Chapter 11
Internet of Cloud: Security and Privacy Issues

Allan Cook, Michael Robinson, Mohamed Amine Ferrag, Leandros A. Maglaras, Ying He, Kevin Jones and Helge Janicke

Abstract The synergy between Cloud and IoT has emerged largely due to the Cloud having attributes which directly benefit IoT and enable its continued growth. IoT adopting Cloud services has brought new security challenges. In this book chapter, we pursue two main goals: (1) to analyse the different components of Cloud computing and IoT and (2) to present security and privacy problems that these systems face. We thoroughly investigate current security and privacy preservation solutions that exist in this area, with an eye on the Industrial Internet of Things, discuss open issues and propose future directions.

Keywords Internet of cloud · Cloud computing · Security · Authentication Intrusion detection · Privacy

11.1 An Introduction to Cloud Technologies

According to forecasts from Cisco Systems, by 2020 the Internet will consist of over 50 billion connected devices, including, sensors, actuators, GPS- and mobile-enabled devices, and further innovations in smart technologies, although this forecast is disputed [53]. New projections talk about 20–30 billion connected devices which is again a huge number [20]. These revolutionary devices are predicted to integrate to form hybrid networks based upon concepts such as the Internet of Things (IoT), Smart Grids, sensor networks etc., to deliver new ways of living and working. Underpinning such operating models will be 'cloud computing' technology that enables

A. Cook · L. A. Maglaras (✉) · Y. He · H. Janicke
De Montfort University, School of Computer Science and Informatics, Leicester, UK
e-mail: leandrosmag@gmail.com

M. Robinson · K. Jones
Airbus Group Innovations, Newport, Leicester, UK

M. A. Ferrag
Department of Computer Science, Guelma University, Guelma, Algeria

B. S. P. Mishra et al. (eds.), *Cloud Computing for Optimization: Foundations, Applications, and Challenges*, Studies in Big Data 39,
https://doi.org/10.1007/978-3-319-73676-1_11

convenient, on-demand, and scalable network access to a pool of configurable computing resources. This remote access to high levels of processing power and storage provides a complementary platform on which to augment the low-power, low-storage characteristics of IoT devices, providing an integrated environment to provide ubiquitous capabilities to end users.

Cloud computing further offers a range of attractive benefits to organisations wishing to optimise their IT resources, such as increases in efficiency and organisational ability, reduced time to market (TTM), and a better balance between capital expenditure (capex) versus operational expenditure (opex) [30]. However, to achieve such returns on investment, organisations require a clear understanding of cloud technologies to drive their strategy, and in particular, the issues surrounding security and privacy. This chapter introduces the reader to cloud computing technologies in general, then proceeds to explain the emerging Internet of Cloud (IoC) before discussing the security and authentication issues of IoT and finally exploring the issues related to the preservation of privacy in the IoC.

11.1.1 A Definition of Cloud Computing

Cloud computing is a technological and operational model for ubiquitous, on-demand network access to a shared pool of configurable infrastructure, processing, storage and application services that can be provisioned and released for use with minimal system management effort or service provider interaction [48]. Many of the technologies that underpin cloud computing environments are not new, as they comprise existing virtualisation, processing and storage capabilities that have existed for many years. It is the operating model that surrounds the use of these technologies that delivers the revolutionary services, where ownership of physical resources rests with one party, and the service users are billed for their use [12].

As such, it is necessary to consider the essential characteristics, service models and deployment models of cloud computing.

11.1.2 Characteristics of Cloud Computing

Cloud computing environments comprise five essential characteristics; On-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service [48]. We shall now review each of these in turn.

- **On-demand Self-service**: In cloud environments, a consumer can request and deploy processing and storage capabilities, such as server capacity and storage space, through the use of automated provisioning services that require no negotiation with the cloud provider [48]. This allows connected devices to remotely exploit such resources and extend their processing capabilities as necessary.

- **Broad Network Access**: The services of a cloud are made available over the network using thick or thin clients, allowing devices using different operating systems and platforms to access common capabilities [48].
- **Resource Pooling**: The computing resources of a cloud service are pooled into a model to serve multiple consumers, with different physical and virtual resources dynamically assigned and reassigned according to demand requirements, irrespective of their geography. The customer is typically unaware of the exact location of the provided resources, although they may be able to define high-level constraints such as country or data centre [48].
- **Rapid Elasticity**: Elasticity is the ability of a cloud provider to scale up or down dependent upon consumer demand, allocating or freeing resources as necessary. To the consumer, the capabilities provided often appear to be unlimited.
- **Measured Service**: In cloud models, consumers pay for the services they use, so it is necessary to monitor, control and report upon the consumption of the infrastructure. This allows usage to be optimised, and provides a transparent understanding to both the provider and consumer [48].

11.1.3 Cloud Service Models

There are various levels of service model available to consumers when they adopt cloud services, each with their own operating paradigm, offering software, platforms, or infrastructure as a service.

- **Software as a Service (SaaS)**: In this model, the consumer uses the provider's applications that run on the cloud infrastructure. The consumer accesses these applications without any knowledge of the underlying infrastructure, and does not request or provision any associated services. They provision and consume application resources, typically against an agreed service level agreement (SLA) that determine performance, and the cloud provider scales the infrastructure to meet its obligations [48].
- **Platform as a Service (PaaS)**: In a PaaS environment, consumers deploy their own (or their acquired) applications, services, libraries or tools, which they control. The cloud provider's role is to provision and maintain sufficient computing, network and storage resources to meet the agreed SLAs for the consumer-deployed elements [48].
- **Infrastructure as a Service(IaaS)**: This service model allows consumers to provision processing, network and storage resources as necessary, onto which they can deploy whichever applications and services the require. The consumer does not control the underlying hardware infrastructure, but can determine the technical detail of what is deployed, such as operating systems etc. [48].
- **Cloud Deployment Models**: The provision of SaaS, PaaS or IaaS is dependent upon the cloud provider's business model. Similarly, the scope of the cloud itself, whether private, community, public, or hybrid mix of these three, allows consumers

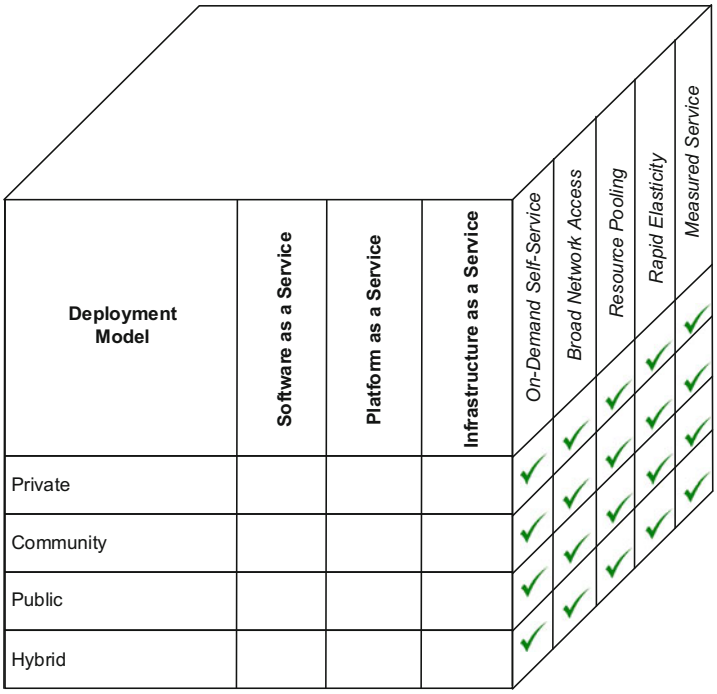

Fig. 11.1 Cloud deployment and service models mapped to essential characteristics

to constrain the exposure of their information. Irrespective of the combination of these choices however, the provider should offer the five essential characteristics of cloud services, as illustrated in Fig. 11.1.

- **Private Cloud**: The service infrastructure is provided for exclusive use by a single organisation. It may be owned, managed, and operated by the organisation, a third party, or some combination thereof, and may exist on or off the organisation's premises [48].
- **Community Cloud**: The cloud is made available for use by a specific community of consumers with shared requirements. The service may be owned, managed, and operated by one or more of the community organisations, a third party, or some combination, and be located either on or off the premises of the community [48].
- **Public Cloud**: The cloud infrastructure is provisioned for use by the general public. The infrastructure is deployed on the premises of the cloud provider [48].
- **Hybrid Cloud**: The cloud infrastructure is a mix of two or more cloud deployment models (private, community, or public) [48].

