocols.* The developer can use weak cryptographic protocols because of the limited resources of IoT devices. That mechanism can be easily breakable. An attacker can get the cryptographic keys, he can compromise them or use them to compromise the security of the system and its users [60].

4. *False data injection.* An attacker can deploy unauthorized or unauthenticated IoT devices or even reverse engineer of a well authenticated and authorized device in order to inject false data into the system. Those data would compromise the system security [74].
5. *Data loss and leakage.* This problem could occur for many accidental reasons as fire, earthquake and deletion by the service provider. Malicious insiders, weak access control mechanism and weak encryption algorithm can also cause data leakage.
6. *Data breaches.* Unauthorized entities can access data and data breaches can occur at any level in a system. The origin might be from outside or inside the system [75].

All Data in a CoT system can not have the same level of sensitivity. Some data as medical or financial data are more sensitive than others, and then need more attention and more care should be taken for it. If not, privacy could be easily invaded.

4.2.4 Service provisioning threats. In a CoT system, many different services and applications are used to ensure smooth operations. The threats here are related to those different services.

1. *Unidentified and unauthorized access.* Services in a CoT system must ensure that unidentified and unauthorized users cannot access data, even sensitive or not. A user can also gain more privileges than normally, which allows him to access sensitive data and analysis. This may result from a problem in the authorization infrastructure [60].
2. *Identity theft.* Key pieces of personal information of a valid user can be obtained by the attacker. With this information, he can gain illegal access to restricted services and resources. The victim can lose his data and can be held accountable for the attacker's actions [76].
3. *Service hijacking.* It is a particular kind of network security attack in which the attacker takes control of a communication between two entities and masquerades as one of them. A user, in a service hijacking attack, while trying to access a valid service, is redirected to an illegal one controlled by the attacker [60].
4. *Insecure or compromising interfaces and API.* It is counted among the top threats in the cloud, because the cloud provider always distributes a set of API that helps consumers to retrieve data and get access to other services [75]. If the interface is not well protected, an attacker can easily exploit his weakness and launch fraudulent services using legitimate data [77,78].

4.2.5 Other threats. Here are various threats which are not related to any of the previous categories.

1. *Malicious insiders.* An insider attack is a malicious attack perpetrated on a network system by a person having access authorization to the system or to sensitive data. The insider may exploit such access to abuse the data and services.
2. *Shared technology issues.* There are many shared resources in a CoT system. These resources might be used via virtualization through multi tenancy architecture. This fact might allow accessing to the virtual machine (VM) of another user [79]. This VM Monitor can have vulnerabilities and a malicious user could exploit it to gain access to another user's VM.
3. *Abusing cloud computing.* With the CC, one of the biggest advantages is that it allows organizations to avail an enormous volume of computing power. However, a

drawback comes with this opportunity as it allows anyone to abuse such computing power to launch attacks. A single attacker can rent out many computer power to launch DoS attacks to another cloud service provider [80].

4.3 Privacy threats

The evolving nature of the CoT as far as technologies and features are concerned by privacy threats. Also, the emerging new ways of interaction in CoT lead to specific privacy threats. Many threats can be exploited to pervade the privacy of some users in a CoT system.

- *Vulnerabilities in web applications.* Only one vulnerability can cause a major data breach. Companies have to keep their patching procedures in order, if not, hackers can exploit vulnerabilities and enter the system.
- *Unnoticed capture and unaware identification.* A deployed IoT device can collect data about users in an extremely discrete way. It can be a small size camera or a small size sensor. Such data, captured without the knowledge and/or the consent of the concerned users, can ultimately be analyzed to identify users and invade their privacy [60].
- *Lacking breach response.* It is possible to have incident even with the best security control procedures. Companies can not prevent all incident, but they can do their best and the maximum will be prevented. They have to be prepare to provide adequate response to minimize the impact of attacks. team.
- *Lack of control and transparency.* Once collected data about users are uploaded to the cloud, sometimes, they may not have access to those data. Even when they, have access to them, users have no or limited control over them. The ubiquitous sensing process which may capture data makes it very difficult for the users to express their consent regarding data collection or what to do with such collected data while they are processed, analyzed, presented and shared in a system. Without such controls it is difficult to create access control rules in a system which can protect the privacy. To efficiently preserve the privacy in a system, consent is a major requirement for collecting, storing and processing personal information. In this light, an access control mechanism that takes on sensitive information has been designed in [81] and well applied on the smart health domain. To consent to something, you might be able to understand what you are consenting to.
- *Unauthorized disclosure and loss of governance.* While using the cloud infrastructures, It is essentially the cloud provider who control the operations, which might impact the customers privacy. The difficulty to collect consent and/or even notify users about data collection and processing might result in unauthorized disclosure of sensitive data.
- *Profiling and tracking.* Sensors deployed in different environments collect data which can be tied to a particular user. So, there is a risk of creating a fake profile of that user and then track him without his knowledge.
- *Unforeseen inference.* An attacker can comprehensively analyze Data from different sensors using extensive computing power of the cloud. Such analysis can lead up to unforeseen inference about any user. The result of such inference is knowledge which could be exploited to invade the privacy of the user, or even worse, to create inference for future events which were not possible otherwise.
- *Outdated or incorrect personal data* Outdate or incorrect personal data have to be rectified. For example, in a medical database, the report of a patient that has been first

