Realizing an Internet of Secure Things: A Survey on Issues and Enabling Technologies

Salma Abdalla Hamad, Quan Z. Sheng, *Member, IEEE*, Wei Emma Zhang, *Member, IEEE*, and Surya Nepal, *Member, IEEE*

***Abstract*—Since the term first coined in 1999, the Internet of Things (IoT) has gained significant momentum in connecting physical objects to the Internet and facilitating machine-to-human and machine-to-machine communications. By offering the capability to connect and integrate both digital and physical entities, IoT becomes an important paradigm that enables a whole new class of applications and services. Security is one of the most challenging issues that need to be addressed before these IoT applications and services can be fully embraced. In this survey, we investigate the major research efforts over the period of 2013-2019 that address IoT security and privacy issues. We provide extensive discussions on securing cloud-based IoT solutions. The main focus of these discussions is on securing the information in transit between IoT devices and IoT applications, where most of the data processing and modelling tasks take place. These discussions include all security aspects and challenges facing the data in transit. Specifically, a number of common attacks that target IoT solutions are first discussed, while presenting the main challenges of IoT security (e.g., the resource limitation of IoT devices, which hinder the ability of such devices to do expensive computations for securing the data). Then we present the main security requirements needed by IoT systems, which include access control, integrity, and authentication. We review recent research work in providing security and privacy services, which delegate the expensive computations to an edge or cloud, to cope with the low computations restrictions in IoT devices. Open research issues and possible research directions in securing cloud-based IoT systems are discussed, while proposing some possible solutions.**

***Index Terms*—Internet of Things, secure M2M, security and privacy, outsourcing computations, attribute based cryptography, access control, anonymous authentication, data integrity.**

I. Introduction

THE SMARTER the network develops the more challenges need to be overcome to ensure Internet of Things (IoT) security and privacy [1]. To realize the recent smart world requirements, systems need models for monitoring physical data and environmental conditions. These models capture environmental data using sensors, and then transfer the data to be processed or monitored through a gateway to the cloud. IoT brings the physical and digital worlds together in the sense that IoT is creating a seamless integration of physical things into communication networks.

In the near future, everything will be embedded with small devices that connect them to the Internet [2], to enhance various application domains in our daily life, such as smart cities, smart homes, smart transportation, smart health and smart surveillance systems. Thus, IoT provides intelligent services for human life improvement [3]. Knowing that, IoT devices are heterogeneous in nature, leading to different types of security threats. Information risk increases with the deployment of growing number of the smart things. The limited resources owned by these devices make them vulnerable to security attacks, such as denial of service attacks [2]. These attacks can be performed on different layers of an IoT architecture.

A. IoT Architecture

The generic architecture of IoT systems consists of three main layers as illustrated in Fig. 1, including the *physical layer* (collection of data), the *information layer* (data analytics, sharing and storage) and the *application layer* (use of data).

The Physical Layer acquires data from sensors and network technologies making up an IoT ecosystem. In IoT services, sensors communicate with each other or with cloud-based servers. IoT devices have limited capacity to transmit large messages, due to the low radio frequency operation mode and low computational abilities. Data collection is done at this layer using actual physical devices, such as RFID (radio frequency identification) sensors and others. Securing the physical device itself is as important as securing data transferred to or from the device. The limited hardware and application protection of IoT systems, caused the most common threats in the physical layer. The devices at this level need to be secured, to protect the collected data and owners privacy.

The Information Layer processes the collected data and then takes actions according to the application needs and requirements. The data are then either stored or sent for distribution towards the application layer. This layer is attracting attention of researchers in the recent years, as it facilitates

Manuscript received April 25, 2019; revised November 1, 2019; accepted February 15, 2020. Date of publication February 25, 2020; date of current version May 28, 2020. The work of Quan Z. Sheng was supported by Australian Research Council Future Fellowship under Grant FT140101247. *(Corresponding author: Salma Abdalla Hamad.)*

Salma Abdalla Hamad and Quan Z. Sheng are with the Department of Computing, Faculty of Science and Engineering, Macquarie University, Sydney, NSW 2113, Australia (e-mail: salma-abdalla-ibrahim-mah.h@students.mq.edu.au; michael.sheng@mq.edu.au).

Wei Emma Zhang is with the School of Computer Science, University of Adelaide, Adelaide, SA 5005, Australia (e-mail: wei.e.zhang@adelaide.edu.au).

Surya Nepal is with the Data61, CSIRO, Sydney, NSW 2121, Australia (e-mail: surya.nepal@data61.csiro.au).

Digital Object Identifier 10.1109/COMST.2020.2976075

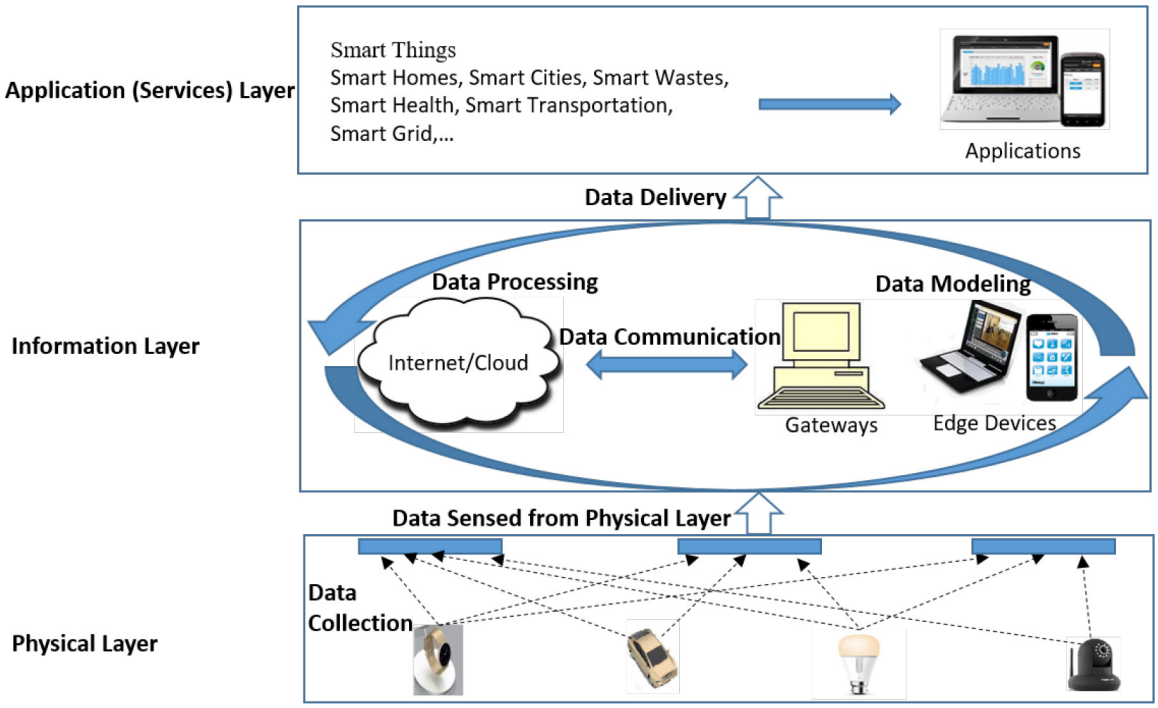

Fig. 1. A generic architecture of IoT systems. The physical layer collects data to be processed and modeled in the information layer, which then delivers the data to the application layer.

the development and integration of services [4]. The security and privacy components are required to ensure the collected data authenticity and to maintain the user's privacy. Different algorithms and techniques can be used in this layer for data processing, decision making, ensuring the protection and maintaining the privacy of the moving data, data owners and data consumers. The details of threats and current solutions to secure and maintain data privacy at this level, will be discussed throughout this survey.

The Application Layer focuses on the feature specification for providing services, according to the final service implementation. This layer provides the user with the system's intended functionalities. It also inherits all the functionalities from the Information Layer [4].

B. Risks and Limitations

This section presents some of the security risks and limitations for IoT devices in general across different layers, with more focus on threats targeting the Information Layer.

Physical Layer: To improve the security of IoT products, IoT devices need to be frequently patched and updated [5]. However, IoT devices have limited battery power as well as limited computational ability. In general, devices can be implemented on a broad spectrum of hardware and software. On the one hand, servers, desktops and some types of smartphones are usually on the high end of the spectrum. On the other hand, embedded systems, RFID and sensor networks are on the lower end of the spectrum [6].

In regards to the hardware, IoT devices rely on microcontrollers which can vary in performance attributes. The most common available microcontrollers are 8-bit, 16-bit and 32-bit microcontrollers [6]. As indicated in [6], there are significant sales of 4-bit microcontrollers for certain ultra-low cost applications. These ultra-low cost microcontrollers usually contain only a small number of simple instructions. Accordingly, a huge number of cycles will be needed to execute traditional cryptographic algorithms, thus making them time and energy inefficient for applications involving these devices [6]. Moreover, some microcontrollers have very limited amount of random-access memory (RAM) and read-only memory (ROM). For instance, for TI COP912C [7], [8], the amount of memory can be as little as 16 bytes of RAM. Furthermore, the bottom of the spectrum lies the RFID tags that are not battery-powered, which are powered by limited surrounding environmental power and have limited number of gates available to serve the security requirements. A study on the constraints of such devices for cryptographic applications was performed in [9].

Regarding the IoT software level, there are a number of operating systems that are designed to perform within constrained memory, size and power used by current IoT devices, such as ARM Mbed [10], Brillo (Google Android Things) [11], Ubunto core [12], RIOT OS [13] and Contiki OS [14]. IoT OS security is very important and should support security services and privacy. However, most of these common operating systems are incapable of addressing the needed security requirements for IoT infrastructures [15], [16]. The challenge is to build less vulnerable standardized, secure operating system for the constrained devices that can provide all of the security and privacy services. Protecting IoT devices with the given limitations is a challenge. Nevertheless, security patching is considered as one of these challenges that will expose IoT systems to a number of security risks.

Information Layer: There are a number of protocols and standards that help empowering IoT devices and applications. The most common IoT infrastructure and transport protocols used are IPv6 over Low-Power Wireless Personal Area Networks (6LowPan), Internet Protocol v4/v6 (IPv4/IPV6), Routing Protocol for Low-Power and Lossy Networks (RPL), Bluetooth, Long Range Wide Area Network (LoRaWan), Zonal Intercommunication Global-standard (ZigBee) and Z-Wave. Regarding IoT data protocols, the most commonly used protocols are Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP) and Advanced Message Queuing Protocol (AMQP), WebSocket and Node [17]. Unfortunately, these protocols mostly are deployed insecurely, resulting in sensitive data leakage, such as device details, credentials, and network configuration information [18]. For instance, it was reported in [18] that the flawed implementations of MQTT which serves as one of the backbones of IoT and industrial IoT communications, expose sensitive information on the devices/servers to attackers using raw commands. Moreover, since MQTT can also be used for IoT devices software and firmware updates, this makes IoT devices more vulnerable to attacks [19]. The authors of [20] discussed the available security protocols and presented them in respect to the IoT layers. They analyzed the risks associated with each of the layers showing protection gaps. For instance, from this analysis, they observed that there is no fragmentation attack protection in the physical layer, the network layer, the transport layer and the application layer. They also highlighted that replay protection is not supported in the physical layer, the network layer and the 6LoWPAN layer [20].

IoT generated data from sensor devices flow to a cloud, Internet, gateway or another device within the information layer. This data will be used in IoT applications. The information layer includes real-time and mobile data that feeds different IoT applications through cloud, gateways or edge devices and are sent from resource constrained sensors. Accordingly, IoT systems have to deal with multiple threats or attacks which are described in Table I.

Application Layer: The exposure and communication of IoT systems to the Internet have introduced new security requirements that applications should follow [24], [25]. Malicious modules can be deployed on nodes by attackers. Moreover, malicious users can attack vulnerabilities on operating systems (e.g., exploiting a buffer overflow vulnerability). Accordingly, software applications should run isolated from any other application, and other applications should not be able to intercept or alter its run-time state [26]. Furthermore, vulnerabilities in Web applications and IoT software can lead to compromised systems. For instance, Web applications can be exploited to either steal user credentials or to inject malicious software.

C. Contributions and Paper Organization

In this work, we have surveyed more than 100 information security related work over the period of 2013-2019, while a number of them are specifically for securing the IoT with the focus on their diversity.

The security and privacy issues in each of the three layers of the IoT system architecture have been studied independently under the theme of IoT device security, cloud/edge security, and application security. However, such independently developed security solutions miss the point that IoT services and applications are delivered by collecting data from the physical layer, processing them at the devices/edges/cloud and then being accessed or consumed by users via applications and services. To the best of our knowledge, none of the previous surveys looks at the security solutions at the information processing layer while considering the interactions with the physical and application layers. To the best of our knowledge, this is the first survey that attempts to include all security aspects and security challenges facing the information layer of IoT solutions including outsourcing techniques for partial computations on edge or cloud, while presenting case studies to map security challenges and requirements in real IoT scenarios. We first study the common security attacks that can target IoT systems, while understanding the significant security requirements to counter such attacks. The significant security requirements for all cases are data secrecy protection, integrity, access control, privacy protection and the need for outsourcing computations to tackle the resource constrained devices problem. Accordingly, we identify and arrange the literature targeting each of these requirements, and study the recent research advances to secure the data and the users in IoT. Then we identify the criteria, to study and compare these research works. We focus on the IoT special requirements due to the resource limitations. This leads us to survey outsourcing and delegation of computation mechanisms in the literature. Finally, after reviewing different techniques for securing IoT and comparing them to the defined requirements for IoT systems, we identify several open issues that researchers can work on, in order to eventually achieve a more secure, efficient, and scalable IoT ecosystem.

The remainder of this survey is presented as follows. Section II presents related work and summarizes the differences between previous surveys and this paper. Section III presents a walk-through on some of the important security concepts and security requirements for cloud based IoT. Three IoT applications are used as case studies, to reflect the security solutions needed for cloud-based IoT systems. Section IV explores possible solutions to mitigate cloud-based IoT threats. Section V discusses recent solutions for IoT cloud data sharing, including solutions for data access control, data and user privacy, integrity of IoT data, outsourcing of computations for IoT devices to edge or cloud, respectively. Section VI discusses some open challenges, to direct researchers in this area. Finally, Section VII concludes the survey.