11.1.4 Enabling Technologies

As previously discussed, cloud services are based upon a common set of underpinning enabling technologies that were developed before cloud computing emerged as a business model. We shall now consider a key subset of these technologies in the context of their operation within a cloud.

- **Virtualisation**: Virtualisation is the ability to deploy multiple host operating environments on one physical device. Typically, operating systems are encapsulated within a 'virtual machine' (VM), a number of which are deployed onto a single physical server (a 'real machine'). A 'hypervisor' that abstracts the VMs from the real machine, accessing hardware components of the server as required by each VM. Hypervisors also allow VMs to be redeployed to other real machines, permitting them to be reallocated to servers with greater or lesser processing capacity as required by the consumers demands [16].
- **Storage**: Storage within cloud environment can be characterised as either file- or block-based services, or data management comprising record-, column- or object-based services. These typically reside on a storage area network (SAN) that provides a persistence platform that underpins a data centre. For file- or block-based services, the cloud ensures that sufficient capacity is provided to support the elasticity of the service, expanding or contracting as required. Record-, column- or object-based services, however, focus on database persistence and the performance of the data used by applications. As data expands within a large database it becomes necessary to optimise the storage based on frequency of access and location of consumers. Data within the cloud can be easily replicated to provide temporary copies in caches etc. that improve performance, as well as reducing the impact of backup services on production data. Similarly, where multiple data centres are used, these local caches can be optimised to focus on the datasets most frequently accessed in each location. The underlying file system elastically supports these replicas of data, expanding and contracting as necessary to support performance SLAs [27].
- **Monitoring and Provisioning**: The ability of a cloud provider to automatically provision services is an key element of its offering. Automated provisioning is typically based on a catalogue, from which consumers can select the extension or contraction of a service over which they have decided to maintain control. The nature of the service they maintain control of is dependent upon the service model they operate within (SaaS, PaaS, IaaS). Similarly, for the cloud provider, they require the ability to modify the execution environment in line with agreed SLAs, with or without human intervention. The provisioning is typically managed by a service orchestration layer that interacts with the monitoring service to determine the levels of performance of cloud elements in line with SLAs, and coordinates the manipulation of the infrastructure, deploying and redeploying resources as necessary to maintain a balanced and cost-efficient use of the available architecture [39].
- **Billing**: Given the differing service and deployment models that cloud providers can offer, the billing service must be integrated with the monitoring and

provisioning to ensure accurate accounting of consumption. The billing services, in some cases, support both prepay and postpay models, requiring the billing service to decrement or accrue respectively. The service must also only account for consumption as it occurs, and be cognisant of the elasticity of deployment and release. As the nature of the cloud service provided to consumers may differ, the billing service must support multiple, and in many cases, complex pricing models to ensure accurate accounting [19].

Cloud computing is based on a mix of technologies brought together in differing service and deployment models to provide cost-effective utilisation of IT resources. The ubiquity of access to these resources allows low-power, low-storage capacity IoT devices to extend their capabilities by leveraging these services on-demand. This integration of IoT and cloud into the Internet of Cloud (IoC) provides opportunities to provide a revolution in the use and exploitation of smart devices.

11.2 Internet of Things (IoT) and Internet of Cloud (IoC)

The Internet of Things is a term that has rapidly risen to the forefront of the IT world, promising exciting opportunities and the ability to leverage the power of the internet to enhance the world we live in. The concept itself is not a new one however, and it is arguable that Nikola Tesla predicted the rise of IoT back in 1926 when he stated:

> When wireless is perfectly applied the whole earth will be converted into a huge brain...and the instruments through which we shall be able to do this will be amazingly simple compared with our present telephone [36].

What Tesla had predicted was the Internet of Things (IoT), which today has been defined as the pervasive presence in the environment of a variety of things, which through wireless and wired connections and unique addressing schemes are able to interact with each other and cooperate with other things to create new applications/services and reach common goals [76]. Put more simply, things are anything and everything around us that are internet connected and are able to send, receive or communicate information either to humans or to other things. There are three primary methods in which things communicate. Firstly, a sensor can communicate machine to machine (M2M). Examples here include a sensor feeding data to an actuator which opens a door when movement is detected. Secondly, communication can be Human to Machine (H2M), such as a sensor which can detect human voice commands. Finally, machine to human (M2H) communication provides the delivery of useful information in an understandable form such as a display or audio announcement. When considering the number of things in our world, and the number of potential combinations of connecting them, the only limit for thinking up valuable use cases is our own imagination. Some well established use cases for the IoT are as follows:

- **Healthcare**: The use of sensors and the internet to monitor the medical variables of human beings and perform analyses on them. A real world example is NHS England's Diabetes Digital Coach Test Bed [51], which trialled the use of mobile health self-management tools (wearable sensors and supporting software). This trial leveraged the IoT to realise a number of benefits. Firstly it enabled people with diabetes to self-manage their condition through the provision of real time data and alerts based upon the data from their sensors. Secondly, the sensors were able to notify healthcare professionals if there was a dangerous condition that was not being corrected by the patient. Thirdly, the data from the sensors could be aggregated to provide a population-wide view of the health status of people with diabetes.
- **Smart Cities**: The use of connected sensors to improve city life and create an urban information system [34]. For example, detecting the amount of waste in containers to schedule a pick-up or the use of sensors to detect city-wide availability of parking and direct drivers to an available space [59]. This has the potential to not only save citizens frustration, but also to reduce congestion, pollution and fuel consumption.
- **Smart Buildings**: Both places of business and people's homes can benefit from the rise of the IoT. Buildings consume 33% of world energy [76], and there is real potential for the IoT to bring this usage down. Sensors can turn off lights when they are not needed, and appliances remotely switched off. Heating can be optimised based upon sensors detecting occupancy and weather conditions. Aggregations of this data can be used by energy providers to plan and optimise their operations.
- **Smart Transport**: The connecting of multiple transport related things. For example, sensors in roadways and vehicles to provide a full view of traffic flow and dynamically alter traffic light sequences, speed limits, information signs or satellite navigation systems to suggest quicker routes.
- **Smart Industry**: Intelligent tracking of goods and components, smart factories and innovative retail concepts such as Amazon Go [2], which offer a checkout-less experience for customers.

A summary of IoT projects around the world ranked by application domain is provided in Fig. 11.2. As the graphic shows, the most active domains for IoT (as of Q3 2016) are connected industry and smart cities. However, all of the domains are showing an upward trend that is likely to continue into the future as new and innovative use cases are developed and the value of IoT becomes increasingly apparent to actors in each domain [6].

11.2.1 IoT Technologies

Behind the things which make up the IoT are a number of essential core technologies. The literature identifies five overall technologies as follows: [41]:

- **Radio Frequency Identification (RFID)**: Passive RFID chips have no battery, and provide information to a reader when it is placed in proximity of the chip. Active

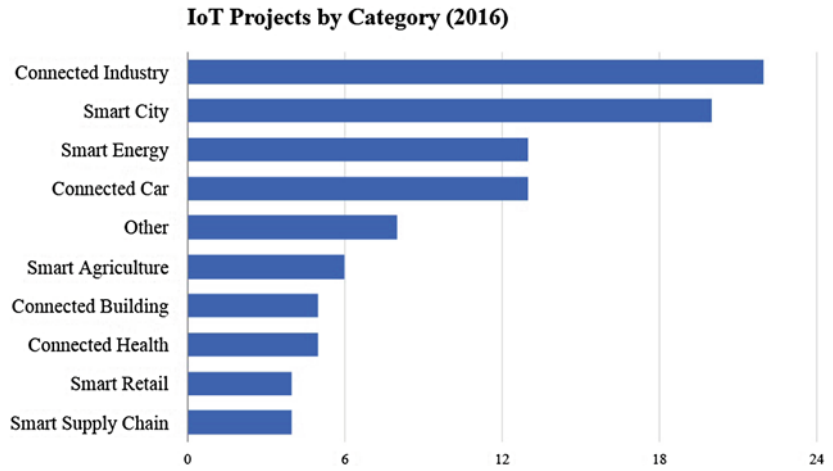

Fig. 11.2 IoT projects by category

RFID chips can initiate communication, and output information in response to a change in its environment (e.g. changes in temperature or pressure).