diagnosed a specific illness, but stated later not to be afflicted. It can be very dangerous if this kind of information are not updated. Companies should make sure that personal data are current and accurate.

Furthermore, cybercriminals are not unfortunately the only privacy threat sources. Sometimes the companies themselves to whom we entrust our data and in which we trust, are the first to manipulate our data without our consent. They sometimes use private information to their gain without considerations to individual's rights. After discussions on security and privacy threats on CoT, the next section is dedicated to the existing solutions addressing these threats as well as the open challenges.

5. Security and privacy solutions for CoT: a brief revue and open challenges

5.1 Literature revue

In the literature, authors proposed many techniques and methods to secure the CoT and ensure data privacy.

Bhattasali et al. [61] present an insight into the security challenges in the environment of CoT with a focus on security and trust. The authors proposed the concept of secure trusted things as a service that aims at reducing the number of privacy and security issues in CoT. The scheme proposed by authors includes an encryption mechanism that enables less overhead. Furthermore, a trust model that enables real-time decision making is the main focus of the proposal. In [82], Alohali et al. proposed a CoT based simple and secure scheme for a smart home. The proposal defines how a device is served from the CoT to bring it back into the secure zone. The authors illustrate how the requirements in terms of security are managed from the CoT and propose a group key management scheme for smart housing. The proposed security ensure a secure data transfer. For secure communication between the devices, symmetric key cryptography is deployed. After security analysis of their scheme, they claim that it is easy to implement, flexible and energy efficient.

Zhu et al., [83] introduced an authenticated reputation and trust computing and management (ATRCM) system for the integration of CC and WSN. To demonstrate the effectiveness of ATRCM, analysis, design and further functionality evaluation results are presented, followed with system security analysis. In [84], Bai and Rabara proposed an integrated secured and intelligent architecture for the IoT and Cloud. This intelligent architecture is suitable for the public to access various smart applications in the cloud, no matter the position, the time, the device and the network. Moreover, in order to ensure complete protection against security threats, Elliptic Curve Cryptography (ECC) has been used. This architecture is without ambiguity, it ensures security with improved performance and helps to realize the vision of "one intelligent smart card for any applications and transactions".

Lee et al. [85] affirmed that the adoption of IoT and fog introduces several particular security concerns. They first discussed the concept of the IoT fog and the existing security measures and then, explore potential threats. They highlighted the need for securing the fog computing environment by using some security technologies. In this light, Henze et al. [86] designed their solution, UPECSI, for User-driven Privacy Enforcement for Cloud-based Services in the IoT. The proposed scheme takes a whole approach to ensure privacy in the CoT by providing an integrated solution that concentrates on the end-users and developers of cloud services individually and together. The approach consists of organizational processes and many technical components. Kumari et al. [87] designed a biometrics-based authentication scheme for multi-cloud-server environment. It uses biometric hashing and the ECC as building blocks. Then the efficiency and performance of the proposed scheme is analyzed to proof its utility. They also compare it with related contemporary schemes for the

evaluation. Besides, Alrawais et al. [88], make investigation and discussion about security and privacy challenges of introducing fog computing in IoT environments. In the context of fog computing coupled with IoT applications, authentication is among one of the challenges that need a particular attention.