II. Related Work

A number of surveys studied and highlighted recent research work that focus on providing solutions for the IoT framework enhancements [27], [28]. In general, most of these surveys focused more on enabling technologies, business process and data modeling related issues. Some surveys focused on IoT

TABLE I
SECURITY THREATS FACING IOT AND POSSIBLE COUNTERMEASURES. THESE PRESENTED ATTACKS INCLUDE NETWORK, SOFTWARE AND HARDWARE ATTACKS THAT CAN TARGET IOT SOLUTIONS

Threat/Attack	**Description and Possible Countermeasures**
Fabricating Attack (forgery)	This attack fabricates a message and sends it to another person, while pretending to be a certain person (e.g, pretend to be your manager and send a promotion email to HR for yourself). To counter this attack, the receiver of the message should authenticate the sender source. This can be achieved by Public Key Infrastructure (PKI) or similar signature techniques such as Attribute Based Signature (ABS).
Masquerade Attack	Malicious attackers duplicate valid entities, to be able to either access systems or impersonate a person. PKI can counter this problem by issuing a trusted identity certificate from a trusted Certificate Authority, while systems should always check on the validity dates of certificates, the certificate trust path (hierarchy) as well as revocation list.
Interception and Eavesdropping Attack	It attacks data and user privacy. Encryption techniques, such as AES should be used, to counter it.
Data Alteration and Modification	The integrity of exchanged or saved data can broke by modifying or deleting part or all of its content. Public Key Infrastructure (PKI) can be used as a way to detect and prevent data alteration. Hash functions as well as HMAC techniques can also help counter such attacks.
Illicit Access	Curious attackers try to access systems that they should not be able to access. To combat such attack, access control techniques should be used. Access control techniques are either cryptographic, such as Identity Based Encryption (IBE) and Attribute Based Encryption (ABE) or non- cryptographic techniques such as Role-Based Access Control Technology (RBAC).
Replay Attack	In this attack, attackers resend correct data, which they gathered maliciously. Their target is to gain access to systems. There are a number of solutions to counter such attack, such as adding timestamps to the messages.
Man-in-the-middle Attack (M-I-T-M)	In M-I-T-M attack, a malicious entity secretly eavesdrop on the communication and can alters the communication between two entities, while the two entities think that they have direct communication. Cryptographic solutions from encryption techniques as well as mutual authentication techniques, are the common ways to prevent this type of attacks.
Impersonation/Sybil Attack	Sybil is a type of impersonation or fabrication attack. To prevent such attack, PKI solutions with trusted identity certificates should be used as well as other signature techniques such as digital signature or ABS.
Collision Attack	One or more illicit entities can collide together and combine their credentials to access data, that each one of them separately can't access. Each access control system has different ways to prevent such attack. For example the use of identity certificate using PKI can mitigate these attacks.
Timing Attack	It is delaying time sensitive information, which can significantly affect time-critical applications. Such attacks can be prevented, by adding timestamps to data as well as by appending digital signatures.
Denial of Service (DOS)	This attack targets the data or system availability, in which malicious entities try to disallow system users from using the service/data. Different techniques can be used to reduce the effect of such attacks. For example, clustering (duplicate or triplicate) of all important servers or services.
Malware Attack	Also called software attacks. Software attacks are the major source of security vulnerabilities in any system. These attacks have different forms such as worms, virus, trojan horse, and logic bombs. These attacks also can exploit a buffer overflow or inject malicious code into the system using different techniques such as sql injection. There are some famous malware attacks targeting IoT operating systems (OS) such as Mirai and the recently discovered malware Silex [21]. Silex is a malware running across the Internet with focus on bricking IoT devices. Once it finds a Unix-based system with default login credentials, it overwrites all of the system's storage with random data, drops its firewall rules and network configuration, and then restarts the system effectively rendering the device useless [21]. To protect devices against such attacks embedded security as well as physical security mechanisms should be implemented.
Ransomware Attack	It is a subset of malware which locks the data on a victim's computer, typically by encrypting it. Backing up data and ensuring business continuity by having disaster recovery plans is one of the usual recommended techniques to protect the data against this attack.
Security Attack on Devices With Limited Resources	IoT sensors and devices have limited computational ability, which makes it difficult to use traditional cryptographic techniques. To handle such problem, lightweight cryptographic solutions as well as delegation or outsourcing part of the encryption and decryption process to a computational powerful device, can be used.
Side Channel Attacks	This is a non-invasive type of attacks that are based on "side channel Information" that can be retrieved from the encryption device that is neither the plain-text to be encrypted nor the cipher-text resulting from the encryption process [22]. Side channel attackers can use different techniques such as timing attack, hardware glitching attack and power analysis. There are a number of countermeasures for these attacks such as blinding. However, the known countermeasures can work on certain scenarios but not for all. Accordingly, security should be embedded as one of the building blocks starting from the design phase.
Hardware Semi-Invasive and Invasive Attacks	Attacks on the device hardware such as decapping package and use infrared emission analysis of backside to find location for attack then use laser to flip bits and break encryption. Other examples of hardware invasive attacks are micro-probing and modify chip with Focused Ion Beam (FIB). Physical security for devices can limit such attacks [23], devices should have physical safeguards against tampering or at least limit the access to the hardware by putting the devices in restricted place or secured with the appropriate locks or other tools.

security such as [2], [29], [30], [31]. The depth and security coverage of these surveys are illustrated in Table II.

In [27], the authors focused on cloud-based IoT, and presented enabling technologies and future applications. A number of IoT concerns were discussed but not security issues. In 2014, the authors of [28] studied 50 projects implemented between 2001 and 2011, and presented a deep analysis of context aware computing in IoT. The analysis included a number of open research ideas. For instance, the authors suggested to address security and privacy issues in different layers of their

TABLE II
SECURITY SERVICE DISCUSSED IN IOT SECURITY SURVEYS

Paper Reference	Year	Security Service Discussed
Gubbi et al. [27]	2013	Identification, Integrity, Privacy.
Perera et al. [28]	2014	Authorization, Authentication, Integrity, Secrecy, Trust.
Granjal et al. [32]	2015	Authorization, Authentication, Integrity, Secrecy, Trust.
Sicari et al. [29]	2015	Authentication, Identification, Privacy, Trust, Integrity, Secrecy.
Gil et al. [33]	2016	Authorization, Identification, Privacy, Integrity, Trust.
Sain et al. [2]	2017	Authentication, Privacy, Authorization, Mobility.
Sfar et al. [30]	2017	Identification, Authorization, Trust, Privacy.
Zhou et al. [31]	2017	Authentication, Anonymous Authentication, Privacy, Mobility.
Noor & Hassan [34]	2019	Authorization, Authentication, Trust.
Our Work	2019	Authentication, Privacy, Secrecy, Authorization, Integrity, Scalability, Outsourcing partial computations to secure the resource constrained devices data.

proposed model. However, the authors did not present actual research work in the security field.

In [32], an investigation of current IoT communication protocols and security mechanisms were presented. The authors presented security requirements and solutions on a standardized five layer protocol stack. The main focus of their work is on security issues related to several standards, e.g., IEEE 802.15.4, Constrained Application Protocol (CoAP) and IPv6 Low-power Wireless Personal Area Networks (6loWPAN), thus, limiting their research activity to a number of standards. Moreover, the authors did not consider other IoT security related issues as well as the limited computational resources in IoT devices.

The authors of [29] analyzed the existing solutions related to security, privacy, and trust in IoT. However, they did not present a clear IoT taxonomy and there was no logical sorting for the listed research activities. Moreover, the paper does not target security from the point of view of resource constrained devices. In 2016, the authors of [33] reviewed IoT techniques and architectures and also spotlighted some data-related challenges. The authors focused mainly on Social Internet of Things (SIoT), while giving little attention to security issues.

Sain *et al.* [2] classified IoT security into communication security, application security, and data security. The authors reviewed recent IoT technologies, techniques and models and showed the security gap in existing communication technologies, application interfaces, and data security. Another focus of the work was highlighting recent IoT related efforts, as well as giving very high-level introduction on network communication technologies used by IoT. The authors then discussed communication security within IoT layers for each IoT protocol. The paper was limited to certain security services, while not covering anonymity. Although the survey mentioned that the devices in IoT are resource constrained, it did not present research works that target such problem.

In [30], security challenges facing the IoT and some solutions proposed for each security challenge were presented. The authors of this paper offered a guideline that considers intellectual IoT techniques, which the authors claimed that it was specifically effective for constrained and heterogeneous IoT ecosystems. The paper described IoT context by a tetrahedron-shaped model, representing end-points and how they connect and interact to each other. The authors then discussed each edge with related security research on it. The authors did not mention that the resource constrained limitation is one of the barriers in IoT security. Accordingly, they did not present any computation delegation or outsourcing techniques to solve such problem.

The authors of [31] discussed the security risks and challenges for IoT cloud based data communication, while presenting some of the IoT security and privacy essentials. They defined the need to identity privacy with the term "conditional identity privacy", focusing on protecting the IoT user's identity from being revealed in public. However, when a disagreement occurs, the identity should be fetched only by the authorities. This paper presented some common attacks and security needs for securing packet forwarding and privacy authentication in cloud based IoT, while focusing on location privacy and mobile IoT devices. This survey focused only on mobile IoT and the location privacy, without consideration of anonymous access control to protect the identity of receivers. Moreover, the scalability issue, as well as users and/or attributes management and revocation, were not discussed.

In [34], the authors categorized IoT threats into three categories: threats in the perception layer, threats in the network layer, and threats in the application layer. The authors also included an overview of current countermeasures for the aforementioned threats. The survey focused on the weakness of current authentication methods, declaring that most of current authentication techniques do not provide an ideal authentication solution for IoT systems. The authors mentioned light weight encryption techniques as for securing end-to-end communications. However, they did not go in depth in current access control methodologies as well as data integrity techniques and the possibility of implementing these methodologies in IoT infrastructures.

A number of surveys focused on specific aspects of IoT security. For instance, the authors of [35] reviewed IoT frameworks and the details of the security features within each framework. The authors of [36] abstracted IoT systems into four layers, and presented a high level overview of the security challenges and solutions for each of the proposed layers.

The previous discussions revealed that most of the introductory surveys did not have a holistic review on IoT security requirements. On the one hand, some of these surveys did not consider securing IoT as a priority. Other surveys included security but with very limited discussions. On the other hand, in our work, we include diverse IoT security services such as, Authentication, Privacy, Confidentiality, Integrity, Access control, Non-repudiation as well as management issues such as attributes and user revocation. Moreover, we present existing works that target securing the limited computational resourced IoT-cloud based devices. The target of this survey is to provide

TABLE III
MAJOR SECURITY REQUIREMENTS FOR IOT SYSTEMS

Requirement/Service	Description
Confidentiality/Secrecy	It prohibits the interpretation of sensory data (in transit or at rest) from attackers. Allowing only legitimate users to access data.
Integrity	Needed to ensure the detection of any modification of the data sent by sensors.
Authentication	It is needed for most secure IoT communications, to be able to identify the communication peer. This helps to prevent fabrications or impersonation attacks.
Privacy Protection	RFID tags are widely spread. Recently, it became, easy to track or identify objects using their tags, thus, raising privacy concerns. In addition, as wearable and implanted health devices increases its pace, our bodies will be connected to the Internet from the small embedded devices. Consequently, people personal information such as, health care records or location must be secured and prevent its unauthorized disclosure.
Conditional Anonymity	Protecting the anonymity of users in some IoT related applications is crucial. Some users are reluctant to share data with others, to protect their privacy. Systems that don't protect user's anonymity may put the users under the risk of being attacked (impersonation, tracking) [38]. However, most IoT application need to authenticate the sender or receiver and ensure only particular authorities can trace this user (conditional Anonymity) which can be used for emergencies.
Access Control (Authorization)	It is needed to limit and control access to data as per the pre-defined access rules/privileges.
Non-repudiation	It prevents the data owner (source), the denial of previous data upload.
Availability	All sensor must be accessible while being used. The systems should be functional, and immune against attacks. High availability and clustering solutions can help maintain services availability
Scalability and Interoperability	The number of users and devices communicating grows widely with the growth in technologies. IoT devices interact with different patterns, with a large number of entities. Capabilities based access control mechanisms, assures and compliment IoT ecosystems security [39]. The proposed security protocols should be scalable enough, to handle massive number of users/sensors. The systems should allow the integration and communication of devices from different environments.
Resilience to Attacks	IoT devices are usually inexpensive with limited physical protection. Sensors can also be in remote locations with limited monitoring, that they can be easily moved. Thus, the sensed data output can be modified, without anyone noticing. As a result, single points of failure should be avoided as well as enforce different security measures to secure systems against different attacks.
Forward and Backward Security	Backward secrecy is to ensure that newly group joining entities, can't decipher data created before they joined the group. While, forward secrecy is to ensure that someone previously already had a key, after revoking him, he does not have access to future keys for the group.

a road map for IoT practitioners and researchers to enhance different IoT areas, thus, improving IoT security.

III. CONCEPTS AND CASE STUDIES

There are three main security requirements that need to be satisfied to protect any system, namely *Confidentiality (Secrecy)*, *Integrity*, and *Availability* [37]. Confidentiality ensures that the interpretation of a message is impossible for anyone except the targeted recipients. The integrity maintains the authenticity of the data in the IoT system. Availability ensures that the system can be accessed anytime and can serve in hostile conditions. Besides these main properties, there are a number of other security services, that are specifically important for IoT systems.

Table III describes the services that are needed in IoT systems. These services are needed by IoT systems to be able to mitigate security challenges and risks as well as other challenges due to the heterogeneous nature and the resources limitation problem of IoT sensors.

The typical entities of an IoT system include a data sender (sensors), a data receiver (users/ sensors or actuators), and a Cloud Service Provider (CSP), as shown in Fig. 2. The sensors send the sensed data to a cloud to be stored for later user's access. Most of the receivers use more cloud services for sharing and securing data. An actuator does not send data, but receives them to be used or further processed as per the application. The user is the entity that retrieves the specific data and accesses the shared data.

IoT solutions can use cloud and edge computing not only for storing data but also for delegating computations to it. This can ensure the data availability as well as to provide the needed processing power for the security operation of the constrained devices. The cloud can participate in the infrastructure management tasks such as keys and/or attributes issuing and revocation to facilitate the use of security services by IoT devices. IoT sensors can delegate partial computations during either encrypting or decrypting data to a powerful computational device.