- **Wireless Sensor Networks (WSN)**: Wireless sensor networks are defined as collections of stand-alone devices which, typically, have one or more sensors (e.g. temperature, light level), some limited processing capability and a wireless interface allowing communication with a base station [29].
- **Middleware**: Middleware sits between the things and the raw data they generate to provide interoperability between things and developers who code the applications for interesting use cases. It provides a level of abstraction, allowing developers to work with sensors without having to know the specifics of their implementation.
- **Cloud Computing**: The cloud provides the seemingly limitless storage and processing power necessary for IoT use cases to become a reality.
- **IoT Applications**: The software that provides end users with a useful product - e.g. A smartphone app through which a driver can find and reserve a free parking space.

The focus of this section is on the cloud aspect of IoT technology, in particular how cloud computing and the IoT have found what appears to be a mutually beneficial relationship and led to the term Internet of Cloud (IoC).

11.2.2 Internet of Cloud (IoC)

The synergy between the cloud and the IoT has emerged largely due to the cloud having attributes which directly benefit the IoT and enable its continued growth. In the IoT's infancy, things either had some local computing resources (storage,

processing) to produce a useful result, or they sent their data to a mainframe which had the necessary computing resources to process the data and generate an output. In effect, the "brain" as Tesla envisioned in 1926 was either highly distributed amongst the things, or it was centrally located with the things simply acting as sensors. Both of these approaches have disadvantages. The mainframe's weaknesses are that it is expensive to maintain and presents a central point of failure. The highly distributed approach whereby things communicate and perform some local computation provides better resilience to failure, but increases the cost of each thing in the network. This additional cost is both financial (the cost of equipping each thing with suitable resources and replacing failed things) and logistical (including such resources required the thing to be physically larger and consume more power). As use cases become more advanced, and the goals more complex, the demand for more complex computation has only increased.

The IoT is not only expanding in its need for more demanding computation resources. Gartner has predicted that the number of internet connected devices will reach 20.8 billion by 2020 [26], suggesting that the IoT is not only expanding in computational complexity, but also in the sheer amount of data that needs to be processed. In effect, the IoT generates big data [58], which places the demand for smaller and cheaper things directly into competition with the demand for more computing resources. Traditional approaches to the IoT cannot satisfy both demands - either the things become more expensive and complex, or limits on their computation resource needs are imposed. However, the cloud presents a solution with the potential to satisfy both demands.

11.2.3 Cloud as a Solution

The rise of cloud computing has provided an alternative solution, presenting the IoT with a virtually limitless source of computing power, easily accessible via the internet, with better resilience and at a lower cost than utilising a mainframe or including computing resources at the thing level. The cloud allows IoT developers to be freed from the constraints of limited resources, and enables the use case to be realised at reduced cost. In effect, things only require the bare minimum of hardware to perform their function (e.g. sense something, actuate something) and to communicate with the cloud. The cloud performs all computation and communicates back the result to the things. This pairing of cloud computing and the IoT has led to the term Internet of Cloud (IoC), and numerous literature reviews of this new paradigm are available [9, 17].

11.2.4 Sensor-Clouds

Cloud infrastructure is not only valuable for taking on the burden of heavy computation and storage, it has also been identified as valuable in forming what are known as Sensor-Clouds [1]. In traditional sensor networks, the deployed sensors provide data for one purpose - to fulfil the purchaser's use case. Unfortunately, this leads to an element of wastage, since the data being collected could be useful for other purposes but is not readily accessible by other organisations or third party developers. For example, if a local council deployed sensors to measure traffic flow in the city centre, a third party may wish to access the sensor data to improve their satellite navigation system and direct travellers away from congested roads. Sensor-Clouds address this scenario by making the sensor data available to multiple parties in the cloud. In effect, they offer what could be termed sensors as a service. This scenario brings a number of benefits. Firstly it allows developers of IoT applications to avoid the burden of manually deploying sensors and focus upon developing interesting use cases through the use of existing sensor networks. Secondly, sensor owners such the local council can recoup some of the cost of deployment and maintenance by charging these third parties to access the data.

A Sensor-Cloud can be visualised in three layers [1]. At the lowest layer, physical sensors around the world upload their data in a standardised format to the Sensor-Cloud. This standardisation of data allows users of the service to use the data without concern over differences in areas such as protocols and formatting. At the second layer, the Sensor-Cloud allows users to create virtualised groups of sensors for use in their applications. These virtual sensors are based upon service templates, which are defined by the sensor owners. At the top layer, application developers can plug these virtual sensors into their applications. This three layer architecture for Sensor-Clouds is shown in Fig. 11.3.

11.2.5 Ongoing Challenges

It has been noted that the cloud brings some valuable attributes to the IoT, but it is not a perfect solution which can solve all of the IoT's problems. In fact, the use of the cloud can present some new and interesting challenges as follows [17]:

- **Security and Privacy**: Cloud security is a well documented challenge, but the pairing between cloud and the IoT presents additional concerns. For example, when considering the sensitive nature of some use cases such as smart health, additional care must be taken to ensure that confidentially, integrity and availability of data is not violated. Confidentiality breaches could result in personal health data being stolen, integrity breaches could be fatal if data is tampered with and a lack of availability could fail to alert to a life threatening condition.
- **Addressing**: If Gartner's predictions on the rapid growth of the IoT are correct, IPv4 will quickly become inadequate to address all of the things. IPv6 has the

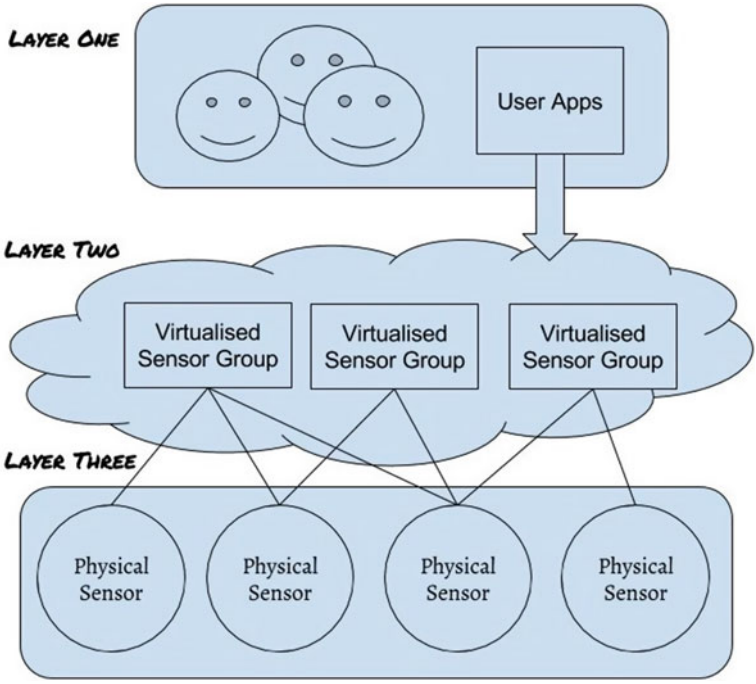

Fig. 11.3 Sensor-cloud layers

potential to address this concern, but it is not yet widely adopted. It has been proposed that an efficient naming and identity management system is required to dynamically assign and manage unique identity for an ever increasing number of things [37].

- **Latency and Bandwidth**: The cloud may provide limitless computing resources, but it cannot necessarily ensure low latency or unlimited bandwidth since this relies upon the public internet which is outside of the cloud provider's control. This challenge has led to the rise of what is termed "fog computing", where computing resources are placed as close to the things as possible in order to act as an intermediary. This intermediary can quickly service time critical processing that is latency sensitive whilst forwarding on non-time critical data for cloud processing [8].
- **Interoperability**: Due to the high number of things from multiple vendors, cloud computing alone cannot solve the issue of interoperability. The IoT would benefit from standards which describe a common format for both handling and communicating data.

11.2.6 Japan Case Study

While the concept of Internet of Cloud and Sensor-Clouds can seem abstract, it has been implemented in some very valuable use cases. One such use case was in the aftermath of the 2011 tsunami in Japan, which led to the second-largest nuclear emergency since Chernobyl. With a lack of reliable government information on the radiation threat, private individuals and organisations donated hundreds of Geiger counters to the affected region. As standalone devices, the use of these counters was limited, and researchers began to investigate methods to link the devices together and make the information available to all. The cloud provided the necessary infrastructure and agility to quickly connect each sensor, and a Sensor-Cloud of around 1000 radiation sensors was formed. This Sensor-Cloud provided emergency services with essential information regarding radiation levels, and the same data was leveraged to produce a smart phone app for local citizens to monitor radiation levels in their area [74]. The project, today known as Safecast [62], has grown beyond the initial use case and is now a global network of radiation sensors, allowing the public to access, contribute and use the sensor data through an API.