In [31], Vasic et al. proposed an adaptable model for securing communication in CoT environment in contrast to the existing pre-configured solutions. The proposed model defines a number of secure communication operations that enable CoT entities to dynamically and autonomously agree on the security protocol and the used cryptographic keys. The authors verified their solution by implementing a prototype of CoT device agreement based on the required security level.

In [89], Sahmim et al. propose in their review paper some privacy solutions to get into some of CoT issues as confidentiality. Many techniques are developed and they propose two classifications of them: techniques and methodologies. Techniques include: encryption, processing encrypted data, obfuscation, anonymization, sticky policy, trusted platform module, data segmentation and trusted third party mediator. For the methodologies, we have: identity, access, security and key management.

In [90], Pacheco et al. propose an architecture that helps to preserve privacy in CoT. With this architecture, users can fully control the access to the data stored in the cloud and generated by their devices, part of the IoT networks. This architecture is supposed to enable fine-grained control over data, because privacy and controls are implemented on the IoT devices instead of at the network border. This component could also represent a single point of failure, it could harm the security of the system if an attack is successful.

In [91], Wang et al. constructed a privacy preserving message forwarding scheme intended for opportunistic CoT in order to guarantee the privacy and to improve transmission efficiency. First of all, they develop an architecture of a cloud server, with two layers in order to improve the communication efficiency of clients. Then, after the integration of a security-based mobility prediction algorithm together with a routing decision scheme, their proposal can effectively protect individual privacy.

In [92], Stergiou et al. proposed a method to secure CoT. They first presented both concepts of IoT and CC. They focused on the security issues in both technologies. After discovering of the benefits of their integration, they surveyed the security challenges of this integration. The authors proposed a new method which improve the privacy and security issues in the CoT.

In [24], Alohali list some of them as the using of private cloud with enterprise parameter, the use of session containers, the encryption of content, the cloud access brokers and the runtime security visualization.

- *Private cloud.* Involves the establishment of a virtual infrastructure inside the corporate firewall. Here, data and applications in the cloud are easily accessible to only authenticated users.
- *Content encryption.* It helps in the protection of the confidentiality of content that you add to a database in case the content is accessed outside. The encryption is related only ta data in the storage area.
- *Session containers.* it ensure the security of the public clouds by helping the user in the initiation of a relatively secure connection that maintains end-to-end closure.
- *Cloud access brokers.* A broker is used to monitor the authentication path from users and provide enhanced security [24].
- *Runtime security visualization.*it implies the dynamic establishment of runtime security visualization.

5.2 Open challenges on security and privacy

It is an absolute necessity to well manage access, usage of available IoT resources and communication between different entities of a CoT system. The access and usage of resources has to be secure and transparent and with no waste. There is a need of secure communication between IoT devices and cloud infrastructure, what is crucial to preserve individual privacy and security in the CoT context. Unfortunately, the integration of IoT environments with the cloud has generated a new set of challenges. Therefore, an implementation of a CoT require further transformation of cloud technologies to well manage the data flow and the data source ownership within CoT environments. Since data can be accessed by third parties and IoT resource are virtualized, new interrogations regarding source of data ownership, verifiable data origin and data trustworthiness are created and need to be addressed. Furthermore, eavesdropping and monitoring without the consent and the knowledge of the observed person is another serious problem.

In the CoT context, devices can have ad hoc interconnections and they can also communicate with a back-end cloud. Hence the need to secure communications. For Vasic et al. [31], securing communications requires an agreement protocol which will enable all communicating parties to agree each other on a cryptographic algorithm and keys used to protect the communication in the exchanged messages. In CoT environments, there is a need of flexible and adaptable agreement mechanisms because of the limitations of IoT devices in terms of storage, computing and bandwidth resources. The key challenges and obstacles to practical security on CoT and the available technology solutions are given hereinafter:

- *Dynamic activity cycle.* Connected devices may realize different roles and functions linked with security challenges of CoT. They may transmit data to other devices or directly to cloud servers.
- *Heterogeneous interactions.* In CoT, connected devices are extremely heterogeneous since they are made by different manufacturers who use different protocols, standards and technical requirements. So, home devices cannot be all homogeneous and interoperable. Due to the heterogeneity of protocols and technical features of connected devices, implementing new light cryptographic algorithms for securing end-to-end secure communication channel becomes a necessity [93].
- *Anti-virus provision.* Anti-virus suites are normally used in classic networks to protect PCs from malware and attacks [94]. Theses suites are memory-consuming. It is very difficult and a great challenge to provision the connected devices with these anti-virus protection.
- *Small packets vulnerability.* Normally, IoT devices are built based under the IEEE 802.15.4 standard created for low-rate wireless personal area network which is a standard supporting 127 byte packets at the physical layer [24]. With this architecture, large packets of security protocols may be fragmented. As a result, new attacks can occur, as Denial of Service (DoS) attacks.