The delegation of computations can be divided into two models. The first model is to delegate the computations directly to the cloud. The cloud has the highest computational power that can assist in all types of operations. However, the latency in communication will increase by sending and receiving directly to the cloud. The other approach is to use edge devices as a delegator. Edge computing is a way to enhance cloud computing by performing data processing at the network edge (e.g., mobile phone, access point, laptop) near the source of the data. In edge computing, substantial computing and storage resources (cloudlets, or fog nodes) are usually adjacent to sensors [40]. Edge devices can be used by IoT sensors/devices as a bridge or gateway to cloud. IoT devices can borrow some computational power from edge devices to do partial encryption/decryption during uploading/downloading data to cloud. Thus, latency will be reduced while maintaining security and countering the resource limitation of devices. Moreover, the use of cloudlet computing can increase scalability and availability (in case the cloud server is not responding or in case

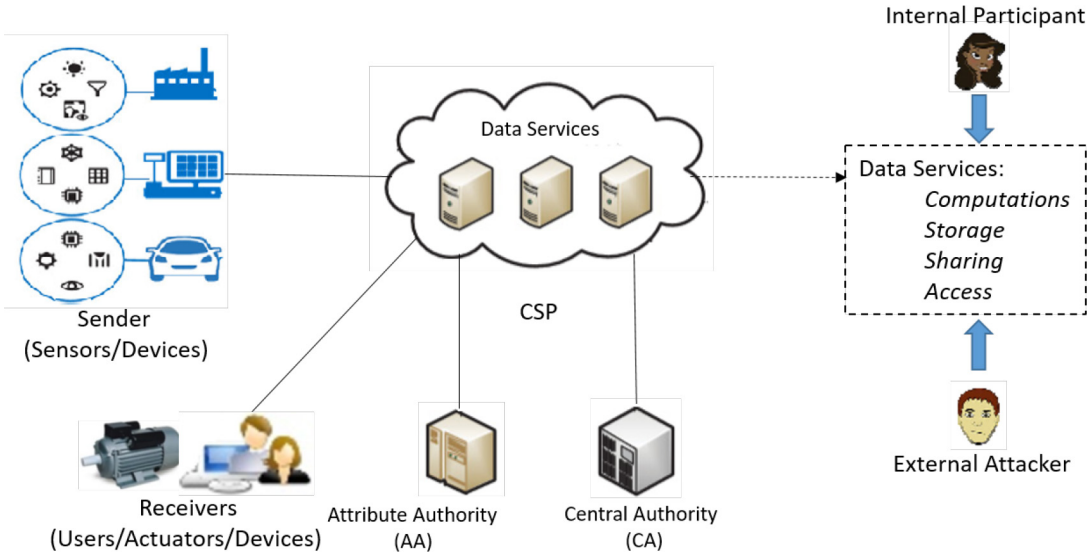

Fig. 2. A system model for cloud based IoT services.

of network failure) of IoT systems. Outsourcing techniques to edge device or cloud will be discussed in Section V.

To ensure security, a third party such as an Attribute Authority (AA) and/or Central Authority (CA) may be involved. An AA is a trusted key authority, that checks a user's identity to generate attribute keys. Moreover, it manages the revocation or updating of user's related keys when needed. In general, an AA verifies the users' identities through a CA.

In an IoT ecosystem, most connected devices do not previously know each other. Accordingly, symmetric security techniques for securing the communication will not be an effective solution. Thus, devices in such a situation usually depends on asymmetric security techniques, and uses a trusted third party for securing the communications. The focus of this proposal is on the techniques used to secure the communication and data sharing in an IoT ecosystem. A brief discussion of the current security techniques' limitations are presented and clarified in the following.

Firstly, authentication of source and confidentiality of data are crucial security requirements that can be achieved by the public key encryption techniques. However, most of the public key encryption algorithms use intensive calculations (e.g., Rivest-Shamir-Adleman (RSA). Moreover, these techniques are mainly based on certificates for identifying and authenticating entities. The verification and management of certificates consumes large amount of computation and bandwidth. Since most IoT devices are based on ultra-low-cost microcontrollers, the excursion of such traditional cryptographic techniques will not be practical enough for IoT applications [6]. Therefore, a lightweight encryption algorithm with limited communication overhead is needed for securing communication between devices with limited resources.

Secondly, some of the current personalized authentication solutions may leak information which can cause privacy concerns [41]. In the IoT scenario, it is important to keep IoT users and devices anonymous from malicious entities as well as the communicating parties, except in emergencies and critical situations.

Thirdly, there is a strong need for delegating the expensive computations to a powerful device to adapt the intensive computational encryption algorithms to the IoT systems with limited resources. There exist many techniques in the literature for outsourcing the computations. However, the challenge is retaining the privacy and secrecy of the data and users, while using the outsourced and lightweight IoT systems.

Finally, there is a demand for a security solution that can be lightweight enough to be used in resource-constrained IoT systems, while satisfying the required security requirements. To mitigate the aforementioned challenges, we set a number of objectives according to each of the following IoT case studies.

A. Smart Grids and Smart Meters

A smart metering system is a type of IoT-enabled technology that supports high frequency data collection compared to the existing metering systems. Smart grid users can securely manage and share their energy usage data. The captured data is analyzed and a report is created. This gives users the ability to inspect their energy consummation and correlate it with others (e.g., from the same suburban area). Accessing, analyzing, and responding to accurate and detailed data features, are crucial for an efficient use of the energy [42]. However, the more frequent the data is collected, the more the consumer's privacy is in risk, as it may expose the consumer's daily habits.

Smart grids and smart meters are essential for efficient energy management [42]. In [43], the authors showed the importance of not revealing the identity of users in smart grids. Moreover, a good number of surveys and technical papers discussed the security needs for smart grids. For example in [44], the authors analyzed the privacy concerns in smart cities, including identity privacy, query privacy, location privacy, footprint privacy and owner privacy [44]. Then, they proposed a model for mitigating these issues to ensure the privacy in smart cities.

Due to the openness of smart cities and smart grids technologies, IoT systems are deployed in a vulnerable

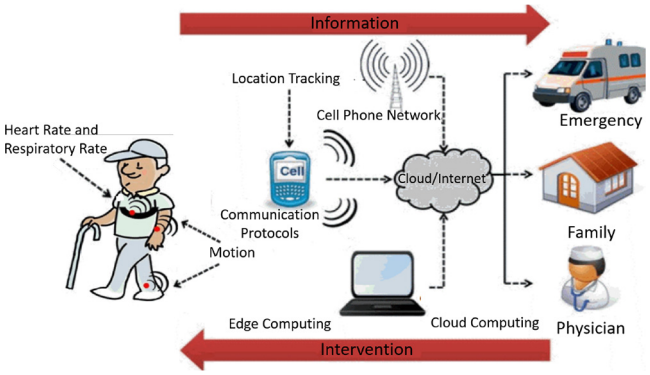

Fig. 3. Smart personal healthcare architecture.

environment under the risk of a number of security threats. Regarding smart grid, there is a number of security objectives for a practical solution, including:

- *Data Authenticity:* In smart grids, if malicious users alter or forge energy usage data, this would provide misleading reports [45]. While the concern can be addressed by using cryptographic and integrity methods, e.g., message authentication code (Integrity) or digital signatures (Authenticity), other issues may be difficult to handle such as anonymity and efficiency. In other words, systems need to make sure data is from an authentic source (from a valid member) and data content does not change.
- *Anonymity:* Energy usage data contains customers' private information [46], [47]. Hence, safeguarding the identity of consumers is crucial for such applications [48], to avoid raising privacy concerns and reluctance from the consumers to share their data.
- *Efficiency:* Data sharing in smart grids could be as big as sharing data of smart grids for a whole country [49]. Thus, the reduction of the computation and communication costs is very important to prevent energy waste.
- *Availability:* The ability to access services or systems even in hostile conditions is critical [45].
- *Access Control:* Access to systems or data is restricted to authorized users only [50].
- *Confidentiality (Privacy):* Data should be protected at all times (at rest and while moving) and can only be interpreted by authorized users and devices [49], [50].

B. Cloud Based IoT Health Devices and Patients Records Sharing

A Personal Healthcare Device (PHD) nowadays is one of the fundamental elements of healthcare applications. The demands for healthcare for chronic and cardiovascular patients have increased significantly over the past years [3]. PHDs are movable medical sensors used by healthcare practitioners, to measure, record, and share user's biomedical information as shown in Fig. 3. The importance of PHDs is evolving, due to the increased demand of people to carefully monitor their health. Accordingly, such devices must be able to securely and easily share information with the healthcare servers. However, the heterogeneity of these devices makes them difficult to be managed and maintained, thus are mostly vulnerable to attacks. For instance, in 2017 some implanted medical devices were attacked where the WannaCry ransomware attacked devices running Windows OS and encrypted the data on the hard drive, making the devices inaccessible by users [51]. Such devices (wearable or implanted health devices) need to sense and send data to authorized recipients. Accordingly, a fine grained access control of patients data sourced from e-health devices is needed, while controlling who to access all data and who to access the data without knowing the identity of patient (anonymity) as well as preventing access to user data if not authorized (e.g., not primary physician or secondary physician). Moreover, a survey on medical device cybersecurity risks [52] showed that healthcare security professionals concern medical device security, patient privacy and data breaches, specifically as the patients physiological data are transmitted through the Internet. Therefore, users need to be securely authenticated before using any of the IoT-based medical care services [3]. There is a number of security objectives for an efficient healthcare solution, including:

- *Data Authenticity (Integrity and Source Authentication):* Authentication is needed to certify that health data sources are credible and legitimate [53], [54].
- *Mutual Authentication:* Both the sender and receiver need to ensure each other's authenticity [3], [55].
- *Conditional Anonymity of Sender:* The true identity of a patient can be revealed to, e.g., primary physician or police but cannot be revealed to, e.g., research students or any other secondary doctor [56].
- *Access Control:* Fine grained access controls is required to define who to access the data [57].
- *Privacy:* Data should be protected at all times (at rest and while moving) [53], [54].
- *PHD and Health Implanted Devices Limited Computational Abilities:* It is critical to be able to offload encryption (partial) and decryption (partial) computations to proximity edge devices such as mobile phones or to the cloud, while preserving the data confidentiality and users keys privacy [3].

C. Smart Transportation (Smart City Applications)

The main goals of smart transportation are to build a real-time intelligent public transportation system to reduce traffic congestion, increase safety and efficient energy consumption, to name a few [58], [59]. Sharing information among vehicles (mobile sensing) can provide location awareness, geo-distribution, and communication efficiency [60]. Such data can be shared from the vehicle self-installed module or using an edge device (e.g., mobile phone) to the cloud as shown in Fig. 4. However, security and privacy in aforesaid infrastructure are challenging. Most of the cloud and fog service providers cannot be fully trusted. This will lead to the unwillingness of vehicle owners to share their collected data with strangers [60]. A trusted entity is needed, to prevent privacy violation, and promote the cooperation in uploading vehicles

Fig. 4. Smart transportation architecture.

data to fog nodes. Practical smart transportation systems should ensure that the following security services are in place:

- *Confidentiality:* The confidentiality of reports from vehicular IoT devices is one of the primary objectives to achieve [61].
- *Authentication of Source and Data Integrity:* Authentication is needed to certify that sources of vehicular sensing reports are credible and legitimate [62]. Blacklist-based authentication can help in preventing impersonation and Sybil attacks.
- *Anonymity and Privacy:* Privacy is a major concern, as the sensed data includes some information related to the drivers or passengers [61], such as their current location as well as their daily habits while driving. Accordingly, a system that can conceal the identity of the data source, while ensuring their authenticity is needed.
- *IoT Low Computational Ability (Secure Delegation to Cloud):* It is critical to be able to outsource partial encryption and/or partial decryption of the vehicular data to a fog device or cloud, while maintaining the data and the users privacy [63].
- *Non-repudiation:* It is important to prevent the data owner (source) the denial of previous uploaded data [63].

There are also several other security requirements that are needed for all the three IoT cases:

- *Unforgeability:* An attacker should not be able to pretend to be an honest sender in creating an authentic signature text that can be accepted by the decryption algorithm. Forging keys and attributes or certificates should also not be allowed [49].
- *Collision Resistance:* It should be infeasible that two or more users collide and combine their credentials to access data that each one of them separately cannot access [64], [65].
- *Unlinkability:* Attackers should not be able to link the used pseudonym (hidden name) with the true identity of the sender (multi-show) [66], e.g., given two messages and their signatures, no one should be able to tell if the same signer signed both messages.
- *Revocation:* User revocation is of great importance to IoT systems. A user/device may have limited subscription period and has expired or the device has been attacked or stolen. Accordingly the communicating party needs to find out whether a user/device is revoked [67]. Any revoked user/device should not be allowed to read the data or authenticate himself. Efficient revocation is very challenging and it is especially important for a large-scale network.

IV. Security Mechanisms

This section explores some of the current or possible solutions to mitigate the previously discussed security threats. To assure data security and preserve the privacy of users in IoT solutions, different security mechanisms are needed for each of the IoT architecture layers. Protection of both the physical and application layers should be ensured by including both software and physical security measures to safeguard data security and data owner's privacy. IoT operating systems require an end-to-end security approach that should address security issues during the design phase. The software that is running on embedded devices needs to be secured, regularly updated and the solutions should have the ability to limit access to embedded systems to a need-to-use basis. Moreover, the embedded systems should provide a way for network administrators to monitor connections to and from the embedded systems. Furthermore, the systems should have the ability to integrate with third-party security management systems.

The operating system should support some important security features, such as securing the memory of the nodes [68]. On the nodes, all modules must not interfere with each other [68] and the implemented software should include cryptographic solutions for authentication and hashing. Moreover, communications among nodes should be secured against sniffing attacks, especially the RFID systems [69]. Encryption and access control services are usually used to protect the communication against such attacks, which will be explained in securing the information layer in details. Furthermore, to prevent the detection of RFID tags, there are a number of solutions in which an RFID reader transmits pseudo-noise. This noise is balanced by the RFID tags, which hinder the detection by malicious readers [70]. Physical security of IoT devices is currently at of high importance. Protecting the hardware-level of IoT systems is a parallel issue, which is under investigation and research in itself such as in [71]. Additionally, access restrictions on such devices and securing the information they contain, must be ensured. Discussions on the current and possible solutions for securing the information and preserving privacy related data in the information layer are detailed in Section V.