This use case highlights how valuable the Internet of Cloud can be not only for its ability to provide the necessary computing resources but also for the speed at which such resources can be provisioned - in this case rapidly providing the back end for a potentially life saving service. As stated in the previous subsection the pairing between cloud and the IoT presents additional concerns in terms of security and privacy. However, for these services to be adopted they must be trusted. Therefore, we must now consider the security and privacy implications of such integration.

11.3 Security and Authentication Issues

IoT ecosystem creates a world of interconnected thing, covering a variety of application and systems, such as smart city systems, smart home systems, vehicular networks, industrial control systems as well as the interactions among them [28]. Cloud computing is a technology that is configured to enable access to a shared pool of resource including servers, data storage, services and application [3]. It has become an important component of the IoT as it provides various capabilities to manage systems, servers and application and performs necessary data analytics and aggregation.

It is undeniable that IoT provides benefits and convenience to our everyday life, however, many of the IoT components (e.g. low cost digital devices and industrial systems) are developed with little to no consideration of security [35, 38, 63]. A successful exploit can propagate within the IoT ecosystem that could render the loss of sensitive information, interruption of the business functionalities, and the damage to critical infrastructure.

We have already seen the security concerns of the cloud services. These include but are not limited to malware injection (malicious code injected into cloud and run

as SaaS), vulnerable application programming interfaces (API), abuse of data and cloud service, insider threats and the newly emerging Man In Cloud Attack [32]. Cloud involves both service providers and consumers; therefore, cloud security is a shared responsibility between the two.

Security issues are still yet to be solved for IoT and Cloud respectively. IoT adopting Cloud services could complicate this situation and raise more security concerns. This section focuses on the security issues on IoT adopting Cloud services and makes recommendations to address those issues.

11.3.1 Data Sharing/Management Issues of IoT Cloud

Within a cloud context, no matter public, private or hybrid, data security management involves secure data storage, secure data transmission and secure access to the data. During transmission, the Transport Layer Security (TLS) cryptography is widely used to prevent against threats. During processing, the cloud service provided applies isolation between different consumers. The isolation [80] is applied at different levels such as operations system, virtual machine or hardware. The secure access to data sometimes depends on the isolation level. It may sometimes separate completely from other resources or may have shared infrastructures and softwares that rely on access control policies. Within an IoT context, one of the benefits is open data sharing among different things. If the data is isolated as is currently offered in the cloud services, open wide data aggregation and analytics would become impossible. A balance needs to be found between data protection and sharing.

There is existing work such as Information Flow Control (IFC) [4, 54] defining and managing the requirements for data isolation and sharing. People can specify to what extent they want to share or protect their data. Other work is related to data encryption, encrypting the things before uploading to the cloud. This would limit the users access to the data, which again affects the IoT's data sharing and analytical capability. There are some solutions to analyse encrypted data. However, this approach is not mature to be applied in practice at this stage [31, 50].

11.3.2 Access Control and Identity Management

Within a cloud context, access control rules are strictly enforced. The service providers use authentication and authorisation services to grant privileges to the consumers to access storage or files. Within an IoT context, there are interactions between different devices that are owned by different people. Access control is usually leveraged through device identity management and configuration [46]. Existing identity management includes identity encoding and encryption [77].

When IoT uses Cloud services, access control involves the interactions among the applications and cloud resources. Policies and mechanism need to be flexibly

defined to accommodate the needs of both and resolve the conflicts of different parties. There is existing work on grouping the IoT devices to enable common policies [64]. However, cares need to be taken to ensure the flexibly defined policies do not introduce vulnerabilities to the system.

11.3.3 Complexity (Scale of the IoT)

One of the benefits of Cloud service adoption is the reduction of cost through elastically resource scaling mechanisms. The increase of IoT devices, data volume, and variety has become a burden for the Cloud. The failure to coordinate and scale the "things" will impact the availability of the data. Security mechanism will bring extra burden that can impact the performance of IoT Cloud [60, 80].

Logging is an important aspect of security as it provides a view of the current state of the system. Logging within the Cloud is centralised and it is an aggregation of the logs from different components such as software applications and operation [68]. IoT logging tends to decentralise it among different components. There are some existing work on logging centralisation (e.g. design analytics tools to collect and correlate decentralised logs from "things" [57]) and decentralisation (e.g. enable logging to capture information in a data-centric manner [56]). A balance needs to be found between logging centralisation and decentralisation.

11.3.4 Protection of Different Parties

IoT Cloud raise security concerns to both service providers and consumers. Cloud service providers used to apply access control to protect data and resources. Now, the "things" can directly interact with the providers. Attacks can be easily launched by compromised "things". We have already seen some real world exploits of smart home applications, that are designed with poor security considerations [61].

From the consumers' perspective, "things" needs to be validated before it can be connected. If the "things" are determined to be compromised or malicious, alerts will be sent either in a human readable or machine-readable format. The determination can be based on reputation, trustworthy network node evaluation [52, 85] and so on.

11.3.5 Compliance and Legal Issues

Cloud demonstrated compliance using contract through service-level agreement (SLA). A typical method to assess compliance is through auditing. Within the area of Cloud, Massonet has proposed a framework that can generate auditing logs

demonstrating that they are compliant with the related policies/regulations [47]. There are also frameworks designed in the area of IoT to demonstrate compliance using auditing logs.

IoT tends to be decentralised in isolated physical locations. The centralisation of cloud allows the data to flow across geographic boundaries, which has raised legal and law concerns of the data across national borders. There are some existing work on constrain data flow geographically by applying legal and management principles to the data [66]. Again this will have an negative impact on data sharing capability of IoT and Cloud.

11.3.6 Cloud Decentralisation

An emerging trend is the Cloud decentralisation in order to accommodate the IoT and big data analytics. Typical method is decentralised computing such as Fog computing [8] and grid computing [25]. Cloud decentralisation helps reduce the typical Cloud attacks such as denial of service (DoS) attack; it also raises new security concerns. Instead of targeting on the Cloud services, the attacks are directed to individual service providers and consumers. There is on-going research in securing the decentralised Cloud through coordinating the communication of things to things, things to clouds and clouds to clouds [67, 68]. Finally cloud decentralization can provide more flexible management.

Following the trend of decentralized cloud deployment, security mechanisms that must be developed for the IoC may also be decentralized. This deployment can have multiple advantages and in this context Intrusion Detection Systems for the IoC are analyzed on Sect. 11.3.7.

11.3.7 Intrusion Detection Systems

Intrusion detection systems (IDS) can be classified into centralized intrusion detection systems (CIDS) and distributed intrusion detection systems (DIDS) by the way in which their components are distributed. In a CIDS the analysis of the data is performed in some fixed locations without considering the number of hosts being monitored [40], while a DIDS is composed of several IDS over large networks whose data analysis is performed in a number of locations proportional to the number of hosts. There are numerous advantages of a DIDS compared to a CIDS. A DIDS is highly scalable and can provide gradual degradation of service, easy extensibility and scalability [14].

Novel intrusion detection Systems (IDS) must be implemented that need to be efficient both in terms of accuracy, complexity and communication overhead, false alarm rate and time among others. IDSs that have been developed for other systems, e.g. Industrial Control Systems [15, 45], wireless sensor networks [11], or cloud

environments [49] can be used as a basis for developing new detection systems for the IoC area. Adaptivity of the IDS on changes in the network topology, which will be a frequent situation for an IoC, is an aspect that needs to be addressed when new IDS are going to be designed [70].

11.4 Privacy Preserving Schemes for IoC

In this subsection, we review the privacy preserving schemes for IoC. Based on the classification of authentication and privacy preserving schemes in our three recent surveys [22–24], the privacy preserving schemes for IoC can be classified according to networks models and privacy models. The summary of privacy preserving schemes for IoC are published in 2014, 2015, and 2016, as presented in Tables 11.1, 11.2, and 11.3, respectively. In addition, Fig. 11.4 shows the classification of privacy preservation models for IoC.