Moreover, challenges about the security issue in the integration of IoT and CC include: heterogeneity, performance, reliability, Big Data, and monitoring Hence, some open research challenges for the enhancement of security and privacy issues in IoT environments using fog computing can be summarized as follow: privacy, updating IoT devices, secure and Efficient protocols, authentication, attack detection, location verification, and access control.

6. Conclusion

The Concept of CoT which is from the combination of modern cloud technology and IoT represents a big leap ahead in the future Internet. The new applications arising from the CoT

technology is a new exciting direction for both business and research. The CoT concept is very relevant to handle and analyze large volumes of data. Thus, considerations of privacy and security become critical. This paper shows how the CoT paradigm arises from the combination of Cloud and IoT in their complementary aspects. It then presents that concept, its architecture and some of its applications. The paper demonstrates that the creation of CoT system faces many challenges and risks, linked with specific characteristics of things. In particular, privacy and security threats related to the resource-constrained nature of the CoT devices were discussed. The paper also presents the literature review on security in CoT. The future research should address the issue of security and privacy in CoT environments. These issues are both critical research ones, they have received a great deal of attention and are still open issues that require more attention.

References

[1] H. Rahman, R. Rahmani, Enabling distributed intelligence assisted Future Internet of Things Controller (FITC), Appl. Comput. Inf. 14 (1) (2018) 73–87.

[2] A.A.A.Ari, A.M.Gueroui, C.Titouna, O.Thiare, Z.Aliouat, Resource allocation scheme for 5G C-RAN: a Swarm Intelligence based approach, Comput. Netw. 165.

[3] L. Atzori, A. Iera, G. Morabito, Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm, Ad Hoc Netw. 56 (2017) 122–140.

[4] A. Farahzadi, P. Shams, J. Rezazadeh, R. Farahbakhsh, Middleware technologies for cloud of things: a survey, Digital Commun. Netw. 4 (3) (2018) 176–188.

[5] C. Dupont, A. Wussah, S. Malo, O. Thiare, F. Niass, C. Pham, S. Dupont, F. Le Gall, P. Cousin, Low-Cost IoT Solutions for Fish Farmers in Africa, in: 2018 IST-Africa Week Conference (IST-Africa), IEEE, 2018, p. 1.

[6] R.Hamidouche, Z.Aliouat, A.M.Gueroui, A.A.A.Ari, L.Louail, Classical and bio-inspired mobility in sensor networks for IoT applications, J. Netw. Comput. Appl.

[7] C.V.Networking, Cisco Global Cloud Index: Forecast and Methodology, 2016–2021 White Paper, Cisco Public, San Jose, CA, USA.

[8] G.A. Akpakwu, B.J. Silva, G.P. Hancke, A.M. Abu-Mahfouz, A survey on 5G networks for the Internet of Things: communication technologies and challenges, IEEE Access 6 (2018) 3619–3647.

[9] M. Collotta, G. Pau, T. Talty, O.K. Tonguz, Bluetooth 5: a concrete step forward toward the IoT, IEEE Commun. Mag. 56 (7) (2018) 125–131.

[10] A.C. Djedouboum, A.A.A. Ari, A.M. Gueroui, A. Mohamadou, Z. Aliouat, Big data collection in large-scale wireless sensor networks, Sensors 18 (12) (2018) 4474.

[11] S. Sahraoui, A. Bilami, Efficient HIP-based approach to ensure lightweight end-to-end security in the internet of things, Comput. Netw. 91 (2015) 26–45.

[12] M. Díaz, C. Martín, B. Rubio, State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing, J. Netw. Comput. Appl. 67 (2016) 99–117.