V. Security Services

A good number of proposals have been presented in the literature on secure systems. Some of these proposals can be studied to see whether they can be implemented in the IoT scenarios to face the IoT specific security challenges. Selected proposals are therefore briefed using security methodologies classification with respect to the targeted security service in Table IV. A brief classification of the security services that will

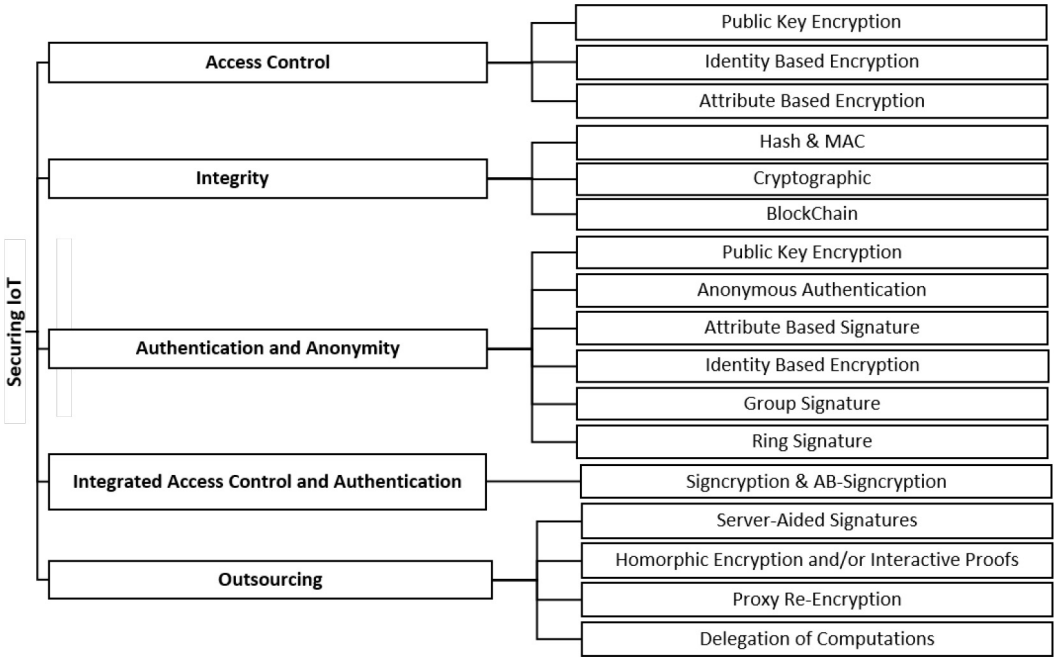

Fig. 5. Classification of security services and the current methodologies.

be covered in this survey and the methodologies of each security service is illustrated in Fig. 5, followed by the discussion of outsourcing techniques of such security services.

A. Access Control

Any access control solution should manage who can do what on data. The system provides permissions and verifies the authorization of a user before accessing data. For IoT systems, access control solutions should take into consideration the special requirements needed by IoT devices, e.g., delegation support due to limited computational power of sensors and devices.

Credential Based Access Control (CBAC) techniques use users' credentials to access the requested data. Public key cryptosystems (PKC) use pairs of keys, i.e., a public key and a private key that belong to a certain owner. PKC can be used to accomplish two functions, namely *authentication* and *confidentiality*. Identity-based Encryption (IBE) is a type of PKC which was firstly proposed in [72]. In IBE, the user's public key can be a user's email address, or any string that particularly identifies the user. A number of identity-based encryption schemes [73], [74], [75], [76] and their variants were introduced and studied. In [77], an identity based encryption for lightweight devices was introduced, by eliminating the use of multiplicative group operations for encryption to reduce computations. Most of the IBE schemes are used for one-to-one encryption or at least need to know all the recipients' public keys, thus, not useful for large scale data sharing.

Attribute Based Encryption (ABE) was introduced in [78] to provide flexible, concrete authorization solutions. All users keep their authorization attributes and private keys. The data owner can encrypt data according to certain access policy. Anyone that has an attribute set that fulfills the access policy can retrieve the data.

There are two variants of ABE as illustrated in Fig. 6: Ciphertext-Policy ABE (CP-ABE), where ciphertexts are encrypted with access policies and keys include user's attributes [79], and Key-Policy ABE (KP-ABE) where keys are associated with access policies and ciphertexts are associated with sets of attributes as defined in [79]. The choice on which ABE variant should be used relies on specific applications. For instance, CP-ABE allows the data encryptor to decide who can access the data and choose an access policy, thus it is more suited for access control applications as compared to the KP-ABE schemes [147].

Many variants of ABE were proposed later. ABE with constant-size ciphertext was proposed in [85], [91], [92], which produce less communication overhead. To limit the credibility of attribute authority, ABE that supports multiple authorities was proposed, such as in [87], [88]. To enhance or reduce ABE computations, on-line/off-line ABE was introduced [86]. The authors of [82], [90] and [89] proposed solutions for efficient ABE revocation and leakage-resilient ABE, respectively. ABE is required for rigid control on private data, such as personal health records (PHR). Narayan *et al.* [81] proposed an attribute-based solution for PHR systems, which encrypted the patient's health records using CP-ABE that allows revocation instantly. However, the proposed solution allowed not only the patient's specific doctor, but also practitioners to access the patient's medical record, without hiding the patient's identity.

An access policy needs to be protected as it may include sensitive private information of a user. To prevent revealing the user's attributes, anonymous ABE has been discussed in [41], [99]. In anonymous CP-ABE, the decryptor can not guess the cipher-text access policy (hidden access policy). In

TABLE IV
THE CLASSIFICATION OF IOT SECURITY METHODOLOGIES ACCORDING TO THE TARGETED SECURITY SERVICES

Threat	Security Services	Security Solutions (Methodology)	References
Illegal access	Access Control (Confidentiality)	Identity-based Encryption	[73], [74], [75], [76], [77]
		Attribute-based Encryption	[78], [79], [80], [81], [82], [83], [84], [85], [86], [87], [88], [89], [90], [91], [92]
		Attribute Based Signcryption	[93], [94], [95], [96], [57], [97], [98]
Disclosure of the user's identity with illegal access control	Anonymous Access Control	Attribute-based Encryption with Hidden Access policy	[99], [100], [101], [41], [47]
Fabrication or impersonation	Authentication	Public Key Cryptography	[102], [103]
		Identity-based Cryptography	[104], [77]
User privacy breach	Anonymous Authentication	Anonymous Credentials	[105], [106], [107]
		Attribute Based Signature	[108], [109], [110], [111], [112], [113], [114]
		Identity-based Signature	[115], [116]
		Group signature	[117], [118]
		Ring signature and Identity-Based Ring Signatures	[119], [120], [121], [122], [123], [124], [125]
		Signcryption, Identity based Signcryption and Attribute Based Signcryption	[93], [126], [127], [128], [94], [95], [96], [57], [97], [98], [49], [129]
Data corruption, alteration and manipulation	Integrity	Public key Infrastructure (PKI)	[102], [103]
		Hash and HMAC	[130], [131], [132]
		Cryptographic and auditing techniques	[133], [134], [135]
		Attribute Based signature	[108], [109], [110], [111], [112], [113], [114].
		Signcryption, Identity based Signcryption and Attribute Based Signcryption	[93], [94], [95], [96], [57], [97], [98], [49], [129]
		Blockchain	[136], [137] ,[138], [139]
Attack on availability	Trusted Computing /Outsourcing (Scalability AND Resource constrained devices)	Server-aided signature schemes	[140], [141]
		Homomorphic Encryption and Interactive Proofs	[142], [143], [144], [145], [146]
		Constant size cipher text	[91], [85], [147], [92], [148]
		Proxy-Re-Encryption (PRE)	[149], [150], [151],[67], [152], [153], [47]
		Delegation of Computations	[154], [155], [156], [157], [158], [159], [148]

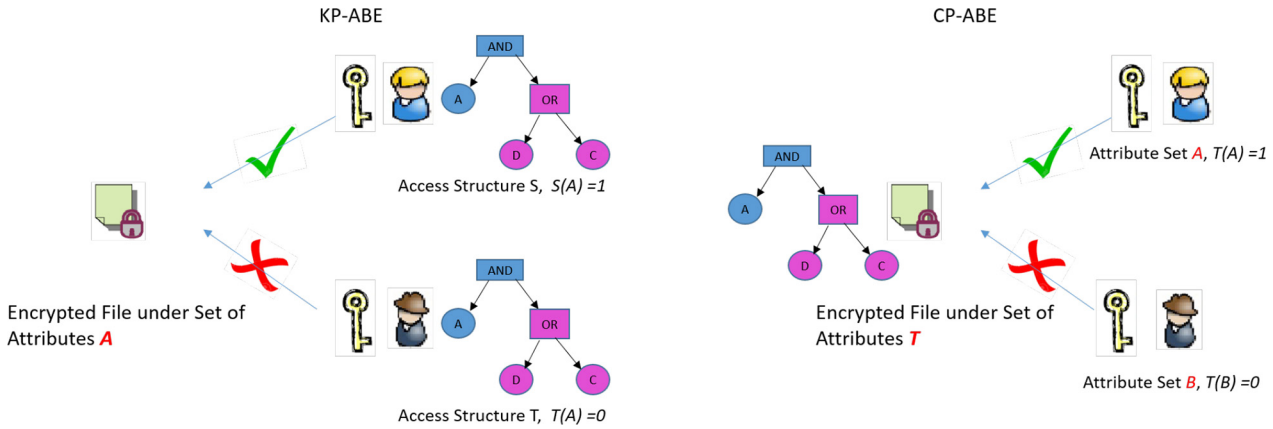

Fig. 6. KP-ABE versus CP-ABE illustration.

a number of anonymous CP-ABE techniques, the user has to perform a number of decryption trials to check if his attributes match the hidden access policy, which will lead to inefficiency in the system. To mitigate such problem, Zhang *et al.* [99] constructed an anonymous CP-ABE scheme with match-then-decrypt, which improved the decryption efficiency. The shortcoming of this proposal is that it does not reinforce access policy updates [41]. The authors of [41] proposed a solution that provides both user access policy update and attribute privacy protection. However, the anonymity in this solution was only for the access policy. Moreover, the attribute and user revocation were not discussed in this paper.

B. Integrity

The authenticity of data is needed, to ensure that the data content is not maliciously altered or deleted. Data integrity solutions should guarantee that a malicious user cannot make any change in the data (even if it is one bit) without being detected by the system as well as the receiver. In the literature, trap-door functions or hash algorithms, such as MD5 [130], SHA1, SHA256 [132] are functions that produce fingerprint of any size input data, while creating a fix sized output. This function reflects any single change in the input data, producing a totally different output fingerprint. Many other forms of integrity checking systems can be used, such as Hash-based Message Authentication Code (HMAC) [131]. HMAC is a message authentication code (MAC) [160], combined with one-way hash function and a secret cryptographic key. This allows the verification of both the authenticity and integrity of a message simultaneously. The strength of HMAC is based on the type of hash function and its output size as well as the size of the key. Usually, integrity checking tools are combined with other cryptographic solutions to provide integrity and other services. For example, PKI and digital signature provide both authenticity of the sender and data integrity. Some techniques that will be discussed later in this survey, provide the integrity service in parallel with its targeted service, such as certificateless attribute based signature (ABS).

Data integrity can be ensured by distributing and replicating data over a set of nodes, which will reduce the possibility of a malicious entity imposing data on any node without being detected. The blockchain technology is a type of data replication disseminated among a huge number of nodes in diversified networks. The blockchain technology has appeared recently in the market, firstly used for the Bitcoin cryptocurrency [161]. Blockchain database provides balanced integrity, while guaranteeing efficiency and stability [136]. There are a number of proposals in the literature [136], [137], [138], [139] that assure data integrity and resilience using blockchain technology.

Blockchain can be used to provide a number of security services besides integrity because blockchain encrypts and hashes data using the conventional cryptographic algorithms [162] and hash functions. However, the use of the conventional cryptographic solutions adds processing overhead on the IoT devices which leads to slow transmissions [162]. Recently, a number of techniques have been proposed that use blockchain to provide security services with enhanced transmission rates. For instance, [163] considered blockchain as a provider of a complete secure IoT network. The authors introduced a blockchain-based framework that provides a number of security key elements such as decentralization, transparency, anonymity and autonomy while considering the quality of service to ensure better transmission rates.

C. Authentication

The ability of the broad spread IoT devices to collect huge amount of information from their surroundings can cause privacy leakage issues and authentication problems, as reported in [164], [165]. Moreover, some studies such as in [166] have shown that the data collection can lead to the identification of individuals.

PKC is usually used to authenticate two entities with the use of identity certificate [102]. It is used to identify and manage users and bind the user's public keys to their identity certificates, in a way that a third party can validate this binding. By binding PKC and trap-door functions (Hash), a digital signature is created, which adds the identity of the sender to any message [103]. This signature can then be verified using the sender's certificate. Identity-based (ID-based) cryptosystem, proposed by [102], eliminates the use of identity certificates and its verification, as the certificate management is time, bandwidth and computation cost consuming. ID-based cryptosystem uses any string that uniquely identifies a user as his/her public key. The string can be a passport number or an email address. Eliminating the certificate validation reduces the communication and computation costs, which makes the whole verification process more efficient. Many more implementations of IBE in the literature were studied. For example, the authors of the work in [104] designed a cloud architecture that uses ID-based cryptography for authenticating users and protecting data privacy.

The interaction of IoT devices and users produce personal information and leave traces that can allow malicious users to trace the users' real identities [166]. For instance, when a user uses a mobile application to adjust his house temperature, the system knows that this command comes from an authorized user. Accordingly, such systems cache the user's information that can reveal his actual identity [166]. Users authenticate themselves to any service before they can use it. The identity provider verifies the user to the requesting provider. This facilitates authentication of identities. However, the involvement of the identity provider in all operations, can give him the ability to trace users' connections to services [166].