Cao et al. [13] defined and solved the problem of multi-keyword ranked search over encrypted cloud data while preserving strict systemwise privacy in the cloud-computing paradigm. Specifically, the authors proposed a preserving scheme, called MRSE, using the secure inner product computation. The MRSE scheme is efficient in terms of the time cost of building index and the time cost of query. Worku et al. [81] proposed a privacy-preserving public auditing protocol in order to provide the integrity assurance efficiently with strong evidence that unfaithful server cannot pass the verification process unless it indeed keeps the correct data intact. Wang et al. [78] proposed a brand new idea for achieving multi-keyword (conjunctive keywords) fuzzy search. Different from existing multi-keyword search schemes, the scheme [78] eliminates the requirement of a predefined keyword dictionary. Based on locality-sensitive hashing and Bloom filters, the scheme [78] is efficient in term of the Bloom filter generation time for a single file. Wang et al. [10] a privacy-preserving public auditing mechanism, called Oruta, to verify the integrity of shared data without retrieving the entire data. Oruta uses ring signatures [7] to construct homomorphic authenticators. In addition, Oruta can achieving following properties: (1) Public Auditing, (2) Correctness, (3) Unforgeability, and (4) Identity Privacy. Yuan and Yu [33] proposed the first secure and practical multi-party the back-propagation neural network learning scheme over arbitrarily partitioned data. Based on two phases, namely, (1) privacy preserving multi-party neural network learning, and (2) secure scalar product and addition with Cloud, the scheme [33] can support the multi-party scenario and efficient in terms of collaborative learning and communication cost compared to both schemes in [73] and [5]. Sun et al. [72] proposed an idea to build the search index based on the vector space model and adopt the cosine similarity measure in the Cloud supporting similarity-based ranking. Based on the vector space model, the scheme [72] is efficient in term of time cost for generating encrypted query. Dong et al. [18] considered four parties in a network, namely, the data owner, the data consumer, the cloud server, and the private key generator. Then,

Table 11.1 Summary of privacy preserving schemes for IoC (Published in 2014)

Scheme	System model	Privacy model	Goals	Main phases	Performances (+) and limitations (-)
Cao et al. [13]	A cloud data hosting service involving three different entities, namely, the data owner, the data user, and the cloud server	Data privacy Index privacy Keyword privacy	Achieving the multi-keyword ranked search with privacy-preserving	- Setup - BuildIndex - Trapdoor - Query	+ Efficient in term of the time cost of building index + Efficient in term of the time cost of query + Resistance to the known ciphertext model and known background model - No consideration for checking the integrity of the rank order
Worku et al. [81]	Three different entities, including, cloud server, user, and third party auditor	- User privacy	Achieving public verifiability, storage correctness, batch auditing, blockless verification, and privacy preserving	KeyGen SigGen ProofGen VerifyProof	+ Efficient in term auditor and server computation overhead compared to the scheme in [79] + Secure in the random oracle model - No threat model presented
Wang et al. [78]	Three different entities, including, data owner, cloud server, and user	- File content privacy - Index privacy - User query privacy	Support multi-keyword fuzzy search	- KeyGen - Index Enc - Query Enc - BuildIndex - Trapdoor - Search	+ Efficient in term of the Bloom filter generation time for a single file + Multi-keyword fuzzy search + Resistance to the known ciphertext model and known background model - No comparison with related schemes

(continued)

Table 11.1 (continued)

Scheme	System model	Privacy model	Goals	Main phases	Performances (+) and limitations (-)
Wang et al. [10]	Three parties: the cloud server, a group of users and a public verifier	- Identity privacy	Achieving following properties: (1) Public Auditing, (2) Correctness, (3) Unforgeability, and (4) Identity Privacy.	- KeyGen - RingSign - RingVerify	+ Efficient in terms of signature generation and communication cost + Efficient in term of auditing time + Efficient in terms of privacy and batch auditing with incorrect proofs - Traceability is not considered
Yuan and Yu [33]	Three major parties: a trusted authority (TA), the participating parties (data owner) and the cloud servers (or cloud)	- Multi-party privacy-preserving	Protecting each participant's private dataset and intermediate results generated during the back-propagation neural network learning process	- Privacy Preserving Multi-Party Neural Network Learning - Secure Scalar Product and Addition with Cloud	+ Efficient in terms of collaborative learning and communication cost compared to both schemes in [73] and [5] + Support the multi-party scenario + Scalable, efficient and secure - Does not allow multiparty collaborative learning without the help of TA

(continued)

Table 11.1 (continued)

Scheme	System model	Privacy model	Goals	Main phases	Performances (+) and limitations (-)
Sun et al. [72]	Three entities: the data owner, the data user, and the cloud server	- Search privacy - Index confidentiality - Query confidentiality - Query unlinkability - Keyword privacy	Achieving high efficiency and functionality (such as expressive/usable queries)	- Setup - GenIndex - GenQuery - SimEvaluation	+ Efficient in term of time cost for generating encrypted query + Help users ensure the authenticity of the returned search results in the multi-keyword ranked encrypted text search scenario - Traceability is not considered
Dong et al. [18]	Four parties in a network: the data owner, the data consumer, the cloud server, and the private key generator	- Backward secrecy - User privacy	Achieving fine-grained access control	- System initialization - Encryption - Key generation and distribution - Decryption	+ Efficient in terms of computation complexity, communication cost, and cost of revocation operation + Fully collusion secure + User access privilege confidentiality - Adversary's model is limited

Table 11.2 Summary of privacy preserving schemes for IoC (Published in 2015)

Scheme	System model	Privacy model	Goals	Main phases	Performances (+) and limitations (-)
Zhou et al. [87]	Cloud-assisted wireless body area networks	- Identity privacy - Location privacy	Detecting two attacks, namely, time-based mobile attack and location-based mobile attack	- Pairwise key establishment - Group key agreement	+ Efficient in terms of storage, computation, and communication overhead compared to the scheme in [75] - Traceability is not considered - No consideration for the patients' selfishness
Zhou et al. [88]	Three components: body area networks (BANs), wireless transmission networks and the healthcare providers equipped with their own cloud servers	- Identity privacy - Data confidentiality	Achieving data confidentiality and identity privacy with high efficiency	- Setup - Key Extract - Sign - Verify	+ Efficient in terms of computational overhead, communication overhead, and storage overhead compared to the scheme in [42] - Location privacy is not considered
Liu et al. [43]	Three main network entities: users, a cloud server, and a trusted third party	- Data anonymity - User privacy - Forward security	Achieving authentication and authorization without compromising a user's private information	- Ideal data accessing functionality - Ideal authority sharing functionality	+ Considers the data anonymity - Need an evolution in terms of computational overhead, communication overhead, and storage overhead - Traceability is not considered - No comparison with related schemes

Table 11.3 Summary of privacy preserving schemes for IoC (Published in 2016)

Scheme	System model	Privacy model	Goals	Main phases	Performances (+) and limitations (-)
Xia et al. [83]	Four different types of entities: the image owner, image user, cloud server and watermark certification authority	- Data privacy	Protecting the privacy of image data in content-based image retrieval outsourcing applications against a curious cloud server and the dishonest query users	- KeyGen - IndexGen - ImgEnc	+ Privacy of image content + Privacy of image features + Privacy of trapdoors + Leakage of similarity information + Efficient in term of time consumption of the trapdoor generation - The proposed watermarking method cannot be regarded as a very robust one
Xia et al. [84]	Three different types of entities: the image owner, image user and cloud server	- Image privacy	The plaintext data needs to be kept unknown to the cloud server	- The generation of unencrypted index - The index encryption	+ The privacy of the image + The privacy of the image features + The privacy of the trapdoors + The leakage of the similarity information + Efficient in four terms, namely, (1) time consumption of the index construction, (2) time consumption of the trapdoor generation, (3) time consumption of the search operation, and (4) storage consumption of the index - The feature extraction in encrypted image

(continued)

Table 11.3 (continued)

Scheme	System model	Privacy model	Goals	Main phases	Performances (+) and limitations (-)
Pasupuleti et al. [55]	Consisting of three main entities, including, data owner, cloud service provider, and authorized users	- Index Privacy - Data privacy	Proposing an efficient and secure privacy-preserving approach with following goals: privacy preserving, index privacy, and data integrity	- Key generation - Index creation - Privacy-preserving - Trapdoor generation - Ranked keyword search - Data decryption	+ Detect the modifications or deletions of data and maintain the consistency of data + Efficient in terms of computation cost and communication cost - Dynamic data updates
Xia et al. [82]	Consisting of three main entities, including, data owner, data user and cloud server	- Index confidentiality - Query confidentiality - Trapdoor unlinkability - Keyword privacy	Supporting multi-keyword ranked search and dynamic operation on the document collection	- Index Construction - Search Process	+ The search precision on different privacy level + The efficiency of index construction, trapdoor generation, search, and update - The users keep the same secure key for trapdoor generation - Location privacy and identity privacy are not considered