[13] A. Botta, W. De Donato, V. Persico, A. Pescapé, On the integration of cloud computing and internet of things, in: 2014 International Conference on Future Internet of Things and Cloud, IEEE, 2014, pp. 23–30.

[14] A. Aissioui, A. Ksentini, A.M. Gueroui, T. Taleb, On enabling 5G automotive systems using follow me edge-cloud concept, IEEE Trans. Veh. Technol. 67 (6) (2018) 5302–5316.

[15] A.A.A. Ari, I. Damakoa, C. Titouna, N. Labraoui, A. Gueroui, Efficient and scalable ACO-based task scheduling for green cloud computing environment, in: 2017 IEEE International Conference on Smart Cloud (SmartCloud), IEEE, 2017, pp. 66–71.

[16] V. Chang, Towards a big data system disaster recovery in a private cloud, Ad Hoc Netw. 35 (2015) 65–82.

[17] P. Sethi, S.R. Sarangi, Internet of things: architectures, protocols, and applications, J. Electr. Comput. Eng. (2017).

[18] F. Bonomi, R. Milito, J. Zhu, 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, ACM, 2012, pp. 13–16.

[19] D. Evans, The internet of things: how the next evolution of the internet is changing everything, CISCO White Paper 1 (2011) (2011) 1–11.

[20] R. Lavanya, Fog computing and its role in the internet of things, in: Advancing Consumer-Centric Fog Computing Architectures, IGI Global, 2019, pp. 63–71.

[21] A. Botta, W. De Donato, V. Persico, A. Pescapé, Integration of cloud computing and internet of things: a survey, Future Gen. Comput. Syst. 56 (2016) 684–700.

[22] B. Mokhtar, M. Eltoweissy, Big data and semantics management system for computer networks, Ad Hoc Netw. 57 (2017) 32–51.

[23] J. Singh, T. Pasquier, J. Bacon, H. Ko, D. Eyers, Twenty security considerations for cloud-supported Internet of Things, IEEE Internet of Things J. 3 (3) (2016) 269–284.

[24] B. Alohali, Security in Cloud of Things (CoT), in: Cloud Security: Concepts, Methodologies, Tools, and Applications, IGI Global, 2019, pp. 1188–1212.

[25] V. Adat, B. Gupta, Security in Internet of Things: issues, challenges, taxonomy, and architecture, Telecommun. Syst. 67 (3) (2018) 423–441.

[26] N. Deepa, P. Vijayakumar, B.S. Rawal, B. Balamurugan, An extensive review and possible attack on the privacy preserving ranked multi-keyword search for multiple data owners in cloud computing, in: 2017 IEEE International Conference on Smart Cloud (SmartCloud), IEEE, 2017, pp. 149–154.

[27] F. Khedim, N. Labraoui, A.A.A. Ari, A cognitive chronometry strategy associated with a revised cloud model to deal with the dishonest recommendations attacks in wireless sensor networks, J. Netw.Comput. Appl. 123 (2018) 42–56.

[28] N. Labraoui, M. Gueroui, L. Sekhri, A risk-aware reputation-based trust management in wireless sensor networks, Wireless Pers. Commun. 87 (3) (2016) 1037–1055.

[29] M. Aazam, I. Khan, A.A. Alsaffar, E.-N. Huh, Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved, in: Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th-18th January, 2014, IEEE, 2014, pp. 414–419.

[30] M.M. Mahmoud, J.J. Rodrigues, S.H. Ahmed, S.C. Shah, J.F. Al-Muhtadi, V.V. Korotaev, V.H.C. De Albuquerque, Enabling technologies on cloud of things for smart healthcare, IEEE Access 6 (2018) 31950–31967.

[31] V. Vasić, A. Antonić, K. Pripužić, M. Mikuc, I.P. Žarko, Adaptable secure communication for the Cloud of Things, Software: Practice Exp. 47 (3) (2017) 489–501.

[32] A. Khanna, An architectural design for cloud of things, Facta Universitatis Series: Electron. Energ. 29 (3) (2015) 357–365.

[33] S. Distefano, G. Merlino, A. Puliafito, Enabling the cloud of things, in: Mobile and Internet Services in Ubiquitous Computing in: 2012 Sixth International Conference on Innovative, IEEE, 2012, pp. 858–863.