To preserve user's identity while achieving the needed authentication, the notion of anonymous authentication has been studied. Anonymous authentication can be achieved using a number of techniques according to the system needs and computations capabilities. Ni *et al.* [167] presented a real-time steering system by utilizing vehicular crowd sensing while preserving users' privacy. In the system, a Trust Authority (TA) issues anonymous credential for each registered vehicle. A vehicle queries the nearby fog or edge, while using a group signature. The information is gathered from the vehicles on roads, where the vehicles send real-time traffic information to the cloud-lets, while preserving their identities by using a signature induced from the anonymous credential. The requesting vehicle can then benefit from the recommendation path and follow the path to reach the target place. More importantly, the TA is able to identify misbehaving or forging data vehicles [168].

As IoT systems communicate with many heterogeneous devices, authentication between devices is needed to ensure they are communicating with the intended party. Authentication usually includes identifying the device or user [169]. However, such identification makes users and devices traceable, hence their privacy is threatened. There are a number of approaches that tackle this problem, such

as Anonymous Credentials [105], [106], Attribute-Based Signatures [108], [109], [110], [111], [112], Identity Based Signatures [115], [116], Group Signatures [117], [118], and Ring Signatures [119], [120], [120], [121], [122], [124], [125].

1) Anonymous Credentials (AC): AC was presented in [105], and then formalized in [106]. These schemes are one of the essential components in privacy-preserving identity management solutions. AC allows users to authenticate themselves to systems while confirming possession of credentials to service providers without being identified. In an anonymous credential system, a credential-issuing entity identifies users by pseudonym and issues a credential to them according to this pseudonym. This pseudonym is related to the actual identity of the user. A user can prove to a service provider that he owns a pseudonym, which he received according to his credentials from an authentic organization [107]. Anonymous credential systems is also capable of providing fine-grained access control [53]. However, it is not efficient to support complex predicates when compared to ABS and ABE [107].

2) Attribute Based Signature (ABS) Scheme: Maji *et al.* [108] formulated ABS and grouped it into KP-ABS (Key Policy ABS) [109] and SP-ABS (Signature Policy ABS) [110]. Liu *et al.* [111] proposed an Anonymous Attribute Based Signature (ABS) for anonymous authentication while outsourcing most of the users' computations to cloud servers, to be able to use this authentication system with low power computational devices. In [112] the authors used ABS as AC, while allowing the users to reveal the required information only to any service provider to ensure unlinkability as well as preserving the anonymity of the user. The authors relied on a non-interactive protocol in their derivations. Guo *et al.* [113] proposed an attribute based signature for electronic health records that ensured the integrity of data within blockchain and disclosed only the related evidence or data as per the attributes used. The authors of [114] proposed a multi-authority ABS that uses only a subset of the attributes to reduce the computation and communication overhead.

3) Fuzzy Identity-Based Signature (IBS): Fuzzy identity-based signature was presented in [115], [116], which enabled users to use part of their attributes to generate signatures. however, IBS does not protect the signer's identity.

4) Group Signature Scheme: Group signature scheme is an approach that allows any group member to anonymously sign data, and the signature will be seen as group signature. It was originally introduced in [117] as a concept. For example, a large company can create a group signature scheme for its employees. An employee from this group can sign a message, and it is acceptable to verify that an employee signed that message, but not who was the specific signer. Then the authors of [118] proposed an attribute-based group signature scheme. It protects the signer's identity, while proving only that the signer's attributes match the policy. The verifier can only identify that the signer is a group member. Attribute-based group signature can provide conditional anonymity, which makes it more useful for attribute-based signature in certain situations. Conditional anonymity is a feature that the group manager can identify the signer of any signature. The identity of the signer can then be revealed, if required.

5) Ring Signature: Ring signatures were firstly proposed by the authors of [120]. It is a type of adjustable signature that protects the signer identity within a group. A user can be a member of a ring spontaneously, in which he can create a group of his choice. The other users in this group might not know that they are a ring group members [107]. Messages can be signed anonymously from any member of this group. By verifying the message, it can be justified to the verifier that a ring member signed the message, without being able to trace the identity of the signer. Ring signatures could be used in applications that need signer anonymity, while not having the complicated group formation stage. A number of different techniques were discussed in [122], [124], [125] since the first proposal and first introduction of ring signature in [119], [120], respectively. The idea of ID-Ring signature was proposed in 2002 [121]. ID-Ring signatures can provide the same features of identity-based crypt-systems, without using the high computational bilinear pairing.

The Ring signatures and ID-ring signatures can provide total anonymity. However, conditional anonymous authentication cannot be achieved as no one can tell who signed from the ring, even in emergencies.

A cloud infrastructure provides solutions that are reliable and ensure data availability at low cost, which is useful for both service providers and consumers. The external storage of a user's data on cloud server owned by third parties, and the ability to access this data from the Internet put data and users privacy under concerns. Accordingly, the security and privacy of user's data have become an active research question recently. To prevent cloud insider attacks, Bleikertz *et al.* [133] introduced a fine-grained privilege levels approach to provide users' privacy and integrity as well as the ability to perform cloud maintenance. Raykova *et al.* [100] proposed a technique that hides private data in policies from the cloud insider attacks. The authors defined an access control system with two sides: the cloud side that has limited access to information, to be used by cloud provider, and the client side, which depends on access control cryptosystems.

D. Integrated Access Control and Authentication

A number of applications require data secrecy while ensuring the authenticity of the origin. For example, e-Health systems as well as Personal Health Record (PHR) share patient's personal health with a number of expected users, such as doctors and insurance providers. The e-Health and PHR service providers usually use cloud for PHR data storage. Storing the health data on a semi-trusted cloud raises security and privacy concerns. The main need of such systems is to guarantee that the health data is available for legitimate authorized users. Health-care fraud or abuse as well as mis-diagnosed patients can happen [54] unintentionally, or intentionally if a malicious unauthorized user accesses the data and modifies the e-Health data before the doctor accesses it. This may lead to an incorrect prescribed treatment for a patient, which could cause threat on the patient's life. To prevent patient's identity, both the

patient's privacy and the authentication of the target receiver should be achieved, during the process of uploading e-Health information to the cloud. Securing the privacy and anonymity of patients while sharing PHR data in cloud computing environments is an evolving issue. Accordingly, fine-grained data access control solutions that ensure confidentiality, authenticity and anonymity of users are essential.

Signcryption provides confidentiality and authenticity simultaneously [93]. It executes both signature and encryption, with less computational overhead compared to Sign-then-Encrypt approaches. Attribute-based signcryption (ABSC) was proposed such as in [95], combining the functionality of ABS and ABE. There are two types of ABSC: *signcryption-policy attribute-based signcryption* (SCP-ABSC) and *key-policy attribute-based signcryption* (KP-ABSC). On the one hand, there are two policies associated with the users' attributes in SCP-ABSC, and a key is tagged with receiver attributes and sender attributes. On the other hand, in KP-ABSC, everything related to policies and attributes are swapped. The authors of [94] described dynamic attribute-based signcryption, that does not need to re-issue users secret keys during the access structure updates. Then, a number of attribute-based signcryption schemes [49], [95], [96] have been proposed in the literature. A number of proposals handled computational limitation of mobile devices [57], [98], [129].

It is noted that the computations and communication overhead of ciphertext policy attribute based signcryption such as in [57], [94] boost linearly with additional attributes. This computation and communication boost has motivated the construction of a ciphertext policy attribute based signcryption scheme with a fixed size and computational cost. For preserving the users' privacy and identities, there is a need to use multi-authority based attribute encryption to limit the capabilities of a single authority, while including a semi or partial ID verification for collision, without exposing the identity of either the sender or the receiver. ABC and AB-signcryption can be used in many applications. But, it is still not widely spread on mobile and IoT applications due to its high computations.

E. Outsourcing of Computations

Cloud computing can provide users with powerful computational ability and resources. Users with mobile devices or limited power devices can outsource their intensive computations or store their data on the cloud. Cloud brings security challenges when users delegate private operations on it, such as signature generation. The cloud can sign user's messages, without the knowledge of the user. To handle the semi-trusted or untrusted cloud or service provider problem, a server-aided signature scheme approach was proposed in [140]. The techniques still need expensive computations, which cannot be afforded by IoT systems. Another methodology centers around outsourcing with methods presented [142], [143], [144], [145], [146] that use homomorphic encryption or interactive proof systems. However, such methods were proved by Gentry and Halevi [145] that they are not efficient enough for systems with limited computational power and resources, such as IoT devices.

In IoT, many devices are resource constrained. Accordingly, a number of security solutions targeting limited computational power systems started to emerge, such as the one presented in [153]. The authors introduced a solution that considers limited capability devices, and delegates the CP-ABE computations to powerful computational devices. The produced ciphered text is then either re-sent to the sending device or forwarded to cloud service provider for storage or sharing [170]. In another work, the authors of [147] proposed a CP-ABE technique that generates constant size ciphertexts and private keys, which is more feasible for IoT devices.

Proxy Re-Encryption (PRE) was introduced in [149] and formally studied in [150]. PRE allows a proxy which holds re-encryption key created by the data owner, to re-encrypt ciphertexts (that are already encrypted with Alice's public key), to be encrypted with Bob's public key instead. In a way that only Bob's private key can decrypt the newly re-encrypted chiphertext. PRE and attribute-based encryption (ABE) can be used for securing data access stored on the cloud. PRE is an ultimate solution specially for cloud storage since we cannot fully trust CSP, while the useful property is the ability to do the ciphertext conversion without revealing the corresponding plaintexts. Integrating ABC and PRE can produce a flexible and practical fine-grained access control data sharing solution. Ciphertext-policy ABPRE technique was first introduced in [151]. In this technique, a proxy is able to convert a ciphered message ciphered under an access policy to a ciphered message ciphered under another access policy. Liang *et al.* [152] constructed the first CP-ABPRE that has only one trusted authority for generating keys. Thus, it is not feasible to be used in scalable big data systems. Massive data systems should be supported by multiple authorities to allow scalability and separate authorities roles. In 2017, the authors of [47] proposed a CP-ABPRE with attribute privacy protection, by hiding the access policy, to protect a user's identity.

IoT devices are usually light weight devices with very limited hardware resources. Unfortunately, the computational cost of cryptographic algorithms (e.g., pairing and exponentiations) are costly. IoT devices cannot afford such cost. Accordingly, it would be desirable that such devices can outsource or delegate part of the extensive computations to a gateway or cloud as illustrated in Fig. 7.

In the literature, there are a number of conducted work that target delegating the computations of encryption, decryption and/or revocation of ABC, as shown in Fig. 8. Green *et al.* [154] described a CP-ABE solution that outsources the decryption process. In [171], the authors described a technique that delegates both the encryption and decryption of CP-ABE to the cloud. Their proposed encryption process has two access structures (T1, T2) connected by an AND root node. This solution requires three exponentiations on the user side, which still needs plenty of resources. The authors of [156] presented a CP-ABE technique that outsources both the encryption and decryption extensive computations. During key generation, a user's secret key and a transformation key are created. This transformation key should be given to a

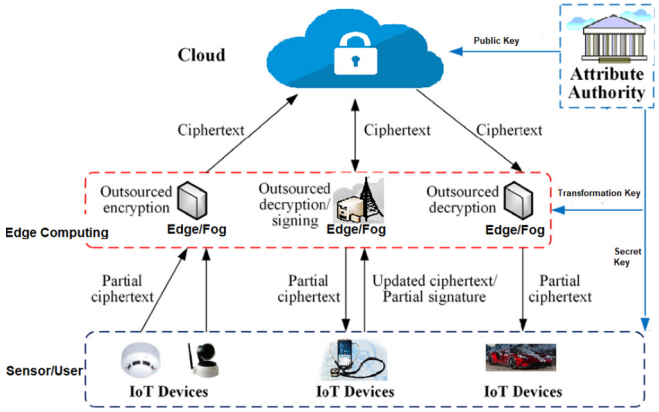

Fig. 7. Delegating partial encryption and decryption to the edge or the cloud.

proxy or cloud service provider. The proxy uses the transformation key for partial decryption of the ciphertext to ElGamal ciphertext [172], only when the user's attributes match the policy. Then the resource-constrained device can decrypt the generated ElGamal ciphertext with limited computations. An efficient outsourced ABSC (OABSC) was presented in [157], which borrows computational resources from a third party cloud to partial decrypt ciphertexts. In this process, users need to select and record their secret keys, which will allow them to do the final decryption of ciphertext. Usually, the ciphertext is stored on cloud. When users request to access the data, they need to get verified by presenting their attributes. Then a transformation key created from the user's key should be sent to the cloud system to partial decrypt data. This will then return a partial decrypted ciphertext. Then the receiver can verify the correctness of the transformed ciphertext, before decrypting to its original form using their kept secret key.

Yang *et al.* [173] proposed a multi-cloud based outsourcing for decryption, while preserving the receiver's attributes from being disclosed. In [159], OEABE outsourcing scheme was introduced, that outsources ABE ciphertext-policy encryption. This proposed solution targets the delegation of the most expensive computations in the ABE encryption to a cloud, while maintaining the confidentiality of data against both external and internal attackers. The encryption process requires only one exponentiation on resource-constrained devices. However, the solution does not target revocation of users and attributes, or the delegation of attributes management (issuance or revocation) to cloud or proxy. Zhang *et al.* [148] proposed an energy efficient KP-ABE decryption outsourcing that takes into consideration of the cipher-text size, making sure that the cipher-text size is constant to reduce the communication overhead.

Regarding attribute revocation, a number of CP-ABE mechanisms that manage attribute revocation have been presented. Yu *et al.* [67] used a semi-trusted proxy for instant attribute revocation. In their proposal, the proxy transforms the ciphertext, as well as refreshes all the authorized users secret keys. Yong *et al.* [155] described a CP-ABE technique that outsources both decryption and attribute revocation. This technique uses attributes versioning to accomplish attributes revocation. Liu *et al.* [158] presented a technique to outsource decryption as well as attribute revocation. Their technique concentrates on ciphertext updates as well as updating user's keys, reflecting the revoked attributes.

There are a number of solutions that tackle the outsourcing of either encryption, decryption or attribute management (i.e., revocation) to the cloud. However, to the best of our knowledge, no technique nor framework in the literature integrates all the needed services for IoT devices. IoT frameworks need to provide conditional anonymous authentication, fine grained access control with receivers and sender privacy and data integrity. Such techniques need to outsource the encryption, decryption, revocation management and access policy management to a gateway or the cloud.