(continued)

Table 11.3 (continued)

Scheme	System model	Privacy model	Goals	Main phases	Performances (+) and limitations (-)
Song et al. [69]	Consisting of three main entities, including, data owner, authorized data user, and cloud server	- Data privacy - Query privacy	Providing the full-text retrieval services with privacy-preserving	- Document processing - Index structure and maintenance mechanism - Full-text retrieval algorithm over encrypted data	+ The index space cost + Time cost for inserting a new document + Query efficiency with different number of documents + Query precision with different number of documents - Traceability is not considered
Zhu et al. [89]	Four parts: trusted authority, location based services (LBS) provider, LBS user, and cloud server	- Location privacy	Providing privacy-preserving LBS data and user's location information with accurate LBS for users.	- System initialization - Cloud server data creation - Privacy-preserving location based services	+ The user query location is privacy-preserving in the proposed EPQ scheme + The proposed EPQ scheme can achieve confidential LBS data + The authentication of the LBS query request and response are achieved in the proposed EPQ scheme + Efficient in term of computation complexity compared with the FINE scheme [65] - Traceability is not considered

(continued)

Table 11.3 (continued)

Scheme	System model	Privacy model	Goals	Main phases	Performances (+) and limitations (-)
Lyu et al. [44]	Four parts: social network, data owner, members, and cloud storage server	- Data privacy	Providing the fine-grained access control	- System initiation - Privacy-preserving data construction - Interested data acquisition - Dynamic attribute management	+ Data confidentiality + Fine-grained access control + Collusion attacks resistant + Efficient in terms of communication overhead and computation cost compared to the scheme in [71] - Location privacy and identity privacy are not considered
Yu et al. [86]	Four parts, key distribution center, cloud user, cloud server and third party auditor	- Data privacy	Formalize the security model of zero knowledge privacy against the third party auditor	- Setup - Extract - TagGen	+ Perfect data privacy preserving + Efficient in terms of costs regarding computation, communication and storage - No comparison with related schemes

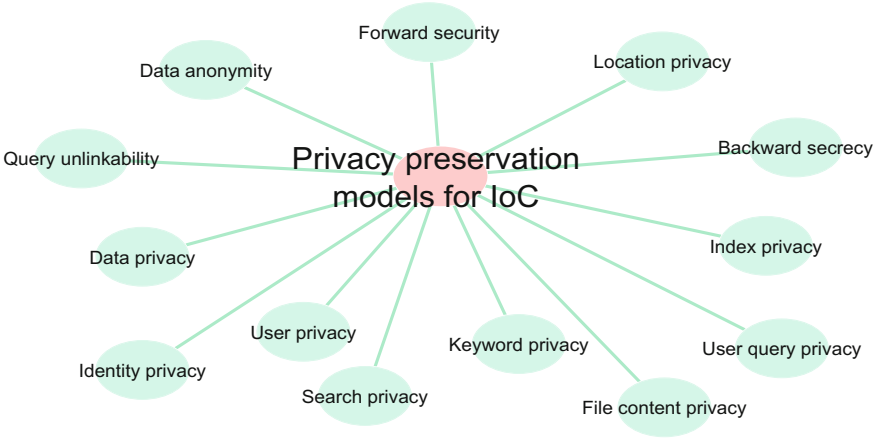

Fig. 11.4 Classification of privacy preservation models for IoC

the authors [18] proposed an idea that the cloud can learn nothing about a user's privacy or access structure, as such the scheme is fully collusion resistant.

To resilient to both time-based and location-based mobile attacks, Zhou et al. [87] proposed a secure and privacy-preserving key management scheme for cloud-assisted wireless body area networks. Based on the body's symmetric structure with the underlying Blom's symmetric key establishment mechanism, the scheme [87] is efficient in terms of storage, computation, and communication overhead compared to the scheme in [75], but the traceability is not considered. Zhou et al. [88] proposed a patient self-controllable and multilevel privacy-preserving cooperative authentication scheme, called PSMPA, to realize three levels of security and privacy requirement in distributed m-healthcare cloud computing system which mainly consists of the following five algorithms: Setup, Key Extraction, Sign, Verify and Transcript Simulation Generation. Based on an attribute based designated verifier signature scheme, PSMPA is efficient in terms of computational overhead, communication overhead, and storage overhead compared to the scheme in [42], but the location privacy is not considered. Therefore, Liu et al. [43] proposed a shared authority based privacy-preserving authentication protocol, named, SAPA, for the cloud data storage, which realizes authentication and authorization without compromising a user's private information. SAPA protocol [43] applied ciphertext-policy attribute based access control to realize that a user can reliably access its own data fields. In addition, SAPA protocol [43] adopt the proxy re-encryption to provide temp authorized data sharing among multiple users.

Xia et al. [83] proposed an idea to protect the privacy of image data in content-based Image retrieval outsourcing applications against a curious cloud server and the dishonest query users. Specifically, the idea is the first work that proposes a searchable encryption scheme, considering the dishonest query users who may distribute the retrieved images to those who are unauthorized. Similarly to the scheme [83],

Xia et al. [84] proposed an idea which the secure k-nearest neighbor algorithm is employed to protect the feature vectors in order to enable the cloud server to rank the search results very efficiently without the additional communication burdens. Based on the pre-filter tables, the scheme [84] is efficient in four terms, namely, (1) time consumption of the index construction, (2) time consumption of the trapdoor generation, (3) time consumption of the search operation, and (4) storage consumption of the index. Pasupuleti et al. [55] proposed an efficient and secure privacy-preserving approach using the probabilistic public key encryption technique to reduce computational overhead on owners while encryption and decryption process without leaking any information about the plaintext. Based on the idea of integrity verification, the scheme [55] can detect the modifications or deletions of data and maintain the consistency of data, also is efficient in terms of computation cost and communication cost. Therefore, Xia et al. [82] proposed two secure search schemes, namely, (1) the basic dynamic multi-keyword ranked search scheme in the known ciphertext model, and (2) the enhanced dynamic multi-keyword ranked search scheme in the known background model. Based on the searchable encryption scheme, the idea in [82] can supports both the accurate multi-keyword ranked search and flexible dynamic operation on document collection. Song et al. [69] defined and solved the problem of full-text retrieval over encrypted cloud data in the cloud computing paradigm. Based on a hierarchical Bloom filter tree index, the scheme [69] can protect user query privacy. Zhu et al. [89] proposed a privacy-preserving location based services query scheme in outsourced cloud, called EPQ, for smart phone. EPQ scheme can achieve confidential location-based services (LBS) data and is efficient in term of computation complexity compared with the FINE scheme [65].

Lyu et al. [44] design an efficient and secure data sharing scheme, named DASS. Based on multi-attribute granularity for social applications, DASS can support searchable encryption over data, and is efficient in terms of communication overhead and computation cost compared to the scheme in [71], but location privacy and identity privacy are not considered. Yu et al. [86] investigated a new primitive called identity-based remote data integrity checking for secure cloud storage. In addition, the scheme [86] showed that it achieves soundness and perfect data privacy. In a recent work, Ferrag and Ahmim in [21] proposed an efficient secure routing scheme based on searchable encryption with vehicle proxy re-encryption, called ESSPR, for achieving privacy preservation of message in vehicular peer-to-peer social network.

11.5 Summary

The synergy between the cloud and the IoT has emerged largely due to the cloud having attributes which directly benefit the IoT and enable its continued growth. IoT adopting Cloud services has brought new security challenges. We have identified key security issues in data management, access control and identity management, complexity and scale, the protections of different parties, compliance and legal issues, as well as the emerging Cloud decentralisation trend. There is existing work addressing

these issues, however future work should primarily focus on the balance between centralisation and decentralisation, data security and sharing as well as associated policy issues.

Regarding privacy preservation, it is not a problem that can be treated in isolation for a system, but interdependencies among different users and platforms must be also analyzed. Also the combination of privacy metrics can help improve the level of privacy by combining the positive aspects of different methods while keeping the total cost, in terms of storage, computation and delay, relatively low.

