Context-Aware Security in the Internet of Things: A survey

Tidiane Sylla, Mohamed Aymeb Chalouf, Krief Francine, Karim Samake

Context-Aware Security in the Internet of Things: A Survey

Tidiane SYLLA

Univ. Bordeaux, Bordeaux INP, CNRS, LaBRI, UMR 5800, 33400 Talence, France/Univ. Sciences, Technique and Technologies of Bamako, ISA, Bamako, Mali
E-mail: tidiane.sylla@u-bordeaux.fr/tidiane.sylla@usttb.edu.ml

Mohamed Aymen Chalouf

Univ. Rennes 1, CNRS, IRISA Lab, UMR 6074, 22300 Lannion, France
E-mail: mohamed-aymen.chalouf@irisa.fr

Francine Krief

Univ. Bordeaux, Bordeaux INP, CNRS, LaBRI, UMR 5800, 33400 Talence, France
E-mail: francine.krief@u-bordeaux.fr

Karim Samaké

Univ. Sciences, Technique and Technologies of Bamako, Bamako, Mali
E-mail: samakek@yahoo.fr

Abstract Internet of Things applications encompass home-automation, health, transportation, etc. The main objective of these applications is to improve user's daily lives. However, security and privacy threats and the lack of adapted security mechanisms could significantly reduce their development and slow-down their adoption. Several researches have been conducted in order to find solutions for securing the IoT systems and to reduce, even eliminate risks for user's privacy. One of the proposed solutions is context-aware security, which enables to consider relevant contextual information while implementing security mechanisms. In this paper, we will conduct a survey of the context-aware security solutions that have been proposed for smart city IoT applications. These applications have a great impact on citizens life. For each solution, we will provide critical analysis in terms of context-aware management, security services and privacy mechanisms. Then, we will identify the different research directions for better context-aware security in these applications.

Keywords: Internet of Things, Security, Privacy, Context-Awareness, Context-Aware Security

1 Introduction

The Internet of Things (IoT) is a paradigm which consists in connecting the virtual world of the Internet to the real world through so-called intelligent objects. These objects are featured with data communication and exchange capabilities on the Internet. The concept was first mentioned in 1999 by K. Ashton (Biron and Follett, 2016). Over the years, IoT has extended the Internet to everyday objects to enable them to be intelligent. These objects include automated door actuators, bulbs, fridges, thermometers, clothes, shoes, watches, etc. The number of connected objects to the Internet has increased exponentially. According to a study published by Ericsson in 2016, there will be at least two connected objects per person, a total of 18 billion connected objects in 2022 with a world population estimated at 7.6 billion of people (Ericsson, 2019).

In addition, IoT covers many application areas: environment, smart city, industry 4.0, smart transportation, etc. The smart city IoT applications encompass e-health, smart homes, smart buildings, smart water management, smart grid, smart mobility, smart waste management, etc. However, despite its advantages, the challenges that hinder the development of the IoT are numerous. In this survey, we study the solutions proposed to provide context-aware security and privacy in smart city IoT application. The reason for this choice is that smart city IoT applications are the applications in which citizens' privacy is most affected. Indeed, the number of users is growing rapidly, with approximately 68% of the world population living in cities in 2050. Moreover, to the best of our knowledge, there is no complete survey on context-aware security in this field. Context-aware security allows the use of context-awareness offered by the IoT in order to dynamically implement security and privacy mechanisms.

For user data consumers, user-centric security and privacy consists of taking measures to implement security and privacy mechanisms when processing information (collection, usage, transmission, storage, etc.) (Svet, 2019). In this sense, the user-centric approach makes it possible to answer these questions by considering user preferences, specificities and regulatory compliance (for example, the General Data Protection Regulation in Europe). As context-aware security could enable users to be aware of security and privacy characteristics, it could be valuable in facilitating the implementation of the user-centric approach in smart city IoT applications. Indeed, smart city IoT applications are sensitive to the user's context, i.e. they are able to react differently according to different user situations.

This paper also outlines the research, and its subsequent challenges, necessary for optimal security and privacy for smart city IoT applications. We believe that this endeavour will help in understanding this area and to undertake more in-depth studies on sub-topics. This paper is organised as follows: in Section 2, we introduce the IoT concept and describe the security problems present in smart city IoT applications. In Section 3, we describe the concepts of context-awareness and context-aware security in IoT. In Section 4, we present the projects that have proposed context-aware security solutions in the context of some smart city IoT applications (smart home, eHealth, etc.). In Section 5, we present a critical review of the considered projects as well as some relevant challenges and research directions. Finally, Section 6 concludes this paper.

2 Background

In this section, we will first describe the concept of IoT. Then, we will present the proposed IoT reference architectures in order to facilitate new applications development (ITU,

2012; Lin et al., 2017). We will describe the reference architecture proposed by the International Telecommunication Union (ITU). The reason for this choice is that ITU is the global organization in charge of information and communication technologies standardization.

2.1 IoT Definition

The term IoT was coined by K. Ashton in 1999 (Biron and Follett, 2016). Since that time, IoT has generated strong interest in academia and industry. This interest is explained by the various advantages that IoT brings to various domains (agriculture, health, environment, industry, transport, etc.). This interest is also explained by the financial windfall it represents (Atzori et al., 2010; Gubbi et al., 2013). IoT's vision is broad and encompasses several technologies: Wireless Sensor Networks (WSN), machine to machine communications (M2M), etc.(Guo et al., 2015; Singh et al., 2014).

The SG20 workgroup of the telecommunications branch of the ITU (ITU-T) defines the IoT in recommendation Y.2060 as:"*A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies*(ITU, 2012)". This definition of ITU-T considers two aspects of IoT: Internet and Things. The first is network oriented since it relies on the existing Internet. The second one is towards the integration of generic objects into networks to offer value-added services.

The Internet Engineering Task Force (IETF) definition focuses on objects and their connectivity aspects (addressing and identification, communication protocols, etc.). Thus, according to the IETF, IoT is a network of physical things that can exchange data. The Joint Technical Committee 1 (JTC1) of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have also defined IoT as follows: an infrastructure of interconnected entities (objects, people, systems) and information resources as well as intelligent services enabling them to process and react to information from the physical and virtual world (ISO/IEC, 2014).