[34] A.M.-H.Kuo, Opportunities and challenges of cloud computing to improve health care services, J. Med. Internet Res. 13 (3).

[35] W. He, G. Yan, L. Da Xu, Developing vehicular data cloud services in the IoT environment, IEEE Trans. Industr. Inf. 10 (2) (2014) 1587–1595.

[36] S.S.Gill, P.Garraghan, R.Buyya, ROUTER: fog enabled cloud based intelligent resource management approach for smart home IoT devices, J. Syst. Softw.

[37] M.L. Mfenjou, A.A.A. Ari, W. Abdou, F. Spies, *et al.*, Methodology and trends for an intelligent transport system in developing countries, Sustain. Comput.: Inf. Syst. 19 (2018) 96–111.

[38] M.L.Mfenjou, A.A.A.Ari, A.N.Njoya, D.J.F.Mbogne, W.Abdou, Kolyang, F.Spies, Control points deployment in an intelligent transportation system for monitoring inter-urban network roadway, J. King Saud Univ. Comput. Inf. Sci.

[39] H.F. Atlam, A. Alenezi, A. Alharthi, R.J. Walters, G.B. Wills, Integration of cloud computing with internet of things: challenges and open issues, in: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2017, pp. 670–675.

[40] Y.S. Patel, T. Parmar, Cloud of Things: a state-of-the-art review on integration of internet of things with cloud computing, in: National Conference on Contemporary Computing(NC3-2016), Int. J. Comput. Appl. (0975–8887) (2016) 37–41.

[41] R. Hamidouche, Z. Aliouat, A.A.A. Ari, A.M. Gueroui, An efficient clustering strategy avoiding buffer overflow in IoT sensors: a bio-inspired based approach, IEEE Access (2019) 1–19, http://dx.doi.org/10.1109/ACCESS.2019.2943546.

[42] J. Soldatos, N. Kefalakis, M. Hauswirth, M. Serrano, J.-P. Calbimonte, M. Riahi, K. Aberer, P.P. Jayaraman, A. Zaslavsky, I.P. Žarko, *et al.*, Openiot: open source internet-of-things in the cloud, in: Interoperability and open-source solutions for the internet of things, Springer, 2015, pp. 13–25.

[43] N. Sinha, K.E. Pujitha, J.S.R. Alex, Xively based sensing and monitoring system for IoT, in: 2015 International Conference on Computer Communication and Informatics (ICCCI), IEEE, 2015, pp. 1–6.

[44] B. Sautner, Nimbits, 2017.

[45] M.A.G.Maureira, D.Oldenhof, L.Teernstra, ThingSpeak – An API and Web Service for the Internet of Things, Leiden Institute of Advanced Computer Science.

[46] A. Atmosudiro, M. Faller, A. Verl, Seamless integration of production data in the cloud, wt-online 3–2014, Springer VDI 104 (2014) 151–155.

[47] D. Guinard, V. Trifa, Building the web of things: with examples in node. js and raspberry pi, Manning Publications Co., 2016.

[48] ThingWorx, Enterprise IoT Solutions and Platform Technology. https://www.thingworx.com.

[49] W. Tärneberg, V. Chandrasekaran, M. Humphrey, Experiences creating a framework for smart traffic control using AWS IOT, in: Proceedings of the 9th International Conference on Utility and Cloud Computing, ACM, 2016, pp. 63–69.

[50] S. Klein, IoT Solutions in Microsoft's Azure IoT Suite, Springer, 2017.

[51] M.A. da Cruz, J.J. Rodrigues, A.K. Sangaiah, J. Al-Muhtadi, V. Korotaev, Performance evaluation of IoT middleware, J. Netw. Comput. Appl. 109 (2018) 53–65.

[52] O. IoT, Oracle Internet of Things Cloud Service. https://www.oracle.com/internet-of-things/.

[53] M. Presser, P.M. Barnaghi, M. Eurich, C. Villalonga, The SENSEI project: integrating the physical world with the digital world of the network of the future, IEEE Commun. Mag. 47 (4) (2009) 1–4.

[54] A. Pintus, D. Carboni, A. Piras, Paraimpu: a platform for a social web of things, in: Proceedings of the 21st International Conference on World Wide Web, ACM, 2012, pp. 401–404.