References

1. A. Alamri, W.S. Ansari, M.M. Hassan, M.S. Hossain, A. Alelaiwi, M.A. Hossain, A survey on sensor-cloud: architecture, applications, and approaches. Int. J. Distrib. Sens. Netw. **9**(2), 917923 (2013). https://doi.org/10.1155/2013/917923
2. Amazon: Amazon go. Online (2017), https://www.amazon.com/b?node=16008589011
3. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica et al., A view of cloud computing. Commun. ACM **53**(4), 50–58 (2010)
4. J. Bacon, D. Eyers, T.F.M. Pasquier, J. Singh, I. Papagiannis, P. Pietzuch, Information flow control for secure cloud computing. IEEE Trans. Netw. Serv. Manag. **11**(1), 76–89 (2014)
5. A. Bansal, T. Chen, S. Zhong, Privacy preserving Back-propagation neural network learning over arbitrarily partitioned data. Neural Comput. Appl. **20**(1), 143–150 (2011)
6. J. Bartje, The top 10 iot application areas - based on real iot projects (2016), https://iot-analytics.com/top-10-iot-project-application-areas-q3-2016/
7. D. Boneh, C. Gentry, B. Lynn, H. Shacham, Aggregate and Verifiably Encrypted Signatures from Bilinear Maps, *Intenational Conference on the Theory Applications of Cryptographic Technology* (Springer, Berlin, Heidelberg, 2003), pp. 416–432
8. 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
9. A. Botta, W. de Donato, V. Persico, A. Pescap, Integration of cloud computing and internet of things: a survey. Future Gener. Comput. Syst. **56**, 684–700 (2016), http://www.sciencedirect.com/science/article/pii/S0167739X15003015
10. W. Boyang, L. Baochun, L. Hui, Oruta: privacy-preserving public auditing for shared data in the cloud. IEEE Trans. Cloud Comput. **2**(1), 43–56 (2014)
11. I. Butun, S.D. Morgera, R. Sankar, A survey of intrusion detection systems in wireless sensor networks. IEEE Commun. Surv. Tutor. **16**(1), 266–282 (2014)
12. B.V., I.N.: CompTIA Cloud Essentials Certification Study Guide (Exam CLO-001) (McGraw-Hill, New York, 2014)
13. N. Cao, C. Wang, M. Li, K. Ren, W. Lou, Privacy-preserving multi-keyword ranked search over encrypted cloud data. IEEE Trans. Parallel Distrib. Syst. **25**(1), 222–233 (2014)
14. M. Crosbie, E.H. Spafford, Active defense of a computer system using autonomous agents (1995)
15. T. Cruz, L. Rosa, J. Proença, L. Maglaras, M. Aubigny, L. Lev, J. Jiang, P. Simões, A cybersecurity detection framework for supervisory control and data acquisition systems. IEEE Trans. Ind. Inf. **12**(6), 2236–2246 (2016)
16. J. Daniels, Server virtualization architecture and implementation. Crossroads **16**(1), 8–12 (2009)
17. 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**(C), 99–117 (2016). https://doi.org/10.1016/j.jnca.2016.01.010

18. X. Dong, J. Yu, Y. Luo, Y. Chen, G. Xue, M. Li, Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing. Comput. Secur. **42**, 151–164 (2014)
19. E. Elmroth, F.G. Marquez, D. Henriksson, D.P. Ferrera, Accounting and billing for federated cloud infrastructures, in *Eighth International Conference on Grid and Cooperative Computing, 2009 GCC'09* (IEEE, 2009), pp. 268–275
20. A. Ericsson, Ericsson mobility report: On the pulse of the networked society. Ericsson, Sweden, Technical Report EAB-14 61078 (2015)
21. M.A. Ferrag, A. Ahmim, Esspr: an efficient secure routing scheme based on searchable encryption with vehicle proxy re-encryption for vehicular peer-to-peer social network. Telecommun. Syst. 1–23 (2017). https://doi.org/10.1007/s11235-017-0299-y
22. M.A. Ferrag, L. Maglaras, A. Ahmim, Privacy-preserving schemes for ad hoc social networks: a survey. IEEE Commun. Surv. Tutor. **19**(4), 3015–3045 (2017)
23. M.A. Ferrag, L.A. Maglaras, H. Janicke, J. Jiang, A Survey on Privacy-preserving Schemes for Smart Grid Communications (2016), arXiv:1611.07722
24. M.A. Ferrag, L.A. Maglaras, H. Janicke, J. Jiang, Authentication Protocols for Internet of Things: A Comprehensive Survey (2016), arXiv:1612.07206
25. I. Foster, Y. Zhao, I. Raicu, S. Lu, Cloud computing and grid computing 360-degree compared, in *Grid Computing Environments Workshop, 2008. GCE'08* (IEEE, 2008), pp. 1–10
26. Gartner, Inc: Gartner says 6.4 billion connected "things" will be in use in 2016, up 30 percent from 2015 (2015), http://www.gartner.com/newsroom/id/3165317
27. R.L. Grossman, Y. Gu, M. Sabala, W. Zhang, Compute and storage clouds using wide area high performance networks. Future Gener. Comput. Syst. **25**(2), 179–183 (2009)
28. J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (iot): a vision, architectural elements, and future directions. Future Gener. Comput. Syst. **29**(7), 1645–1660 (2013)
29. C. Guy, Wireless Sensor Networks, in *Sixth International Symposium on Instrumentation and Control Technology: Signal Analysis, Measurement Theory, Photo-Electronic Technology, and Artificial Intelligence*, ed. by J. Fang, Z. Wang, (eds.) SPIE-International society for optical engineering, vol. 6357 (2006), pp. 63571I–63571I–4. https://doi.org/10.1117/12.716964
30. K.K. Hausman, S.L. Cook, T. Sampaio, Cloud Essentials: CompTIA Authorized Courseware for Exam CLO-001 (Wiley, New York, 2013)
31. D. Hrestak, S. Picek, Homomorphic encryption in the cloud, in *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (IEEE, 2014), pp. 1400–1404
32. M. Jensen, J. Schwenk, N. Gruschka, L.L. Iacono, On technical security issues in cloud computing. in *IEEE International Conference on Cloud Computing, 2009. CLOUD'09* (IEEE, 2009), pp. 109–116
33. J. Yuan, S. Yu, Privacy preserving back-propagation neural network learning made practical with cloud computing. IEEE Trans. Parallel Distrib. Syst. **25**(1), 212–221 (2014)
34. J. Jin, J. Gubbi, S. Marusic, M. Palaniswami, An information framework for creating a smart city through internet of things. IEEE Internet Things J. **1**(2), 112–121 (2014)
35. Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, D. Qiu, Security of the internet of things: perspectives and challenges. Wirel. Netw. **20**(8), 2481–2501 (2014)
36. J.B. Kennedy, When woman is boss: an interview with nikola tesla, in *Colliers* (1926)
37. R. Khan, S.U. Khan, R. Zaheer, S. Khan, Future internet: the internet of things architecture, possible applications and key challenges, in *2012 10th International Conference on Frontiers of Information Technology (FIT)* (IEEE, 2012), pp. 257–260
38. M.T. Khorshed, A.S. Ali, S.A. Wasimi, A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Gener. Comput. Syst. **28**(6), 833–851 (2012)
39. J. Kirschnick, J.M.A. Calero, L. Wilcock, N. Edwards, Toward an architecture for the automated provisioning of cloud services. IEEE Commun. Mag. **48**(12), 124–131 (2010)
40. S. Kumar, Classification and detection of computer intrusions. Ph.D. thesis, Purdue University (1995)