From these definitions, we define IoT as:"*An infrastructure of interconnected devices using information and communication technologies, and enabling the physical world to be connected to the virtual world in order to provide advanced and intelligent services*".

2.2 IoT Applications

IoT applications enable smart services that make the everyday life easier. They help in optimizing business and production processes. Apart from these, they also increase productivity in agriculture.

- **e-Health**: IoT applications are particularly valuable for monitoring a person's health. They are based on several devices including sensors that provide data about blood glucose level, blood pressure, heart rate, etc. They make it possible to better care for babies, elderly and patients with special disease (e.g. diabetics).

- **Smart home**: Smart homes are one of IoT's flagship applications. A smart home is one whose lighting and security systems can be remotely controlled by a smartphone or a computer. These applications help to save energy by automatically turning off lights, televisions and other home electronics when they are no longer in use (Khan et al., 2018).

- **Smart city**: IoT applications for smart cities improve water management and save energy in cities. They enable cities to improve the safety of citizens, through Closed-Circuit Television (CCTV) cameras and automatic alerts.

- **Transports:** IoT has many applications in the field of transport and logistics (Mehta et al., 2018). Intelligent Transport Systems (ITS) allow vehicles to travel safely on the road. Internet of Vehicles (IoV) allows vehicles to exchange information such as their positions, speeds, directions, etc. among themselves, improving road safety.

- **Logistics**: In logistics, transport vehicles, containers and goods are equipped with geolocation devices and sensors (e.g. temperature). IoT logistics applications enable real time tracking of goods and helps to quickly take decisions, optimize paths and reduce costs.

2.3 IoT Characteristics

In this part, we will explore some characteristics of IoT, which must be taken into account when implementing security in IoT.

- **Intelligence**: Intelligence means the application of knowledge in IoT. It is usually implemented by a combination of algorithms and techniques for advanced data processing (e.g. artificial intelligence) and computation. This intelligence is present at the service level layer of an IoT architecture.

- **Context-Awareness**: IoT is mainly driven by the collection of data from devices. This data collection reflects dynamic changes that occur in the device environment. The devices must also cope with changes in context (change of geographical location), number of devices present (adding or removing devices on the fly) and network configuration (frequent changes in access network). The device state also changes dynamically with sporadic activity and connectivity times, changing them from standby to active or from connected to disconnected.

- **Adaptation**: IoT systems must be integrated with their surrounding IT infrastructure.

- **Sensitive data**: According to the General Data Protection Regulations (GDPR) of the European Union, sensitive data is defined as follows: "*a data is considered sensitive if it can reveal a person's ethnic or racial origin, religious belief and political opinions. Sensitive data also includes a person's genetic code, biometric data used to identify the person, health data and sex life or sexual orientation* (Council and Parliament of European Union, 2016)". In addition to these data, other personal data may also be considered sensitive, such as location, preferences, etc. Therefore, the user data collected by IoT devices is mostly sensitive.

- **Heterogeneity**: IoT involves devices and systems based on different hardware, software and network configurations. These devices can interact with each other or with different service platforms via heterogeneous networks. The applications and systems to be implemented will have to support the heterogeneity of IoT, i.e., to allow interoperability and modularity.

- **High devices density**: IoT is distinguished by the large number of connected devices. This number is estimated to be about eighteen billion by 2022 (Ericsson, 2019). Therefore, its implementation should allow scalability.

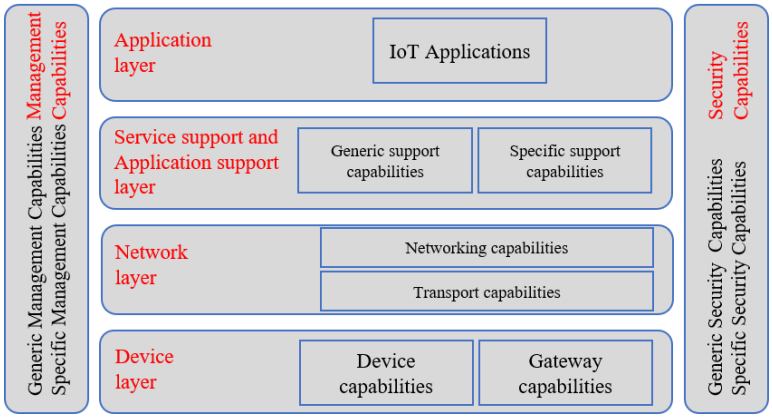

Figure 1 ITU-T Reference Architecture (ITU, 2012)

- **Constrained resources**: Connected devices are the essential elements of an IoT architecture. Their low cost and environmental constraints affect their capabilities. This results in limited resources (CPU, memory, energy) available for the vast majority of devices (Bormann et al., 2014).

- **Real-time**: Some IoT applications need to process collected data in real-time. Applications aiming to provide a new user experience or a responsive critical system require real-time data processing. This ranges from monitoring patient health to the adaptation of commands and controls in vehicular networks.

2.4 IoT Architectures

ITU has proposed through recommendation Y.2060 a reference architecture for IoT (ITU, 2012; Cheng et al., 2013; Darwish, 2015; Di Martino et al., 2018). This architecture is composed of four main layers and two transversal layers (Figure 1). The main layers are: device layer, network layer, service and application support layer and application layer.

The device layer is composed of device and gateway capabilities. They interact with communication networks. Device capabilities make it possible for devices to collect and share data with the physical world. It also supports device sleep and wake-up states for energy saving. Gateway capabilities provide multiple interface support to devices. This enables devices connected through different communication technologies (IEEE 802.15.4, Bluetooth Low Energy, ZigBee, etc.) to communicate over their local networks. Gateway capabilities also provide protocol conversion to devices. As an example, we can consider Bluetooth as the device layer and 3G as the network layer.

The network layer consists in network and transport capabilities. Transport capabilities provide connectivity for the service transport and application-specific data. Secondly, it ensures the transmission of related control and management information. Networking capabilities provide connectivity control functions: authentication, access control, transport resource control, mobility management, etc.

The service and application support layer connect infrastructure and applications. Generic support capabilities provide common capabilities to different IoT applications, (e.g. data processing and storage). Specific support capabilities consist in the different detailed capabilities to provide various support functions to IoT applications. Furthermore, it allows

to hide internal details of applications and/or infrastructure as well as the implementation of applications made with heterogeneous objects and technologies.
The application layer is composed of IoT applications, such as smart home, e-health, etc.