VI. Open Research Issues

In recent years, although active research efforts have been dedicated on securing IoT, there are still a number of open issues that need to be tackled. This section will describe some of the major open research questions in securing and privacy preservation of IoT systems.

Comprehensive Security: Several promising opportunities [3], [22], [26], [48], [92], [114] have emerged with the evolution of IoT and cloud computing, facing IoT security challenges [2], [17], [29], [31]. However, a complete solution has not yet been implemented, as most of the available solutions target on only certain security requirements. To the best of our knowledge, there is still no methodology that develops security attack free, conditional anonymous authentication and fine-grained access control protocol to be used by the various IoT use case scenarios. This framework should also outsource part of the heavy computations in either uploading or downloading data, to a computational powerful device or the cloud. Existing techniques can be integrated to accomplish an all-inclusive security solution. However, the integration is not simple, due to the possibility of techniques interference, usability and efficiency problems. We believe that comprehensive security solutions are needed for usable and efficient IoT data sharing.

Non-Repudiation: In any system involving with user interactions, non-repudiation is needed to prevent the data owner (sender) the denial of previous data upload. Most of the work in IoT security, however, neglected the importance of non-repudiation. IoT systems concentrate more on privacy of users and devices. However, non-repudiation can still be provided, while preserving user privacy. This can be achieved by conditional anonymity, as the sender still needs to be anonymous, and for security or emergency reasons, certain authorities need to find out the real identity of a user. Conditional anonymity can be achieved by a number of techniques such as group signatures. However, providing conditional anonymity feature on limited-resourced IoT devices is a challenging task, and extensive research is needed in this direction.

Scalability: IoT devices interact in different patterns with different entities. The number of users and devices communicating together within an IoT ecosystem is growing widely with the growth in technologies. Accordingly, the efficiency and scalability of systems need to be ensured by not only

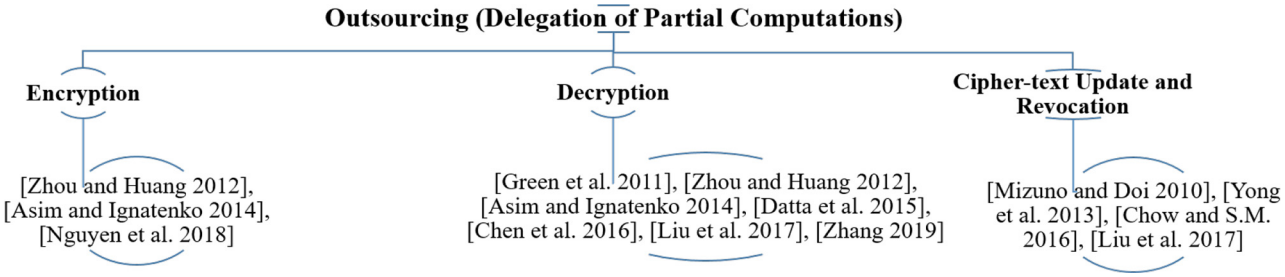

Fig. 8. Classification of research in outsourcing according to what to be outsourced.

storing secured data on the cloud, but also by delegating the encryption and decryption in a secured manner to a cloudlet or cloud. Outsourcing the revocation management and access list management to cloud (proxy) are also needed, to reduce computational load of both sender and receiver in different perspectives. Additionally, the size of the encrypted data (sent or received) should be minimized to reduce communication overhead, which can be achieved by using constant size ABE encryption techniques.

Revocation: As the user/device may have limited subscription periods or the device has been hacked/attacked or stolen, the communicating party needs to find out whether a user/device is revoked. The revoked entity authentication and access to data should be disabled. Efficient revocation is very challenging and it is especially important for a large scale network. Scalable key management revocation in IoT systems is an important aspects. It should ensure both backward and forward secrecy. Newly joined users to a group, should not be able to interpret data encrypted, before their joining time. Revoked users that previously had a key, should not be able to interpret future encrypted data using their previous revoked keys. Finding the proper and efficient way to revoke attributes and/or users is still an issue. The existing schemes are not flexible nor efficient enough. For instance, some existing techniques are based on users to interact online with the authority, such as in [80]. Some techniques do not allow revocation instantly, such as in [67]. More research is therefore needed to enhance the user and attribute revocation and management systems. Outsourcing the management to a semi-trusted cloud can add flexibility and scalability of infrastructure management systems (issuing and revocation of keys and attributes).

Interoperability: Interoperability in IoT is needed, knowing that there are some legacy proprietary hardware and software deployed systems. Governmental efforts to create standards for IoT interoperability and backward compatibility should be taken into consideration during all phases of IoT systems implementation and fabrication. Moreover, governmental and non-governmental entities should provide a way to set universal privacy policies and find a way to impose them. This is needed to allow the interoperability of different systems, while maintaining user's privacy.

Trust Management: Trust management is needed to establish trust across different IoT systems and domains. In such a large scale IoT network, it is a big challenge to build trust between different domains and a large number of limited resources devices [174]. The number of IoT consumers can be huge and dynamic. Accordingly, the trust management system must be adaptive and scalable. Moreover, the accuracy of trust systems is crucial. To improve the trust result accuracy, different techniques can be integrated such as reputation and recommendation techniques. However, most of the available trust management systems cannot be easily integrated with each other [175], [176]. Accordingly, more research is needed for providing techniques to efficiently integrate various trust feedbacks. This should be done while protecting user's privacy. Furthermore, the response time of trust management systems is of great importance. The longer the response time, the lower the number of inquiries that the system can handle. Systems with minimal response time are urgently needed for IoT systems.

Latency Constraint: It is important to note that not only the information in IoT should be stored and processed in a timely manner, but also services should be secured with minimal added latency. It is not recommended to rely on the cloud for applications that require fast processing and minimal delays [40]. Edge computing and federated-machine learning [177] are some of the promising ways that can ensure the rapid delivery of IoT cloud-based services as well as scalability and privacy-policy enforcement. More research efforts are needed in finding efficient ways to use edge computing with IoT and the cloud to combat the security challenges in IoT systems.

VII. Conclusion

This paper presents a better understanding of security threats and security requirements in the Internet of Things (IoT), as well as approaches to address different threats and security challenges. IoT systems should be constructed with the due consideration of security, privacy, and trust. Security requirements should be addressed in all of the architecture layers of IoT systems. Furthermore, constraints introduced by the IoT such as big data, distributed and low powered devices, should be taken into consideration during the solutions design phase. In this paper, IoT security threats and possible counter measures for each threat are investigated. Challenges to IoT devices and the exchange of data between IoT systems, edge device and the cloud are evaluated. In particular, we present a detailed survey on security mechanisms that address different security services and challenges in IoT, namely confidentiality, access control, authentication, privacy, integrity and resource

constrained IoT devices. Finally, we identify the gap in IoT security research and development, as well the future research efforts needed. We hope these research questions will stimulate further research in this important area, thereby realizing an Internet of Secure Things eventually.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable feedback on this work.

REFERENCES

[1] Q. Z. Sheng, Y. Qin, L. Yao, and B. Benatallah, Eds., *Managing the Web of Things: Linking the Real World to the Web*. Cambridge, MA, USA: Morgan Kaufmann, 2017.

[2] M. Sain, Y. J. Kang, and H. J. Lee, "Survey on security in Internet of Things: State of the art and challenges," in *Proc. Int. Conf. Adv. Commun. Technol. (ICACT)*, 2017, pp. 699–704.

[3] C. T. Li, T. Y. Wu, C. L. P. Chen, C. C. Lee, and C. M. Chen, "An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system," *Sensors*, vol. 17, no. 7, pp. 1–18, 2017.

[4] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, 2010.

[5] E. Bertino, K.-K. R. Choo, D. Georgakopolous, and S. Nepal, "Internet of Things (IoT): Smart and secure service delivery," *ACM Trans. Internet Technol.*, vol. 16, no. 4, pp. 1–7, 2016.

[6] K. A. Mckay, L. B. Meltem, S. Turan, and N. Mouha, "Report on lightweight cryptography," Nat. Inst. Stand. Technol., Gaithersburg, MA, USA, Rep. NISTIR 8114, 2017. [Online]. Available: https://doi.org/10.6028/NIST.IR.8114

[7] Texas Instruments. *COP8CCE9 8-Bit CMOS Flash Microcontroller With 8k Memory, Virtual EEPROM, 10-Bit A/D and 4.17V to 4.5V Brown*. Accessed: May 11, 2019. [Online]. Available: http://www.ti.com/product/COP8CCE9

[8] Microchip. *New/Popular 8-Bit Microcontrollers Products—Microchip Technology Inc*. Accessed: May 12, 2019. [Online]. Available: https://www.microchip.com/ParamChartSearch/chart.aspx?branchID=1012

[9] M.-J. O. Saarinen and D. W. Engels, "A do-it-all-cipher for RFID: Design requirements (extended abstract)," Cryptol. ePrint Archive, Rep. 2012/317, 2012.

[10] Arm MBED. *MBED*. Accessed: May 11, 2019. [Online]. Available: https://www.mbed.com/en/

[11] Think Incredible. (2019). *Brillo, Internet of Things OS—Intraway*. [Online]. Available: https://thinkincredible.intraway.com/blog-post/brillo-internet-of-things-os/

[12] Canonical. *Ubuntu Core*. Accessed: May 15, 2019. [Online]. Available: https://ubuntu.com/core

[13] H. Will, K. Schleiser, and J. H. Schiller, "A real-time kernel for wireless sensor networks employed in rescue scenarios," in *Proc. IEEE Conf. Local Comput. Netw.*, 2009, pp. 834–841.

[14] Contiki. *Contiki-NG*. Accessed: Aug. 15, 2019. [Online]. Available: https://www.contiki-ng.org

[15] Kaspersky Labs. (2017). *Kaspersky Embedded Security Solutions Secure OS for the Internet of Things, Technical Report*. [Online]. Available: http://www.securelist.com/

[16] J. McBride, B. Arief, and J. Hernandez-Castro, "Security analysis of Contiki IoT operating system," in *Proc. Int. Conf. Embedded Wireless Syst. Netw.*, 2018, pp. 278–283.

[17] N. Ii, Y. M. Tech, and V. Pai, "Survey on IoT security issues and security protocols," *Int. J. Comput. Appl.*, vol. 180, pp. 975–987, May 2018.

[18] D. Q. F. Maggi. (2018). *When Machines Can't Talk: Security and Privacy Issues of Machine-to-Machine Data Protocols*. [Online]. Available: https://www.blackhat.com/eu-18/briefings/schedule/index.html

[19] L. Lundgren. (2017). *Taking Over the World Through MQTT-AfterMath*. [Online]. Available: https://www.blackhat.com/us-17/briefings.html

[20] S. Deshmukh and S. S. Sonavane, "Security protocols for Internet of Things: A survey," in *Proc. Int. Conf. Nextgen Electron. Technol. (ICNETS2)*, 2017, pp. 71–74.

[21] L. Cashdollar, *As We Warned, Iran Strikes Back With New Silex Malware Bricking IoT Devices*. Accessed: Jul. 2, 2019. [Online]. Available: https://blog.tmcnet.com/blog/rich-tehrani/security/as-we-warned-iran-strikes–back-with-new-silex-malware-bricking-iot-devices.html

[22] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, "Proposed embedded security framework for Internet of Things (IoT)," in *Proc. Int. Conf. Wireless Commun. Veh. Technol. Inf. Theory Aerosp. Electron. Syst. Wireless (VITAE)*, 2011, pp. 1–5.

[23] S. P. Skorobogatov, "Semi-invasive attacks—A new approach to hardware security analysis," Comput. Lab., Univ. Cambridge, Cambridge, U.K., Rep. NISTIR 8114, 2005. [Online]. Available: https://doi.org/10.6028/NIST.IR.8114

[24] G. Tuna, D. G. Kogias, V. C. Gungor, and C. Gezer, "A survey on information security threats and solutions for machine to machine (M2M) communications," *J. Parallel Distrib. Comput.*, vol. 109, pp. 142–154, Nov. 2017.

[25] A. H. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, "IoT middleware: A survey on issues and enabling technologies," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 1–20, Feb. 2017.

[26] J. L. Hernández-Ramos, M. V. Moreno, J. B. Bernabé, D. G. Carrillo, and A. F. Skarmeta, "SAFIR: Secure access framework for IoT-enabled services on smart buildings," *J. Comput. Syst. Sci.*, vol. 81, no. 8, pp. 1452–1463, 2015.

[27] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[28] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the Internet of Things: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 414–454, 1st Quart., 2014.

[29] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015.

[30] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in Internet of Things," *Digit. Commun. Netw.*, vol. 4, no. 2, pp. 118–137, 2017.

[31] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26–33, Jan. 2017.

[32] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.

[33] D. Gil, A. Ferrández, H. Mora-Mora, and J. Peral, "Internet of Things: A review of surveys based on context aware intelligent services," *Sensors*, vol. 16, no. 7, p. 1069, 2016.

[34] M. Noor and W. H. Hassan, "Current research on Internet of Things security: A survey," *Comput. Netw.*, vol. 148, pp. 283–294, Jan. 2019.

[35] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Security Appl.*, vol. 38, pp. 8–27, Feb. 2018.

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

[37] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973–993, 2014.

[38] X. Huang *et al.*, "Cost-effective authentic and anonymous data sharing with forward security," *IEEE Trans. Comput.*, vol. 64, no. 4, pp. 971–983, Apr. 2015.

[39] R. M. Zolanvari, "IoT security: A survey," in *Recent Advances in Networking (Data Center Virtualization, SDN, Big Data, Internet of Things)*. New York, NY, USA: Nova Sci., 2015, pp. 1–15.

[40] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, Jan. 2017.

[41] Y. Zhang, J. Li, X. Chen, and H. Li, "Anonymous attribute-based proxy re-encryption for access control in cloud computing," *Networks*, vol. 9, no. 14, pp. 2397–2411, 2016.

[42] C. Clastres, "Smart grids: Another step towards competition, energy security and climate change objectives," *Energy Policy*, vol. 39, no. 9, pp. 5399–5408, 2011.

[43] S. Ijaz, M. Ali, A. Khan, and M. Ahmed, "Smart cities: A survey on security concerns," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 2, pp. 612–625, 2016.