[55] P. IoT, Platform San Francisco Busi- ness. https://www.particle.io.

[56] C. Dobre, F. Xhafa, Intelligent services for big data science, Future Gen. Comput. Syst. 37 (2014) 267–281.

[57] C. Liu, C. Yang, X. Zhang, J. Chen, External integrity verification for outsourced big data in cloud and IoT: a big picture, Future Gen. Comput. Syst. 49 (2015) 58–67.

[58] Z.Su, F.Biennier, Z.Lv, Y.Peng, H.Song, J.Miao, Toward architectural and protocol-level foundation for end-to-end trustworthiness in Cloud/Fog computing, IEEE Transactions on Big Data.

[59] G. Suciu, A. Vulpe, S. Halunga, O. Fratu, G. Todoran, V. Suciu, Smart cities built on resilient cloud computing and secure internet of things, in, 19th international conference on control systems and computer science, in: 2013 19th International Conference on Control Systems and Computer Science, IEEE, 2013, pp. 513–518.

[60] M.S. Ferdous, R. Hussein, A. MadiniAlassafi, R. Walters, G. Wills, Threat taxonomy for Cloud of Things, Internet of Things and Big Data Analysis: Recent Trends and Challenges 1 (2016) 149–191.

[61] T. Bhattasali, R. Chaki, N. Chaki, Secure and trusted cloud of things, in: 2013 Annual IEEE India Conference (INDICON), IEEE, 2013, pp. 1–6.

[62] M. Babaghayou, N. Labraoui, A.A.A. Ari, EPP: Extreme Points Privacy for Trips and Home Identification in Vehicular Social Networks, in: 3rd edition of the National Study Day on Research on Computer Sciences (JERI2019), Saida, Algeria, 2019. http://ceur-ws.org/Vol-2351/paper_67.pdf.

[63] S. Pearson, Privacy, security and trust in cloud computing, in: Privacy and Security for Cloud Computing, Springer, 2013, pp. 3–42.

[64] W.M.El-Sayed, H.M.El-Bakry, S.M.El-Sayed, Integrated data reduction model in wireless sensor networks, Appl. Comput. Inf.

[65] Y.Zhang, R.Deng, D.Zheng, J.Li, P.Wu, J.Cao, Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT, IEEE Trans. Ind. Inf.

[66] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Netw. 57 (10) (2013) 2266–2279.

[67] S.Vidalis, O.Angelopoulou, Assessing identity theft in the Internet of Things, J. IT Convergence Practice.

[68] I. Stojmenovic, S. Wen, The fog computing paradigm: Scenarios and security issues, in: 2014 Federated Conference on Computer Science and Information Systems, IEEE, 2014, pp. 1–8.

[69] F.A. Alaba, M. Othman, I.A.T. Hashem, F. Alotaibi, Internet of Things security: a survey, J. Netw. Comput. Appl. 88 (2017) 10–28.

[70] A. Akhunzada, A. Gani, N.B. Anuar, A. Abdelaziz, M.K. Khan, A. Hayat, S.U. Khan, Secure and dependable software defined networks, J. Netw. Comput. Appl. 61 (2016) 199–221.

[71] K. Zhao, L. Ge, A survey on the internet of things security, in: 2013 Ninth International Conference on Computational Intelligence and Security, IEEE, 2013, pp. 663–667.

[72] S. Babar, A. Stango, N. Prasad, J. Sen, R. Prasad, Proposed embedded security framework for internet of things (iot), in: 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), IEEE, 2011, pp. 1–5.

[73] P. Mahalle, S. Babar, N.R. Prasad, R. Prasad, Identity management framework towards internet of things (IoT): Roadmap and key challenges, in: International Conference on Network Security and Applications, Springer, 2010, pp. 430–439.

[74] N. Komninos, E. Philippou, A. Pitsillides, Survey in smart grid and smart home security: issues, challenges and countermeasures, IEEE Commun. Surveys Tutor. 16 (4) (2014) 1933–1954.

[75] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, J. Netw. Comput. Appl. 34 (1) (2011) 1–11.

[76] C. Modi, D. Patel, B. Borisaniya, A. Patel, M. Rajarajan, A survey on security issues and solutions at different layers of Cloud computing, J. Supercomput. 63 (2) (2013) 561–592.