The two transversal layers are management and security capabilities. Security capabilities are composed of two types: generic and specific. Generic security capabilities are application independent. They aim to ensure security services at main layers. Specific security capabilities are dependent on application requirements (e.g. mobile payment).
The management capabilities layer ensures the proper functioning of the IoT network. It can be divided into generic and specific management capabilities. Generic management capabilities include but are not limited to device management (firmware update, diagnostics), local network topology management, quality of service, etc. Specific management capabilities are application dependent, e.g., the patient's vital signs transmission requirements.

2.5 Security

Despite the numerous advantages of IoT, there are many challenges that hinder its development. In the following subsections, we will present security challenges of IoT. We will also address the threats to privacy and proper functioning of IoT applications.

2.5.1 Security challenges

Security and privacy are among the most important concerns in IoT ((Kumar and Patel, 2014; Borgohain et al., 2015; Li et al., 2017; Oracevic et al., 2017; Sadique et al., 2018)). According to the literature, several security risks in IoT are mainly due to the device vulnerability (Woolf, 2016; Li et al., 2017). These vulnerabilities are essentially the result of constraints related to their limited capacity and the absence of security measures at the design stage. They facilitate unauthorized access to personal information and larger networks. For example, an attacker can launch denial of service attack through a compromised device.

IoT devices collect huge amounts of data that can pose several privacy risks. According to a report by the Federal Trade Commission, just 10,000 households using smart home technology can generate up to 150 million discrete data points per day (Staff, 2015). These data often contain sensitive information. The more data there is, the more it is possible to infer and link the data together to establish a profile. Another problem that privacy faces in IoT is the possibility for adversaries to practice eavesdropping, i.e., to virtually invade a person's home, follow his movements and actions, or even predict where he might go.

2.5.2 Security threats

Each layer of the IoT architecture has several vulnerabilities. Attacks exploiting these can target different communication protocols as well as applications and services. These threats come from known and zero-day vulnerabilities, taking advantage of limited capacity of devices and their physical location. Thus, the detection layer faces two types of attacks: attacks against devices (physical capture, unauthorized access and extraction of sensitive data, vulnerable firmware, cloning and device spoofing) and attacks against communications (malicious code execution, denial of service (DoS), information interception, etc.).

The network layer must protect itself from attacks against routing, Man-in-the-middle, eavesdropping and data transmission attacks Garcia-Morchon et al. (2018); Li et al. (2017). The service layer must be protected from access attacks on privacy, unauthorized access to the service, and DoS (Li et al., 2017). At the application layer, the user himself because of

his negligence and lack of awareness, is a perfect entry point for an attacker, and therefore constitutes a vulnerability. Thus, this layer must protect itself against attacks on authentication systems, privacy breaches, data falsification, and unauthorized commands and controls.

In addition, tools for automatically discovering flaws and vulnerabilities in IoT devices are available on the Internet and are easily accessible. These tools allow even low-skilled people to detect flaws and vulnerabilities in IoT devices, no matter where in the world the device is located. As a consequence, they increase the risk of attacks on IoT application security and user privacy. Among these tools, we have Shodan, a search engine for vulnerable devices connected to the Internet. More recently, a tool called Autosploit has been published on the Internet (Sass, 2018). OWASP (Open Web Application Security Project) has compiled a list of known IoT vulnerabilities (Miessler and Smith, 2018).

As we said before, security vulnerabilities are present in the IoT architecture's layers. This is due to the specific and heterogeneous characteristics of devices, their attractiveness to hackers, communication protocols and technologies, and the services and applications that make up the different layers of the architecture. Therefore, the risks of security and privacy are high. It is then very important to take into account the security and privacy requirements of users from the design of the systems to their deployment. It is also important to educate users about security and privacy issues in their use of IoT applications.

3 Context-Aware Security in IoT

In this section, we will discuss the concepts of context-awareness and context-aware security. Next, we will describe the implementation of context-aware security in IoT.

3.1 Context-Aware Computing in IoT

A context-aware computing system has been defined in (Abowd et al., 1999) as follows:"*A system is context-aware if it uses context to provide relevant information and/or services to the user, where relevancy depends on the user's task* (Abowd et al., 1999)". From this definition, we define a context-aware IoT system as follows:

"*A context-aware IoT system is a system that uses the context to obtain relevant information that allows the optimization of services provided to the user through dynamic actions and adaptations made without the user's intervention*".

3.2 Context-aware security in IoT

Context-aware security has recently emerged to address the new security challenges brought by the increased presence of ubiquitous, heterogeneous and mobile computer systems. Brézillon et Mostéfaoui (Brézillon and Mostéfaoui, 2004) have defined context-aware security as follows: "*Context-aware security is all about considering "context" explicitly in the specification of security solutions (access control models, cryptographic protocols,etc.)* (Brézillon and Mostéfaoui, 2004)".

We define context-aware security in IoT as follows: "*Security is context-aware in an IoT system if the choice and implementation of security mechanisms are based on the user's context and are done without explicit user's intervention*".

The pervasiveness of IoT devices and applications raises security and privacy issues. Thus, several studies have been carried out to solve these problems, but most of the proposed

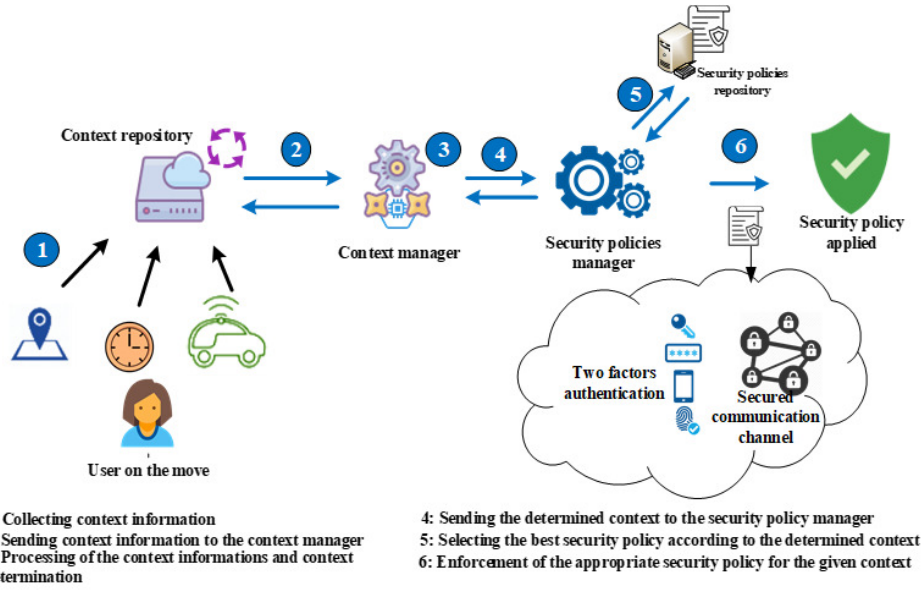

Figure 2 Implementation of context-aware security in IoT application

solutions are static and not adapted to the dynamic nature of the IoT.