[44] A. Martinez-Balleste, P. Perez-martinez, and A. Solanas, "The pursuit of citizens' privacy: A privacy-aware smart city is possible," *IEEE Commun. Mag.*, vol. 51, no. 6, pp. 136–141, Jun. 2013.

[45] J. Wang, L. C. K. Hui, S. M. B. Yiu, and X. Cui, "A survey on the cyber attacks against non-linear state estimation in smart grids," in *Proc. Inf. Security Privacy ACISP*, vol. 1, 2016, pp. 40–56.

[46] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2010, pp. 238–243.

[47] H. Yin and L. Zhang, "Security analysis and improvement of an anonymous attribute-based proxy re-encryption," in *Proc. Int. Conf. Security Privacy Anonymity Comput. Commun. Storage (SpaCCS)*, 2017, pp. 344–352.

[48] T. Dimitriou and G. O. Karame, "Enabling anonymous authorization and rewarding in the smart grid," *IEEE Trans. Depend. Secure Comput.*, vol. 14, no. 5, pp. 565–572, Sep./Oct. 2017.

[49] E. Ahene, J. Dai, and H. Feng, "A certificateless signcryption with proxy re-encryption for practical access control in cloud-based reliable smart grid," *Telecommun. Syst.*, vol. 70, pp. 491–510, Nov. 2018.

[50] N. Saxena, B. J. Choi, and R. Lu, "Authentication and authorization scheme for various user roles and devices in smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 907–921, May 2016.

[51] S. Sidhu and B. J. Mohd, "Hardware security in IoT devices with emphasis on hardware Trojans," *J. Sensor Actuator Netw.*, vol. 8, no. 3, p. 42, 2019.

[52] Healthcare Information and Management Systems Society Organization. (2017). *HIMSS Cybersecurity Survey*. [Online]. Available: https://www.himss.org/himss-healthcare-cybersecurity-environmental-scan-reports

[53] S. E. Coull, M. Green, and S. Hohenberger, "Access controls for oblivious and anonymous systems," *ACM Trans. Inf. Syst. Security*, vol. 14, no. 1, pp. 1–28, 2011.

[54] D. Arrowood *et al.*, "Integrity of the healthcare record: Best practices for EHR documentation (2013 update)," *J. Amer. Health Inf. Manag. Assoc.*, vol. 84, no. 8, pp. 58–62, 2013.

[55] J. Zhou, X. Lin, X. Dong, and Z. Cao, "PSMPA: Patient self-controllable and multi-level privacy-preserving cooperative authentication in distributed m-healthcare cloud computing system," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 6, pp. 1693–1703, Jun. 2015.

[56] M. Barua, X. Liang, R. Lu, and X. Shen, "PEACE: An efficient and secure patient-centric access control scheme for eHealth care system," in *Proc. Int. Workshop Security Comput. Netw. Commun. (NeTCoM)*, vol. 1, 2011, pp. 987–992.

[57] J. Liu and X. Huang, "Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute-based signcryption," *Future Gener. Comput. Syst.*, vol. 52, pp. 67–76, Nov. 2015.

[58] S. Djahel, R. Doolan, G.-M. Muntean, and J. Murphy, "A communications-oriented perspective on traffic management systems for smart cities: Challenges and innovative approaches," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 125–151, 1st Quart., 2015.

[59] A. Mahmood, W. E. Zhang, and Q. Z. Sheng, "Software-defined heterogeneous vehicular networking: The architectural design and open challenges," *Future Internet*, vol. 11, no. 3, p. 70, 2019.

[60] M. Wang, D. Liu, L. Zhu, Y. Xu, and F. Wang, "LESPP: Lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication," *Computing*, vol. 98, pp. 685–708, Jul. 2016.

[61] S. O. Ogundoyin, "An autonomous lightweight conditional privacy-preserving authentication scheme with provable security for vehicular ad-hoc networks," *Int. J. Comput. Appl.*, vol. 42, no. 2, pp. 196–211, 2018.

[62] N. Kumar, R. Iqbal, S. Misra, and J. J. Rodrigues, "An intelligent approach for building a secure decentralized public key infrastructure in VANET," *J. Comput. Syst. Sci.*, vol. 81, no. 6, pp. 1042–1058, 2015.

[63] J. Li, H. Lu, and M. Guizani, "ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 4, pp. 938–948, Apr. 2015.

[64] J. Han, W. Susilo, Y. Mu, J. Zhou, and M. H. Au, "PPDCP-ABE: Privacy-preserving decentralized cipher-policy attribute-based encryption," in *Proc. Eur. Symp. Res. Comput. (ESORICS)*, 2014, pp. 73–90.

[65] G. Ohtake, R. Safavi-Naini, and L. F. Zhang, "Outsourcing scheme of ABE encryption secure against malicious adversary," in *Proc. Int. Conf. Inf. Syst. Security Privacy (ICISSP)*, 2017, pp. 71–82.

[66] J. L. Hernández-Ramos, J. B. Bernabe, M. V. Moreno, and A. F. Skarmeta, "Preserving smart objects privacy through anonymous and accountable access control for a M2M-enabled Internet of Things," *Sensors*, vol. 15, no. 7, pp. 15611–15639, 2015.

[67] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, 2010, pp. 1–9.

[68] J. Noorman *et al.*, "Sancus 2.0: A low-cost security architecture for IoT devices," *ACM Trans. Privacy Security*, vol. 20, no. 3, pp. 1–33, 2017.

[69] Q. Z. Sheng, X. Li, and S. Zeadally, "Enabling next-generation RFID applications: Solutions and challenges," *IEEE Comput.*, vol. 41, no. 9, pp. 21–28, Sep. 2008.

[70] O. Savry, F. Pebay-Peyroula, F. Dehmas, G. Robert, and J. Reverdy, "RFID noisy reader how to prevent from eavesdropping on the communication?" in *Proc. Cryptograph. Hardw. Embedded Syst. (CHES)*, 2007, pp. 334–345.

[71] W. Diehl, A. Abdulgadir, J.-P. Kaps, and K. Gaj, "Comparing the cost of protecting selected lightweight block ciphers against differential power analysis in low-cost FPGAs," in *Proc. Int. Conf. Field Program. Technol. (ICFPT)*, 2017, pp. 128–135.

[72] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proc. Annu. Int. Cryptol. Conf. (CRYPTO)*, 2001, pp. 213–229.

[73] B. Waters, "Efficient identity-based encryption without random oracles," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, vol. 3494, 2005, pp. 114–127.

[74] C. Gentry, "Practical identity-based encryption without random oracles," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, 2006, pp. 445–464.

[75] A. Lewko and B. Waters, "New techniques for dual system encryption and fully secure HIBE with short ciphertexts," in *Proc. Theory Cryptography Conf. (TCC)*, 2010, pp. 455–479.

[76] K. He, J. Weng, J.-N. Liu, J. K. Liu, W. Liu, and R. H. Deng, "Anonymous identity-based broadcast encryption with chosen-ciphertext security," in *Proc. Int. Symp. Inf. Comput. Commun. Security (ASIA CCS)*, 2016, pp. 247–255.

[77] F. Guo, Y. Mu, W. Susilo, H. Hsing, D. S. Wong, and V. Varadharajan, "Optimized identity-based encryption from bilinear pairing for lightweight devices," *IEEE Trans. Depend. Secure Comput.*, vol. 14, no. 2, pp. 211–220, Mar./Apr. 2017.

[78] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, 2005, pp. 457–473.

[79] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM Conf. Comput. Commun. Security (CCS)*, 2006, p. 89.

[80] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Security Privacy (SP)*, 2007, pp. 321–334.

[81] S. Narayan, M. Gagné, and R. Safavi-Naini, "Privacy preserving EHR system using attribute-based infrastructure," in *Proc. ACM Workshop Cloud Comput. Security Workshop (CCSW)*, 2010, p. 47.

[82] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 7, pp. 1214–1221, Jul. 2011.

[83] S. Garg, C. Gentry, S. Halevi, A. Sahai, and B. Waters, "Attribute-based encryption for circuits from multilinear maps," in *Proc. Annu. Cryptol. Conf. (CRYPTO)*, vol. 8043, 2013, pp. 479–499.

[84] Y. Zhang, X. Chen, J. Li, H. Li, and F. Li, "Attribute-based data sharing with flexible and direct revocation in cloud computing," *KSII Trans. Internet Inf. Syst.*, vol. 8, no. 11, pp. 4028–4049, 2014.

[85] Y. B. Zhang, D. Zheng, X. Chen, J. Li, and H. Li, "Computationally efficient ciphertext-policy attribute-based encryption with constant-size ciphertexts," in *Proc. Int. Conf. Provable Security (ProvSec)*, 2014, pp. 259–273.

[86] S. Hohenberger and B. Waters, "Online/offline attribute-based encryption," in *Proc. Int. Workshop Public Key Cryptography (PKC)*, 2014, pp. 293–310.

[87] Y. Rahulamathavan, S. Veluru, J. Han, F. Li, M. Rajarajan, and R. Lu, "User collusion avoidance scheme for privacy-preserving decentralized key-policy attribute-based encryption," *IEEE Trans. Comput.*, vol. 65, no. 9, pp. 2939–2946, Sep. 2016.

[88] Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer, O. Farràs, and J. A. Manjón, "Contributory broadcast encryption with efficient encryption and short ciphertexts," *IEEE Trans. Comput.*, vol. 65, no. 2, pp. 466–479, Feb. 2016.

[89] Z. Yu, M. H. Au, Q. Xu, R. Yang, and J. Han, "Leakage-resilient functional encryption via pair encodings," in *Proc. Aust. Conf. Inf. Security Privacy*, 2016, pp. 443–460.

[90] K. Yamada, N. Attrapadung, K. Emura, G. Hanaoka, and K. Tanaka, "Generic constructions for fully secure revocable attribute-based encryption," in *Proc. Eur. Symp. Res. Comput. (ESORICS)*, 2017, pp. 532–551.

[91] S. Belguith, N. Kaaniche, M. Laurent, A. Jemai, and R. Attia, "Constant-size threshold attribute based signcryption for cloud applications," in *Proc. Int. Conf. Security Cryptography (SECRYPT)*, 2017, pp. 212–225.

[92] Z. Zhang, C. Li, B. B. Gupta, and D. Niu, "Efficient compressed ciphertext length scheme using multi-authority CP-ABE for hierarchical attributes," *IEEE Access*, vol. 6, pp. 38273–38284, 2018.

[93] Y. Zheng, "Digital signcryption or how to achieve cost(signature & encryption) cost(signature) + cost(encryption)," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. (CRYPTO)*, 1997, pp. 165–179.

[94] K. Emura, A. Miyaji, and M. S. Rahman, "Dynamic attribute-based signcryption without random oracles," *Int. J. Appl. Cryptography*, vol. 2, no. 3, p. 199, 2012.

[95] C. Chen, J. Chen, H. W. Lim, Z. Zhang, and D. Feng, "Combined public-key schemes: The case of ABE and ABS," in *Proc. Int. Conf. Provable Security*, 2012, pp. 53–69.

[96] T. Pandit, S. K. Pandey, and R. Barua, "Attribute-based signcryption: Signer privacy, strong unforgeability and IND-CCA2 security in adaptive-predicates attack," in *Proc. Int. Conf. Provable Security (ProvSec)*, vol. 8782, 2014, pp. 274–290.

[97] Y. S. Rao and R. Dutta, "Efficient attribute-based signature and signcryption realizing expressive access structures," *Int. J. Inf. Security*, vol. 15, no. 1, pp. 81–109, 2016.

[98] Y. S. Rao, "Attribute-based online/offline signcryption scheme," *Int. J. Commun. Syst.*, vol. 30, no. 16, pp. 1–20, 2017.

[99] Y. Zhang, X. Chen, J. Li, D. S. Wong, and H. Li, "Anonymous attribute-based encryption supporting efficient decryption test," in *Proc. ACM SIGSAC Symp. Inf. Comput. Commun. Security (ASIA CCS)*, 2013, p. 511.

[100] M. Raykova, H. Zhao, and S. M. Bellovin, "Privacy enhanced access control for outsourced data sharing," in *Proc. Financial Cryptography Data Security*, 2012, pp. 223–238.

[101] T. Jung, X.-Y. Li, Z. Wan, and M. Wan, "Privacy preserving cloud data access with multi-authorities," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, 2013, pp. 2625–2633.

[102] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, 1985, pp. 47–53.

[103] G. S. G. N. Anjaneyulu, P. V. Reddy, and U. M. Reddy, "Secured digital signature scheme using polynomials over non-commutative division semirings," *Int. J. Comput. Sci. Netw. Security*, vol. 8, no. 8, p. 278, 2008.

[104] H. Li, Y. Dai, and B. Yang, "Identity-based cryptography for cloud security," in *Proc. IACR Cryptol. ePrint Archive*, vol. 169, 2011, pp. 1–9.

[105] D. Chaum, "Blind signatures for untraceable payments," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, 1982, pp. 199–203.

[106] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, 2001, pp. 93–118.

[107] J. Li, M. H. Au, W. Susilo, D. Xie, and K. Ren, "Attribute-based signature and its applications," in *Proc. ACM Symp. Inf. Comput. Commun. Security (ASIA CCS)*, 2010, pp. 60–69.

[108] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures: Achieving attribute-privacy and collusion-resistance," in *Proc. IACR Cryptol. ePrint Archive*, 2008, pp. 1–23.

[109] S. F. Shahandashti and R. Safavi-Naini, "Threshold attribute-based signatures and their application to anonymous credential systems," in *Proc. Progr. Cryptol. AFRICACRYPT*, 2009, pp. 198–216.

[110] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures," in *Proc. Topics Cryptol. CT-RSA*, 2011, pp. 376–392.

[111] Z. Liu, H. Yan, and Z. Li, "Server-aided anonymous attribute-based authentication in cloud computing," *Future Gener. Comput. Syst.*, vol. 52, pp. 61–66, Nov. 2015.

[112] N. Kaaniche and M. Laurent, "Attribute-based signatures for supporting anonymous certification," in *Proc. Eur. Symp. Res. Comput. (ESORICS)*, vol. 9878, 2016, pp. 279–300.

[113] R. Guo, H. Shi, and Q. Zhao, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11676–11686, 2018.