[77] S.B. Chebrolu, V. Bansal, P. Telang, Top 10 cloud risks that will keep you awake at night, CSICO. Available at: https://www.owasp.org/images/4/47/Cloud-Top10-Security-Risks.pdf.

[78] D. Catteddu, G. Hogben, The European Network and Information Security Agency (ENISA) is an EU agency created to advance This work takes place in the context of ENISA's Emerging and Future Risk programme. C ONTACT DETAILS: this report has been edited by, Computing 72 (1) (2009) 2009–2013.

[79] B.O.Yenke, A.A.Ari, C.D.Mbeuyo, D.A.Voundi, Virtual Machine Performance upon Intensive Computations, GSTF J. Comput. 4 (3).

[80] K. Hashizume, D.G. Rosado, E. Fernández-Medina, E.B. Fernandez, An analysis of security issues for cloud computing, J. Internet Services Appl. 4 (1) (2013) 5.

[81] Y. Zhang, D. Zheng, R.H. Deng, Security and privacy in smart health: Efficient policy-hiding attribute-based access control, IEEE Internet Things J. 5 (3) (2018) 2130–2145.

[82] B. Alohali, M. Merabti, K. Kifayat, A Secure Scheme for a Smart House Based on Cloud of Things (CoT), in: 2014 6th Computer Science and Electronic Engineering Conference (CEEC), IEEE, 2014, pp. 115–120.

[83] C. Zhu, H. Nicanfar, V.C. Leung, L.T. Yang, An authenticated trust and reputation calculation and management system for cloud and Sensor Networks Integration, IEEE Trans. Inf. Forensics Secur. 10 (1) (2015) 118–131.

[84] T.D.P. Bai, S.A. Rabara, Design and development of integrated, secured and intelligent architecture for Internet of Things and Cloud Computing, in: 2015 3rd International Conference on Future Internet of Things and Cloud, IEEE, 2015, pp. 817–822.

[85] K. Lee, D. Kim, D. Ha, U. Rajput, H. Oh, On security and privacy issues of fog computing supported Internet of Things environment, in: 2015 6th International Conference on the Network of the Future (NOF), IEEE, 2015, pp. 1–3.

[86] M. Henze, L. Hermerschmidt, D. Kerpen, R. Häußling, B. Rumpe, K. Wehrle, A comprehensive approach to privacy in the cloud-based Internet of Things, Future Gen. Comput. Syst. 56 (2016) 701–718.

[87] S. Kumari, X. Li, F. Wu, A.K. Das, K.-K.R. Choo, J. Shen, Design of a provably secure biometrics-based multi-cloud-server authentication scheme, Future Gen. Comput. Syst. 68 (2017) 320–330.

[88] A. Alrawais, A. Alhothaily, C. Hu, X. Cheng, Fog computing for the internet of things: security and privacy issues, IEEE Internet Comput. 21 (2) (2017) 34–42.

[89] S. Sahmim, H. Gharsellaoui, Privacy and security in internet-based computing: cloud computing, internet of things, cloud of things: a review, Proc. Comput. Sci. 112 (2017) 1516–1522.

[90] L. Pacheco, E. Alchieri, P. Solis, Architecture for Privacy in Cloud of Things, ICEIS 2 (2017) 487–494.

[91] X. Wang, Z. Ning, M. Zhou, X. Hu, L. Wang, B. Hu, R.Y. Kwok, Y. Guo, A privacy-preserving message forwarding framework for opportunistic cloud of things, IEEE Internet of Things J. 5 (6) (2018) 5281–5295.

[92] C. Stergiou, K.E. Psannis, B.-G. Kim, B. Gupta, Secure integration of IoT and cloud computing, Future Gen. Comput. Syst. 78 (2018) 964–975.

[93] S. Sharma, M.A.R. Shuman, A. Goel, A. Aggarwal, B. Gupta, S. Glickfield, I.D. Guedalia, Context aware actions among heterogeneous internet of things (iot) devices, uS Patent App. 14/187,156, 2014.

[94] T. Shon, J. Cho, K. Han, H. Choi, Toward advanced mobile cloud computing for the internet of things: current issues and future direction, Mobile Netw. Appl. 19 (3) (2014) 404–413.

Corresponding author
Ado Adamou Abba Ari can be contacted at: adoadamou.abbaari@gmail.com