To better meet the security and privacy needs of users in smart cities, the solutions proposed must enable the user to play a central role. In this sense, these solutions must include mechanisms that adapt to the different contexts of the user (for example, according to the location: home, work, public places, etc.). Unlike traditional methods, which are static, the user will be continuously protected appropriately and effectively in all contexts. Indeed, the change of context or situation at a given time "t" may make a level of security insufficient whereas it was quite appropriate and sufficient in the previous context or situation at the given time "t-1". Figure 2 illustrates an IoT system implementing context-aware security.

Several studies have shown that it is possible to use context-awareness to ensure effective security in IoT (de Matos et al., 2018b; Hayashi et al., 2013; Neisse et al., 2015a). Examples of such approach include authenticating the user based on geographical location (home, office, public transport, hospital, etc.), usage of a secure communication channel with certain devices based on the user's activities, or not disclosing user data in the presence of a suspicious application. Table 1 summarizes the advantages of context-aware security compared to conventional security.

4 Projects integrating a context-aware security architecture in IoT

Context-aware security in ubiquitous computing applications has generated research interest in recent years. Thus, several projects have been carried out with the objective of proposing architectures and systems that offer context-aware security in different settings, including the IoT. In the following subsections, we will examine some important and representative projects that were proposed in the context of Smart City between 2010 and 2018.

Table 1 Benefits of context-aware security

Security services	Conventional	Context-aware	Benefits
Authentication and access control	• Fixed authentication method. • Fixed allocation of authorization tokens. • Single authorization of the user or not.	• Simple or strong authentication method depending on the context and risks. • Allocation or reallocation of dynamic authorization tokens based on context and reputation. • Dynamic access control to data based on attributes or roles depending on the context. • Access control based on defined roles or attributes.	• Compromise between security and usability. • Ability to add and dynamically revoke authorizations. • Protection against unauthorized access.
Privacy	• Static data disclosure. • Static anonymization of data.	• Data collected under user control. • Disclosure of data based on context and risks without user intervention. • Implicit anonymization of data according to context. • Dynamic user intervention required if the context risks are high.	• Better control over user data. • Contextual and dynamic access control (to private data). • The data is automatically disclosed or anonymized using high granular and contextual access control. • Privacy protected in all contexts.
Communication security	• Only one mode of communication: secure protocol (application, transport, net-work, etc.).	• Selection of the communication mode according to the user's context: choice of the layer that will implement security. • Choice of security level (algorithms, keys, etc.).	• Sensitive communications are secure regardless of the user's situation.
Security of stored data	• Encrypted data when stored in dedicated servers. • Static verification of data integrity.	• Data encrypted during storage regardless of the location (Cloud, Fog, etc.). • Dynamic verification of data integrity.	• Sensitive data secured according to the storage location and the user's context.

4.1 Context-Aware Scalable Architecture (CASA)

In (Hayashi et al., 2013), the authors proposed to use a set of sensors located in a user's environment to determine some contextual information such as habits or geographical location in order to lighten or strengthen authentication. Indeed, the problem identified here is to choose the authentication mechanism appropriate to the context.

First, the system uses sensors in the user's environment (body sensors, home automation sensors, etc.) to deduce passive factors such as geographical location or the time of the last connection. A Bayes classifier is then used to combine several factors to infer the user's context (e.g. home, work). The inferred context then determines the appropriate type of authentication; either strong authentication with a password and PIN code, or simple authentication with a PIN code only. The main contextual parameter used in this work is the location of the user's mobile phone.

The main advantage of this solution is to address user negligence during smartphone access. However, it has some drawbacks. Indeed, it only aims to authenticate smartphone users, and does not take into account other security services. In addition, secure context-awareness management is not ensured.

4.2 Context-Aware Security Framework for Mobiles Applications (CASFMA)

In (Mowafi et al., 2014), the authors proposed a context-aware security solution to address security and privacy issues in mobile applications. The objective is to use the user context to dynamically adapt the security settings of mobile applications. Mobile applications are run inside enclaves to control their access to mobile network resources. This allows security and communication control mechanisms to be applied individually to each application.

This solution advantage is the individual and adaptive enforcing of specific security and communication control mechanisms. Users will have to decide when applications are allowed to access the network. However, this solution does not address the authentication as well as communication security. In addition, adaptive access control of the solution is not quite complete. Indeed, it does not address resource access control for devices.

4.3 Managing Context Information for Adaptive Security in IoT environments (MCIASIoTE)

Ramos et al. considered the use of contextual information in the implementation of security decisions in IoT (Ramos et al., 2015). The work carried out has made it possible to extend IoT security architecture proposed in (Bernal Bernabe et al., 2014). Based on the Architecture Reference Model (Bassi et al., 2013) of the European IoT-A EU[1] project, this architecture allows extending the security functionalities of the former, by adding components that allow the implementation of the context-aware security.

The main objective of this architecture is to demonstrate that the different components proposed in the Privacy-Preserving Security Framework for a Social-Aware Internet of Things project (Bernal Bernabe et al., 2014) can use contextual information to enable things to make security decisions. A novelty of this approach is that it considers security issues in the management of contextual information. For example, the context manager will only process contextual information from safe things.

This work presents several advantages. It allows implementing adaptive security and privacy mechanisms. Secondly, it enables contextual authorization management by using contextual access control tokens. In addition, it addresses the security issues of context-awareness management. However, the solution presents some drawbacks. Indeed, the scope of IoT applications covered by the solution and the way they can be integrated are not given. The contextual access token management does not allow users to dynamically deliver or revoke authorisations. Moreover, solution evaluation is not provided.