[114] O. Bicer and A. Kupcu, "Versatile ABS: Usage limited, revocable, threshold traceable, authority hiding, decentralized attribute based signatures," Cryptol. ePrint Archive, Rep. 2019/203, 2019, pp. 1–21. https://eprint.iacr.org/2019/203

[115] P. Yang, Z. Cao, and X. Dong, "Fuzzy identity based signature," in *Proc. IACR Cryptol. ePrint Archive*, vol. 2008, 2008, p. 2.

[116] S. Guo and Y. Zeng, "Attribute-based signature scheme," in *Proc. Int. Conf. Inf. Security Assurance (ISA)*, 2008, pp. 509–511.

[117] D. Chaum and E. van Heyst, "Group signatures," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, 1991, pp. 257–265.

[118] D. Khader, "Attribute based group signature with revocation," in *Proc. IACR Cryptol. ePrint Archive*, 2007, p. 241.

[119] R. Cramer, I. Damgård, and B. Schoenmakers, "Proofs of partial knowledge and simplified design of witness hiding protocols," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. (CRYPTO)*, 1994, pp. 174–187.

[120] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. (ASIACRYPT)*, 2001, pp. 552–565.

[121] F. Zhang and K. Kim, "ID-based blind signature and ring signature from pairings," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. (ASIACRYPT)*, 2002, pp. 533–547.

[122] S. S. M. Chow, J. K. Liu, V. K. Wei, and T. H. Yuen, "Ring signatures without random oracles," in *Proc. ACM Symp. Inf. Comput. Commun. Security (ASIACCS)*, 2006, pp. 297–302.

[123] N. Chandran, J. Groth, and A. Sahai, "Ring signatures of sub-linear size without random oracles," in *Proc. Automata Lang. Program.*, 2007, pp. 423–434.

[124] H. Shacham and B. Waters, "Efficient ring signatures without random oracles," in *Proc. Public Key Cryptography (PKC)*, 2007, pp. 166–180.

[125] C. A. Melchor, P.-L. Cayrel, P. Gaborit, and F. Laguillaumie, "A new efficient threshold ring signature scheme based on coding theory," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 1–16, Jul. 2011.

[126] S. Haber and B. Pinkas, "Securely combining public-key cryptosystems," in *Proc. ACM Conf. Comput. Commun. Security (CCS)*, 2001, p. 215.

[127] B. Libert and J.-J. Quisquater, "Efficient signcryption with key privacy from gap Diffie–Hellman groups," in *Proc. Public Key Cryptography (PKC)*, 2004, pp. 187–200.

[128] A. W. Dent, M. Fischlin, M. Manulis, M. Stam, and D. Schröder, "Confidential signatures and deterministic signcryption," in *Proc. Public Key Cryptography (PKC)*, 2010, pp. 462–479.

[129] S. Ullah, L. Marcenaro, B. Rinner, S. Ullah, L. Marcenaro, and B. Rinner, "Secure smart cameras by aggregate-signcryption with decryption fairness for multi-receiver IoT applications," *Sensors*, vol. 19, no. 2, p. 327, 2019.

[130] R. Rivest, "The MD5 message-digest algorithm," Comput. Sci. MIT Lab., Cambridge, MA, USA, Rep. RFC 1321, 1992.

[131] W. Mehuron, *The Keyed-Hash Message Authentication Code (HMAC) Category: Computer Security Subcategory: Cryptography*, document FIPS PUB 198, NIST, Gaithersburg, MA, USA, 2008.

[132] Q. H. Dang, *Secure Hash Standard*, NIST, Gaithersburg, MA, USA, 2015.

[133] S. Bleikertz, A. Kurmus, Z. A. Nagy, and M. Schunter, "Secure cloud maintenance: Protecting workloads against insider attacks," in *Proc. ACM Symp. Inf. Comput. Commun. Security (ASIA CCS)*, 2012, p. 83.

[134] B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing shared data on the cloud via security-mediator," in *Proc. IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS)*, 2013, pp. 124–133.

[135] L. Wei *et al.*, "Security and privacy for storage and computation in cloud computing," *Inf. Sci.*, vol. 258, pp. 371–386, Feb. 2014.

[136] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "Blockchain-based database to ensure data integrity in cloud computing environments," in *Proc. CEUR Workshop*, 2017, pp. 146–155.

[137] X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards data assurance and resilience in IoT using blockchain," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, 2017, pp. 261–266.

[138] A. Moinet, B. Darties, and J.-L. Baril, "Blockchain based trust & authentication for decentralized sensor networks," 2017. [Online]. Available: arXiv.1706.01730.

[139] R. Kalis and A. Belloum, "Validating data integrity with blockchain," in *Proc. Int. Conf. Cloud Comput. Technol. Sci. (CloudCom)*, 2018, pp. 272–277.

[140] M. Jakobsson and S. Wetzel, "Secure server-aided signature generation," in *Proc. Public Key Cryptography*, 2001, pp. 383–401.

[141] K. Bicakci and N. Baykal, "Server assisted signatures revisited," in *Proc. Topics Cryptol. CT-RSA*, 2004, pp. 143–156.

[142] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. ACM Symp. Theory Comput. (STOC)*, 2009, p. 169.

[143] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. (CRYPTO)*, 2010, pp. 465–482.

[144] K.-M. Chung, Y. T. Kalai, F.-H. Liu, and R. Raz, "Memory delegation," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. (CRYPTO)*, 2011, pp. 151–168.

[145] C. Gentry and S. Halevi, "Implementing gentry's fully-homomorphic encryption scheme," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, 2011, pp. 129–148.

[146] J. Li, X. Chen, M. Li, J. Li, P. P. C. Lee, and W. Lou, "Secure deduplication with efficient and reliable convergent key management," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 6, pp. 1615–1625, Jun. 2014.

[147] V. Odelu, A. K. Das, Y. S. Rao, S. Kumari, M. K. Khan, and K.-K. R. Choo, "Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment," *Comput. Stand. Interfaces*, vol. 54, pp. 3–9, Nov. 2017.

[148] J. Zhang, B. Wang, F. Xhafa, X. A. Wang, and C. Li, "Energy-efficient secure outsourcing decryption of attribute based encryption for mobile device in cloud computation," *J. Ambient Intell. Humanized Comput.*, vol. 10, pp. 429–438, Feb. 2019.

[149] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, 1998, pp. 127–144.

[150] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Trans. Inf. Syst. Security*, vol. 9, no. 1, pp. 1–30, 2006.

[151] X. Liang, Z. Cao, H. Lin, and J. Shao, "Attribute based proxy re-encryption with delegating capabilities," in *Proc. Int. Symp. Inf. Comput. Commun. Security (ASIA CCS)*, 2009, p. 276.

[152] K. Liang, L. Fang, W. Susilo, and D. S. Wong, "A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security," in *Proc. Int. Conf. Intell. Netw. Collaborative Syst.*, 2013, pp. 552–559.

[153] L. Touati, Y. Challal, and A. Bouabdallah, "C-CP-ABE: Cooperative ciphertext policy attribute-based encryption for the Internet of Things," in *Proc. Int. Conf. Adv. Netw. Distrib. Syst. Appl. (INDS)*, 2014, pp. 64–69.

[154] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," in *Proc. Adv. Comput. Syst. Assoc. Conf. Security (USENIX SECURITY)*, 2011, p. 34.

[155] L. Yong, Z. Zeng, and X. Zhang, "Outsourced decryption scheme supporting attribute revocation," *J. Tsinghua Univ. Sci. Technol.*, vol. 53, no. 12, pp. 1664–1669, 2013.

[156] M. Asim and T. Ignatenko, "Attribute-based encryption with encryption and decryption outsourcing," in *Proc. Aust. Inf. Security Manag. Conf. (ISM)*, 2014, pp. 21–28.

[157] F. Chen *et al.*, "Outsourcing the unsigncryption of compact attribute-based signcryption for general circuits," *Soc. Comput.*, vol. 623, pp. 533–545, Jul. 2016.

[158] H. Liu, P. Zhu, Z. Chen, P. Zhang, and Z. L. Jiang, "Attribute-based encryption scheme supporting decryption outsourcing and attribute revocation in cloud storage," in *Proc. IEEE Int. Conf. Comput. Sci. Eng. (CSE) IEEE Int. Conf. Embedded Ubiquitous Comput. (EUC)*, 2017, pp. 556–561.

[159] K. T. Nguyen, N. Oualha, and M. Laurent, "Securely outsourcing the ciphertext-policy attribute-based encryption," in *Proc. World Wide Web TheWebConf*, 2018, pp. 169–183.

[160] RSA Laboratories. (2018). *What Are Message Authentication Codes*. [Online]. Available: http://www.rsasecurity.com/rsalabs/node.asp?id=2177

[161] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: http://www.bitcoin.org/

[162] M. H. Miraz and M. Ali, "Blockchain enabled enhanced IoT ecosystem security," in *Proc. Int. Conf. Emerg. Technol. Comput.*, vol. 200, 2018, pp. 38–46.

[163] D. G. Roy, P. Das, and D. De, "QoS-aware secure transaction framework for Internet of Things using blockchain mechanism," *J. Netw. Comput. Appl.*, vol. 144, pp. 59–78, Oct. 2019.

[164] C. C. Aggarwal, N. Ashish, and A. Sheth, "The Internet of Things: A survey from the data-centric perspective," in *Managing and Mining Sensor Data*. Boston, MA, USA: Springer, 2013, pp. 383–428.

[165] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the Internet of Things: Threats and challanges," *Security Commun. Netw.*, vol. 7, no. 12, pp. 2728–2742, 2014.

[166] G. Alpár *et al.*, "New directions in IoT privacy using attribute-based authentication," in *Proc. ACM Int. Conf. Comput. Front. (CF)*, 2016, pp. 461–466.

[167] J. Ni, X. Lin, K. Zhang, and X. Shen, "Privacy-preserving real-time navigation system using vehicular crowdsourcing," in *Proc. IEEE Veh. Technol. Conf. (VTC)*, 2016, pp. 1–5.

[168] J. Ni, A. Zhang, X. Lin, and X. S. Shen, "Security, privacy, and fairness in fog-based vehicular crowdsensing," *IEEE Commun. Mag.*, vol. 55, no. 6, pp. 146–152, Jun. 2017.

[169] S. A. Hamad, W. E. Zhang, Q. Z. Sheng, and S. Nepal, "IoT device Identification via network-flow based fingerprinting and learning," in *Proc. IEEE Int. Conf. Trust Security Privacy Comput. Commun. (TrustCom)*, 2019, pp. 1–9.

[170] S. Perez, J. L. Hernandez-Ramos, D. Pedone, D. Rotondi, L. Straniero, and A. F. Skarmeta, "A digital envelope approach using attribute-based encryption for secure data exchange in IoT scenarios," in *Proc. Global Internet Things Summit (GIoTS)*, 2017, pp. 1–6.

[171] Z. Zhou and D. Huang, "Efficient and secure data storage operations for mobile cloud computing," in *Proc. Int. Conf. Netw. Service Manag. (CNSM)*, 2012, pp. 37–45.

[172] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 4, pp. 469–472, Jul. 1985.

[173] L. Yang, A. Humayed, and F. Li, "A multi-cloud based privacy-preserving data publishing scheme for the Internet of Things," in *Proc. Comput. Security Appl. (ACSAC)*, 2016, pp. 30–39.

[174] W.-L. Chin, W. Li, and H.-H. Chen, "Energy big data security threats in IoT-based smart grid communications," *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 70–75, Oct. 2017.

[175] T. H. Noor, Q. Z. Sheng, Z. Maamar, and S. Zeadally, "Managing trust in the cloud: State of the art and research challenges," *IEEE Comput.*, vol. 49, no. 2, pp. 34–45, Feb. 2016.

[176] A. Mahmood, B. Butler, W. E. Zhang, Q. Z. Sheng, and S. A. Siddiqui, "A hybrid trust management heuristic for VANETs," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, 2019, pp. 748–752.

[177] Q. Yang and Y. Liu, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 1–19, 2019.

Salma Abdalla Hamad received the bachelor's and master's degrees (with Distinction) in electronics and communication engineering from the Arab Academy for Science, Technology, and Maritime Transport, Egypt, in 2005 and 2009, respectively. She is currently pursuing the Ph.D. degree with the Department of Computing, Macquarie University. She is working under the supervision of Prof. M. Sheng and Dr. W. E. Zhang. She also possesses over 13 years of working experience in both governmental sector and financial sector, where she executed several projects pertinent to Information Security. Her research interests are concentrated in the domain of information security, more specifically, for the Internet of Things, Smart cities, and smart homes.

Quan Z. Sheng (Member, IEEE) received the Ph.D. degree in computer science from the University of New South Wales. He is a Full Professor and the Head of the Department of Computing, Macquarie University, Sydney, Australia. He was a Postdoctoral Researcher and a Research Scientist with CSIRO ICT Centre. His research interests include Internet of Things, service oriented computing, distributed computing, Internet computing, and pervasive computing. He is a recipient of the AMiner Most Influential Scholar in IoT Award in 2019, the ARC Future Fellowship in 2014, the Chris Wallace Award for Outstanding Research Contribution in 2012, and the Microsoft Fellowship in 2003.

Wei Emma Zhang (Member, IEEE) received the Ph.D. degree in computer science from the University of Adelaide in 2017, where she is currently a Lecturer with the School of Computer Science. She has authored and coauthored more than 50 papers. Her research interests include Internet of Things, text mining, data mining, and knowledge base. She has also served on various conference committees and international journals in different roles, such as the track chair, the proceeding chair, the PC member, and a reviewer. She is the member of ACM.

Surya Nepal (Member, IEEE) is a Senior Principal Research Scientist with CSIRO Data61. He currently leads the Distributed Systems Security Group. He has more than 200 peer-reviewed publications to his credit. His main research focus is in the development and implementation of technologies in the area of distributed systems (including cloud, IoT, and edge computing) and social networks, with a specific focus on security, privacy and trust. He is currently a Theme Leader of Cybersecurity Cooperative Research Centre, a national initiative in Australia. He is a member of the editorial boards of the IEEE TRANSACTIONS ON SERVICE COMPUTING, the *ACM Transactions on Internet Technology*, the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, and the *Frontiers of Big Data-Security Privacy, and Trust*.