41. I. Lee, K. Lee, The internet of things (iot): applications, investments, and challenges for enterprises. Bus. Horiz. **58**(4), 431–440 (2015), http://www.sciencedirect.com/science/article/pii/S0007681315000373
42. Li, M., Yu, S., Ren, K., Lou, W.: Securing personal health records in cloud computing: patient-centric and fine-grained data access control in multi-owner settings, in *International Conference on Security and. Privacy in Communication Systems* (Springer, Berlin, Heidelberg, 2010), pp. 89–106, http://link.springer.com/10.1007/978-3-642-16161-2_6
43. H. Liu, H. Ning, Q. Xiong, L.T. Yang, Shared authority based privacy-preserving authentication protocol in cloud computing. IEEE Trans. Parallel Distrib. Syst. **26**(1), 241–251 (2015)
44. C. Lyu, S.F. Sun, Y. Zhang, A. Pande, H. Lu, D. Gu, Privacy-preserving data sharing scheme over cloud for social applications. J. Netw. Comput. Appl. **74**, 44–55 (2016)
45. L.A. Maglaras, J. Jiang, T.J. Cruz, Combining ensemble methods and social network metrics for improving accuracy of ocsvm on intrusion detection in scada systems. J. Inf. Secur. Appl. **30**, 15–26 (2016)
46. 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
47. P. Massonet, S. Naqvi, C. Ponsard, J. Latanicki, B. Rochwerger, M. Villari, A monitoring and audit logging architecture for data location compliance in federated cloud infrastructures, in *2011 IEEE International Symposium on Parallel and Distributed Processing Workshops and Phd Forum (IPDPSW)* (IEEE, 2011), pp. 1510–1517
48. P. Mell, T. Grance et al., The NIST Definition of Cloud Computing (2011)
49. C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, M. Rajarajan, A survey of intrusion detection techniques in cloud. J. Netw. Comput. Appl. **36**(1), 42–57 (2013)
50. M. Naehrig, K. Lauter, V. Vaikuntanathan, Can homomorphic encryption be practical? in *Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop* (ACM, 2011), pp. 113–124
51. NHS England: Digital diabetes coach (2015), https://www.england.nhs.uk/ourwork/innovation/test-beds/diabetes-digital-coach/
52. M. Nitti, R. Girau, L. Atzori, Trustworthiness management in the social internet of things. IEEE Trans. Knowl. Data Eng. **26**(5), 1253–1266 (2014)
53. A. Nordrum, Popular internet of things forecast of 50 billion devices by 2020 is outdated. IEEE Spectrum, http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billiondevices-by-2020-is-outdated. Accessed 18 2016
54. T.F.M. Pasquier, J. Singh, J. Bacon, Clouds of things need information flow control with hardware roots of trust, in *2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom)* (IEEE, 2015), pp. 467–470
55. S.K. Pasupuleti, S. Ramalingam, R. Buyya, An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing. J. Netw. Comput. Appl. **64**, 12–22 (2016)
56. A. Rabkin, M. Arye, S. Sen, V.S. Pai, M.J. Freedman, Making every bit count in wide-area analytics, in *HotOS* (2013), p. 6
57. A. Rabkin, R.H. Katz, Chukwa: a system for reliable large-scale log collection. LISA **10**, 1–15 (2010)
58. B.B.P. Rao, P. Saluia, N. Sharma, A. Mittal, S.V. Sharma, Cloud computing for internet of things & sensing based applications, in *2012 Sixth International Conference on Sensing Technology (ICST)* (2012), pp. 374–380
59. Rico, J., Sancho, J., Cendon, B., Camus, M.: Parking easier by using context information of a smart city: enabling fast search and management of parking resources, in *2013 27th International Conference on Advanced Information Networking and Applications Workshops* (2013), pp. 1380–1385
60. J.W. Rittinghouse, J.F. Ransome, Cloud computing: Implementation, Management, and Security (CRC press, Boca Raton, 2016)

61. R.J. Robles, T.h. Kim, D. Cook, S. Das, A review on security in smart home development. Int. J. Adv. Sci. Technol. **15** (2010)
62. SafeCast Project: Safecast project website (2017), http://safecast.jp/en/
63. P. Samarati, S.D.C. di Vimercati, S. Murugesan, I. Bojanova, Cloud Security: Issues and Concerns (Wiley, New York, 2016)
64. R.M. Savola, H. Abie, Metrics-driven security objective decomposition for an e-health application with adaptive security management, in *Proceedings of the International Workshop on Adaptive Security* (ACM, 2013), p. 6
65. J. Shao, R. Lu, X. Lin, FINE: A fine-grained privacy-preserving location-based service framework for mobile devices, in IEEE INFOCOM 2014 - IEEE Conference on Computer Communications (IEEE, 2016), pp. 244–252
66. J. Singh, J. Bacon, J. Crowcroft, A. Madhavapeddy, T. Pasquier, W.K. Hon, C. Millard, Regional clouds: technical considerations, University of Cambridge, Computer Laboratory, Technical Report (2014)
67. J. Singh, J. Bacon, D. Eyers, Policy enforcement within emerging distributed, event-based systems, in *Proceedings of the 8th ACM International Conference on Distributed Event-Based Systems* (ACM, 2014), pp. 246–255
68. J. Singh, T. Pasquier, J. Bacon, H. Ko, D. Eyers, Twenty security considerations for cloud-supported internet of things. IEEE Internet Things J. **3**(3), 269–284 (2016)
69. W. Song, B. Wang, Q. Wang, Z. Peng, W. Lou, Y. Cui, A privacy-preserved full-text retrieval algorithm over encrypted data for cloud storage applications. J. Parallel Distrib. Comput. **99**, 14–27 (2017)
70. B. Stewart, L. Rosa, L.A. Maglaras, T.J. Cruz, M.A. Ferrag, P. Simoes, H. Janicke, A novel intrusion detection mechanism for scada systems that automatically adapts to changes in network topology (2017)
71. J. Sun, X. Zhu, Y. Fang, A privacy-preserving scheme for online social networks with efficient revocation, in *2010 Proceedings IEEE INFOCOM* (IEEE, 2010), pp. 1–9
72. W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y.T. Hou, H. Li, Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking. IEEE Trans. Parallel Distrib. Syst. **25**(11), 3025–3035 (2014)
73. T. Chen, S. Zhong: Privacy-preserving backpropagation neural network learning. IEEE Trans. Neural Netw. **20**(10), 1554–1564 (2009)
74. University of Southampton, Southampton researchers develop new tool to provide radiation monitoring in Japan (2013), http://www.southampton.ac.uk/news/2013/05/radiation-monitoring-in-japan.page
75. K. Venkatasubramanian, A. Banerjee, S. Gupta, PSKA: usable and secure key agreement scheme for body area networks. IEEE Trans. Inf. Technol. Biomed. **14**(1), 60–68 (2010)
76. O. Vermesan, *IERC Cluster Book 2016*, Innovation and Deployment. European Research Cluster on the Internet of Things, IoT Digital Value Chain Connecting Research (2016)
77. O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I.S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer et al., Internet of things strategic research roadmap. Internet Things-Global Technol. Soc. Trends **1**, 9–52 (2011)
78. B. Wang, S. Yu, W. Lou, Y.T. Hou, Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud, in *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications* (IEEE, 2014), pp. 2112–2120
79. C. Wang, S.S. Chow, Q. Wang, K. Ren, W. Lou, Privacy-preserving public auditing for secure cloud storage. IEEE Trans. Comput. **62**(2), 362–375 (2013)
80. L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, A.V. Vasilakos, Security and privacy for storage and computation in cloud computing. Inf. Sci. **258**, 371–386 (2014)
81. S.G. Worku, C. Xu, J. Zhao, X. He, Secure and efficient privacy-preserving public auditing scheme for cloud storage. Comput. Electr. Eng. **40**(5), 1703–1713 (2014)
82. Z. Xia, X. Wang, X. Sun, Q. Wang, A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. IEEE Trans. Parallel Distrib. Syst. **27**(2), 340–352 (2016)

83. Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, K. Ren, A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing. IEEE Trans. Inf. Forensics Secur. **11**(11), 2594–2608 (2016)
84. Z. Xia, N.N. Xiong, A.V. Vasilakos, X. Sun, EPCBIR: An efficient and privacy-preserving content-based image retrieval scheme in cloud computing. Inf. Sci. (Ny). **387**, 195–204 (2017)
85. Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for internet of things. J. Netw. Comput. Appl. **42**, 120–134 (2014)
86. Y. Yu, M.H. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, G. Min, Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. IEEE Trans. Inf. Forensics Secur. **12**(4), 767–778 (2017)
87. J. Zhou, Z. Cao, X. Dong, N. Xiong, A.V. Vasilakos, 4S: a secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks. Inf. Sci. (Ny). **314**, 255–276 (2015)
88. J. Zhou, X. Lin, X. Dong, Z. Cao, PSMPA: patient self-controllable and multi-level privacy-preserving cooperative authentication in distributedm-healthcare cloud computing system. IEEE Trans. Parallel Distrib. Syst. **26**(6), 1693–1703 (2015)
89. H. Zhu, R. Lu, C. Huang, L. Chen, H. Li, An efficient privacy-preserving location-based services query scheme in outsourced cloud. IEEE Trans. Veh. Technol. **65**(9), 7729–7739 (2016)