4.4 Dynamic Context-Aware Scalable and Trust-Based IoT Security, Privacy Framework (DCASTBISPF)

In (Neisse et al., 2015a), the authors have proposed an architecture that allows defining security policies that can be deployed dynamically according to the user context. As a result, different security policies can be defined for different contexts, roles and things. The main objective is to dynamically provide security and privacy according to the context of a smart city citizens. Depending on the user's context, the corresponding security policy will automatically be applied by all the involved things.

The proposed architecture is essentially based on SecKit, a security toolbox developed by the same authors (Neisse et al., 2015b) and uses policy-based security management defined by the IETF (Scherling et al., 2001).

The main contribution of this solution is the implementation of contextual security policies in the smart city IoT applications. However, some important security mechanisms are not provided by the solution (e.g. authentication and communication security). In addition, secure context-awareness management is not ensured.

4.5 Context-Aware Authentication Service for Smart Homes (CASSH)

In (Ashibani et al., 2017), the authors have proposed a context-aware authentication service for mobile users in smart home environments. The main objectives are, on the one hand, the implementation of a dynamic authentication model for users by allowing them to access smart home services using traditional and contextual identification information. On the other hand, flexible and secure access to services.

The proposed architecture combines several contextual parameters for deducing authentication type to be enforced. The identified context parameters are user profile (name, ID, etc.), location (IP and Bluetooth address), calendar and history information (log and access patterns). The central element of the architecture is a gateway. This is an application installed on a Raspberry pi.

This solution has many advantages. First, it leverages user agenda combined with his location and access network for context detection. Secondly, it takes into account user context security levels for choosing adapted authentication type. However, this solution has a few drawbacks too. It only addresses adaptive authentication in the smart home application. Other security and privacy mechanisms are not addressed. In addition, the solution is application-specific. Solutions that support multiple smart city applications and IoT devices are needed. This is due to a large number of heterogeneous applications and devices in the smart city context. Moreover, secure context-awareness management is not ensured.

4.6 Context-Based Security and Privacy for Healthcare IoT (CBSPHIoT)

In (Alagar et al., 2018), the authors have addressed patient-centric security and privacy issues in the Healthcare Internet of Things (HIoT) system. According to the authors, the proposed solution ensures security and privacy in the HIoT system. It is based on the enforcement of different strategies for each context.

The architecture includes Contextual Role-Based Access Control, which controls access to a patient's information. It uses a combination of constraints, i.e, context and role to allow or deny an action. A patient's information is represented in the system by the Personal Health Model. Patient health monitoring information is combined with PHM to form the

Table 2 Benefits of context-aware security

Projects	CASA	CASF MA	MCIAS IoTE	DCAST BISPF	CASSH	ECSA	CBSPH IoT
Scope	PMC	PMC	IoT	IoT	IoT	IoT	IoT
Privacy	No	No	Yes	Yes	No	Yes	Yes
Authentication	Yes	No	Yes	Yes	Yes	Yes	Yes
Access control	No	Yes	Yes	Yes	Yes	Yes	Yes
Confidentiality	No	No	Yes	No	No	No	Yes
Integrity	No	No	No	No	No	No	No
Availability	No	No	No	No	No	No	No
Accountability	No	No	No	Yes	No	No	No
Context-aware	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Evaluated	Yes	Yes	No	Yes	Yes	No	No
Scalability	No	No	No	Yes	No	Yes	No
Heterogeneity	No	No	No	No	No	Yes	No

PMC: Pervasive Mobile Computing, IoT: Internet of Things

Electronic Patient Record.

The major contribution of this solution is the contextual role-based access control system. Its advantage is that it allows enforcing access control using the role and context of users. It also ensures confidentiality of patient sensitive data. Nevertheless, this solution presents some drawbacks , by not being adapted to to many smart city IoT applications like smart home, smart car, etc. This can be explained by the system focused on by the authors, i.e, HIoT. Otherwise, all adaptive security and privacy mechanisms are not ensured. Moreover, context-awareness management security is not ensured.

4.7 Edge-centric Context Sharing Architecture (ECSA)

In (de Matos et al., 2018b), the authors have proposed an architecture to address adaptive security and privacy issues in IoT. This architecture provides context-aware security by using shared contextual information. Context sharing is the sharing of contextual information at all levels of a system's architecture, in order to have a common understanding of the context (Perera et al., 2014).

The proposed architecture takes advantage of Fog and Edge computing for improving scalability and reduce network latency. It includes a module responsible for context-sensitive security, the Context-Aware Security Manager. The ECSA architecture has been implemented and evaluated in (de Matos et al., 2018a). To the best of our knowledge, the context-aware security module (de Matos et al., 2018b) has not been evaluated yet.

This solution presents interesting features for adaptive security and privacy in smart city IoT applications. First, it leverages edge/fog network architecture integration to make it scalable. Secondly, it provides all adaptive security and privacy mechanisms. However, it presents some drawbacks. The authors did not provide any evaluation of the context-aware security manager. In addition, context-awareness management security is not ensured.
Table 2 provides a comparison between the proposed solutions for context-aware security concerning some smart city applications. In the following sections, we will analyze these architectures in terms of secure context-awareness management and security services. We will also compare these different architectures in terms of heterogeneity and scalability.

5 Critical review of context-aware security needs in the IoT

This section provides a critical review of security needs in IoT and discusses how to make these services context-aware. First, we will compare studied projects according to a cross-cutting element to context-aware security and privacy services: secure context-awareness management. Then, we will make a detailed comparison of the studied projects in terms of context-aware privacy and security services. Thus, we will compare these projects according to the used approach (user-centric or classic) and the context-aware mechanisms proposed.

5.1 Secure context-awareness management

In this section, we will focus on the security of context-awareness management. We will identify research to be carried out for a secure management of context-awareness.

5.1.1 Critical analysis of the studied projects

The context-awareness management may be threatened by adversaries who can monitor the system, attempt to reproduce contexts and to mislead system perception. Therefore, its security must be ensured. In this sense, context information should be acquired from trusted devices and protected from prying eyes. Finally, the trustworthiness of the determined context should be ensured. Apart from the MCIASIoTE project, none of the projects studied have tackled these issues.

In the MCIASIoTE, the authors proposed the use of Ciphertext Policy Attribute-Based Encryption (CP-ABE) (Bethencourt et al., 2007) for securing context information acquisition. The CP-ABE enables devices to send encrypted context information that only the recipient, i.e., the context-awareness manager, will be able to decrypt. The devices responsible for sending secured context information are said to be trusted. This scheme presents two advantages. It uses well-known encryption system for securing context information acquisition. Secondly, it ensures that only trusted context sources will be able to send context information to the system. However, the authors have not addressed the trustworthiness of the context. Indeed, an adversary can take control of a context source and manipulate it to send fake context information.

5.1.2 Research directions

The issues raised regarding secure context-awareness management warrant further research. Initially, this research should focus on securing context information by using lightweight cryptographic schemes. This will reduce the risk of interception and modification attacks during transfer. Much work has been done on lightweight attribute-based encryption based on the Elliptic Curve Cryptography (ECC) schemes (Singh et al., 2015; Yao et al., 2015). Moreover, research should be done on post-quantum cryptographic schemes adapted to IoT and resistant to quantum computing algorithms (Cheng et al., 2017; Liu et al., 2018; Guneysu and Oder, 2017). Indeed, public-key cryptography schemes (e.g. ECC) may be broken by quantum computers in the future.

Secondly, research should be done to exclude any unauthorized device for sending contextual information to the management system. This allows the context-awareness management system to process only contextual information from trusted devices. There are several well known trust management techniques in the IoT, one of them being reputation-based trust management. Here, devices trust should be evaluated in a distributed manner.

The distributed ledger, e.g., the Blockchain presents good features for distributed trust management in IoT (Di Pietro et al., 2018).

Finally, the trustworthiness of the context prevents several attacks on a context-aware security system. What happens when this is not the case? Indeed, an adversary can try to compromise the context perception, say by trying to send fake context information to the system. This issue must be looked into. One possible solution is to use feedback systems coupled with the correlation between the context and the user profile.

5.2 Privacy

In the following subsections, we will focus on privacy. We will make a detailed comparison of the studied projects according to the context-aware privacy-preserving mechanisms. Finally, we will identify research initiatives for effective context-aware privacy in IoT.

5.2.1 Critical analysis of the studied projects

We conducted an in-depth review of projects that have integrated context-aware security in section 4. Some of these projects have proposed context-aware privacy mechanisms. Table 3 compares the studied solutions in terms of context-aware privacy.

Context-aware privacy has been proposed in several projects. The main difference between the proposed solutions is the privacy mechanism (pseudonymization, anonymization, obfuscation, etc.). For each project, we start by recalling the approach used, before discussing the context-awareness of privacy and the proposed mechanisms.

The user-centric approach to privacy in the aforementioned IoT applications has been poorly addressed in the studied projects. In the DCASBISPF project, the authors implemented a user-centric approach to making privacy decisions. They considered privacy issues at the design stage (privacy by design). They also considered issues related to the digital divide, usability and compliance with regulations. According to the authors, the user defines his privacy preferences for each context through a graphical interface. This scheme has the advantages of being easy to use and privacy regulation-compliant. But giving preferences does not guarantee the user that his data is disclosed as stated. However, the mechanism implemented does not allow the user to control the collection of his data by his devices.

The other projects that supported context-aware privacy (CBSPHIoT, ECSA and MCIASIoTE) used a classical approach. The mechanisms proposed in these projects are not suitable for the aforementioned IoT applications. Indeed, the user cannot define his privacy preferences. The user is also not aware of the possible consequences of his actions regarding his privacy. In addition, these projects do not take into account existing privacy regulations, such as the General Data Protection Regulation (GDPR) in Europe (Council and Parliament of European Union, 2016).

Finally, context-aware privacy must use context perception to deploy appropriate mechanisms adapted to different contexts. In the MCIASIoTE project, a context-aware privacy mechanism based on anonymization was proposed. This mechanism consists of a user using a subset of his identity attributes depending on context while sharing his data with applications. These partial identities are mapped to user identity attributes. The main advantage of this scheme is the dynamic aspect of data anonymization. Indeed, the user can choose a different partial identity for a different context. Data anonymization is a data transformation technique which consists of irreversibly altering a user's personal data in a way that anonymizes this data. However, it presents some drawbacks. An adversary with enough user data can recover the identity of the user, due to its link with the user's partial identities.

We note that this mechanism has not been evaluated.

The DCASBISPF project implemented the pseudonymization of identities according to context and the delay in message delivery. This solution has two contributions. Firstly, the context-based pseudonymization is advantageous for the user. Depending on the context, it anonymizes user data using pseudonyms. Secondly, the user has the possibility to delay message delivery. Indeed, message delivery can prevent real-time tracking of the user. This mechanism has actually been evaluated, as opposed to the MCIASIoTE project. One of its shortcomings is that it does not protect user location. Data is also not protected at the device level (Abi Sen et al., 2018). In addition, it is possible for an adversary to identify a person by inferring on the data or by cross-checking them with other data of the same person. The risk of de-anonymization is even greater with social networks, through which users share multiple data (Lee et al., 2017).

The CBSPHIoT project has implemented data anonymization and confidentiality. However, this privacy mechanism, unlike the others implemented in the MCIASIoTE and DCASBISPF projects, is not context-aware. Indeed, the authors focused on the access control system, which preserves patients' privacy. But this mechanism is not suitable for smart city applications, as it does not consider their characteristics. Furthermore, as in the case of the MCIASIoTE project, it has not been implemented and evaluated. In the ECSA project, no details are given on the mechanism proposed.

5.2.2 Research directions

The solutions proposed to ensure privacy-preserving in a context-adaptive manner in the projects discussed above only propose a mechanism with several limitations, and most of them are still at the proposal stage.

The attacks described in subsection 2.3.2 can threaten privacy in all layers of an IoT architecture. First, the research to be conducted must focus on user-centric privacy using context-awareness. In a second step, the solutions to be developed will have to consider the context for effective protection, by exploiting the characteristics of the smart city's IoT applications. Thus, the solutions to be proposed must allow the user's identity and private data to be protected, whatever the context.

These solutions should focus on the user's ability to define his privacy preferences. Privacy preferences vary from user to user. Regulations are designed to enable user-centric privacy preserving. To this end, the research to be carried out should make it possible to implement and comply with the recommendations resulting from the regulations in force (e.g. the GPDR). For example, in (Barhamgi et al., 2018), the authors proposed a user-centric and regulatory compliance architecture for privacy. This mechanism is independent of other security services and is not context-aware. However, privacy must be complementary to security services such as authentication, integrity, access control, confidentiality, etc., to mitigate the risks of attacks threatening privacy.

Furthermore, research is needed to enable users to exercise more effective control on the collect and disclosure of their data according to the context, but also to reduce the amount of collected data. One possible approach is the proposal of a context-aware data management module that will make it possible to filter the data collected by devices before they are sent to consumer entities, according to the user's preferences. This module will also allow data to be disclosed according to risks and user's preferences, using appropriate anonymization mechanisms. For example, Torre et al. have proposed a similar module (Torre et al., 2016). However, the proposed module is not context-aware. As with the architecture proposed in (Barhamgi et al., 2018), this module does not include an additional security service.

Table 3 Comparison of work that has proposed mechanisms for context-aware privacy in IoT

Projects	Contributions	Limits
MCIASIoTE (Ramos et al., 2015)	• Context-based anonymization of object and user identities	• Insufficient for optimal privacy-preserving • Not user-centric • Lack of mechanisms allowing the user to effectively control his data (collect and disclosure) • Not evaluated
DCASTBISPF (Neisse et al., 2015a)	• User identity pseudonymization according to the contextual security policy • Delayed delivery of messages to prevent tracking	• Possible identification of the user by inferring on the data • Lack of control on data collect
ECSA (de Matos et al., 2018b)	• Contextual security rules	• Lack of details on the mechanisms and techniques implemented • Not user-centric • Not evaluated
CBSPHIoT (Alagar et al., 2018)	• Data anonymization during extraction	• Not user-centric • Lack of mechanisms allowing the user to effectively control his data (collect and disclosure) • Not evaluated • No context-awareness in data anonymization

Based on the previous privacy-preserving issues, it is clear that a single privacy mechanism is not sufficient. This is explained by the difference between the types of sensitive information to be protected: identities, location data, profile data, etc. Therefore, research must be done to support a combination of several privacy mechanisms for optimal protection. For example, a combination of anonymization for identity protection, obscuration for location data protection, encryption and data management techniques for data security.

Furthermore, standard privacy mechanisms should be proposed. This will standardize privacy techniques in a similar way to standardized and recognized cryptographic systems (e.g. RSA: Rivest Shamir Adleman, AES: Advanced Encryption Standard (Mahajan and Sachdeva, 2013)). Privacy also includes data security at the storage and during transit level. These points will be discussed in subsections 5.4.1 and 5.5.

5.3 Authentication and Access control

Authentication and access control have been the subject of several proposals in the studied projects. In the following subsections, we will focus on the context-aware authentication and access control mechanisms proposed or implemented in these projects.

5.3.1 Authentication

In the next subsections, we will provide a detailed comparison of the studied projects in terms of context-aware authentication mechanisms proposed or implemented. Then, we will identify some research direction to enable context-aware authentication for effective context-aware security in IoT smart city applications.

5.3.1.1 Critical analysis of the studied projects

The great majority of the studied projects has proposed or implemented an authentication mechanism in their solution. Some of these mechanisms are context-aware, others are not. In table 4, we provide a comparison between these works.

In subsection 3.3, we presented several IoT applications use-cases, in which context-aware authentication could solve problems of security and usability of these applications. These applications are usually installed on smartphones and tablets to allow users to interact with them. In CASA project, the proposed authentication mechanism allows to dynamically propose to the user a simple or strong authentication method, in order to provide security while facilitating access to his phone. Thus, this mechanism is part of the user-centric approach, as it emphasizes usability. This contribution has been an innovation in the authentication of users on a smartphone. In addition, it has paved the way for many works in this field. However, it has some drawbacks. The mechanism implemented proposes only the use of a PIN code or password as an authentication factor. Passwords or PIN codes are vulnerable to several attacks (e.g. brute force).

The CASSH project uses a mechanism to assess the level of trust in addition to context-awareness. Like the CASA solution, it uses traditional authentication factors (login/password). This contribution has two benefits. Firstly, it assesses the risk of a context by leveraging the level of trust in this context. Based on that, it dynamically enforces an adequate authentication technique. Secondly, this solution has good performances in smart homes applications authentication. Nevertheless, the scheme is vulnerable to password guessing attacks. Most users choose short passwords that are easy to guess (a parent's birthday, etc.) and easy to crack.

The user authentication mechanisms proposed in the MCIASIoTE, CBSPHIoT, DCASTBISPF projects are not context-aware. The context-awareness of the ECSA project mechanism has not been implemented and evaluated.

Furthermore, strong and reliable authentication of IoT devices to the IoT system is necessary to ensure that the devices connected to the system are trustworthy devices. To do this, each device needs a unique identity that allows it to be authenticated during exchanges with the system and that must use one or more authentication factors. Apart from the DCASTBISPF and CBSPHIoT projects, none of the studied projects implemented a mechanism for device authentication. However, the authentication mechanisms of the devices implemented in the DCASTBISPF and CBSPHIoT projects are not context-aware. Nevertheless, unlike the CBSPHIoT project, the mechanism used in the DCASTBISPF project has been implemented and evaluated. However, the mechanisms implemented have not been described. In addition, we note the lack of detail regarding the management of device identification.

5.3.1.2 Research directions

User authentication in IoT applications was the most addressed security service in the studied projects. The CASA and CASSH projects focused on the issue of the trade-off be-

Table 4 Comparison of work that has proposed context-aware authentication mechanisms in IoT

Projects	Contributions	Limits
CASA (Hayashi et al., 2013)	• Context-aware mobile phone authentication • User-friendly	• Lack of several strong authentication methods (e. g. double factor, triple factor) • Lack of device authentication
CASSH (Ashibani et al., 2017)	• Context-aware authentication on smart home application. • User-friendly	• Lack of object authentication • Proposed authentication mechanisms not described
ECSA (de Matos et al., 2018b)	• Adaptive authentication	• Lack of details on authentication mechanisms and methods used for user and device authentication • Lack of device authentication • Not evaluated

tween security (application authentication) and usability. It must be noted that the answer to this problem is not insignificant in the adoption of the IoT by a large public. However, the context-aware authentication mechanisms proposed in these projects are vulnerable to attacks that threaten the context-awareness management of the different solutions. As noted in subsection 5.1.2, research is needed to address these issues.

Furthermore, these context-aware authentication mechanisms are vulnerable to several known attacks against authentication systems. This is because, regardless of the user's context, authentication with a single factor (PIN code or password) is used. Thus, research must be conducted to find authentication mechanisms, which can implement, depending on the context, the appropriate authentication method, i.e., simple (with a single factor) in a low-risk environment, or strong (with several factors: fingerprint, facial recognition, etc. in addition to a strong password) in a hostile environment with a high risk of attack. Some smart city IoT applications cited in this paper often have several other users in addition to the main user, such as spouses, children or other relatives. In this context, research must be conducted to place greater emphasis on the ability of the user to easily add or remove the people they want. This will have to be done by allowing him to define who can authenticate himself on the application, how he should authenticate himself and in which context.

Despite the mechanisms proposed in the studied projects, much remains to be done for device authentication in smart city IoT applications. The research to be conducted on this point should cover the following areas. First, the development of authentication mechanisms based on lightweight cryptographic protocols, the use of digital certificates, or a combination of both, depending on the user's context. This prevents cloning, intrusion and replacement by illegitimate devices. For example, in (Claeys et al., 2017), authors proposed a new authentication technique based on OAuth1.0a and ACE (Authentication and Authorization for Constrained Environments). In this solution, a cryptographic protocol EDHOC (Ephemeral Diffie Hellman over Cose (Concise Object Signing and Encryption (Bormann and Hoffman, 2013; Schaad, 2016)) (Selander et al., 2016) is used for authentication.

The second axis concerns the renewal of session keys, depending on the context. In-

deed, in general, when an IoT device is authenticated, a session key is assigned to it for an indefinite period of time. However, some attacks allow sensitive information such as cryptographic keys to be recovered from compromised devices: session key, public key, private key. The renewal of the session key makes it possible to mitigate the reuse of keys, and thus to prevent a compromised object from authenticating itself on the system.

The third axis of research concerns the physical security and trusted execution environment (TEE) of IoT devices. Physical security mitigates the attacks on the extraction of sensitive information highlighted above. In the industry, several proposals have been made to this effect. For example, we have Intel Software Gard Extension (SGX) embedded in some Intel processors, and ARM's CryptoIsland-300P and Cortex-M35P processors (Ukil et al., 2011; Shepherd et al., 2016; Guan et al., 2017). However, these solutions are proprietary. Moreover, this last research axis is also applicable to confidentiality. Indeed, confidentiality implementation mechanisms should be done into secured physical devices to prevent several attacks highlighted in subsection 2.3.2.

5.3.2 Access control

Controlling access to resources is the step that follows authentication. This subject has been well discussed in studied projects. In the following, a detailed comparison of the studied projects in terms of context-aware access control mechanisms proposed or implemented will be provided. Some research direction for context-aware access control will be identified.

5.3.2.1 Critical analysis of the studied projects

Most of the studied projects proposed or implemented a context-aware access control mechanism. Table 5 provides a comparison of these works.

Access control ensures that only legitimate entities (users, applications and services) have access to device resources and data. Therefore, an effective and context-aware access control mechanism is essential for the implementation of effective security in the aforementioned applications. In the CASSH and ECSA projects, an access control mechanism is announced. However, no details are provided about the used access control technique and its evaluation. This can be explained by the fact that the authors of CASSH project focused on the implementation of context-aware authentication on the one hand, and the authors of ECSA project, on the other hand, were based on context-aware security management.

In the CASFMA project, the proposed mechanism allows, depending on the user's context, to control mobile application access to mobile network resources. It was described by the authors as opposed to CASSH project solution. The advantage of MCIASIoTE solution is that user can manage authorization. However, this solution has some drawbacks. The authors did not provide a mechanism that enables dynamic authorizations management (assign or revoke authorizations) as required in an IoT environment. Moreover, this solution has not been evaluated.

Compared to the two previous projects, the mechanism proposed in the MCIASIoTE project is much more suitable for the IoT, as it allows authorizations to be managed through the use of contextual authorization tokens.

The advantage of the mechanism proposed in the CBSPHIoT project over the previous ones is the possibility of defining authorizations with high granularity. Indeed, it takes advantage of role-based access control. In the DCASTBISPF project, the authors used policy-based management to define a mechanism based on the use of contextual access rules. These rules are in the form of Access Control Lists (ACLs). The advantage of this

Table 5 Comparison of work that has proposed context-aware access control mechanisms in IoT

Projects	Contributions	Limits
CASFMA (Mowafi et al., 2014)	• Context-aware control of mobile applications opening	• The control mechanism is for informational purposes only does not prevent the user from opening applications. • Does not control UDP connections • Insufficient for optimal access control
MCIASIoTE (Ramos et al., 2015)	• Authorization token for context-aware access control	• Lack of dynamism in the allocation and revocation of contextual authorization tokens • Not evaluated
DCASTBISPF (Neisse et al., 2015a)	• Dynamic context-aware access control	• Complex ACL management • Not scalable
ECSA (de Matos et al., 2018b)	• Contextual access control security rules	• Lack of details on the mechanisms and techniques used • Not user-centric • Not evaluated
CBSPHIoT (Alagar et al., 2018)	• Context-Aware Role-based access control	• Lack of dynamism in the allocation and revocation of contextual authorization tokens • Not user-centric • Not evaluated

scheme is the simplicity of defining access control list element. Unlike the MCIASIoTE and CBSPHIoT projects, the mechanism proposed in the DCASTBISPF project is adapted to smart city applications and has been implemented. In this sense, a graphical user interface allows the user to define the different authorizations. Nevertheless, the use of ACLs can be problematic, as they require much computing resources for IoT devices. In addition, they do not allow dynamic authorization management.

5.3.2.2 Research directions

Access control is an essential service in security and privacy protection in the IoT. Indeed, it allows defining a granularity of access level to user information and device resources. The mechanisms implementing context-aware access control are present in most of the studied projects. Despite the proposed solutions, much remains to be done in the implementation of context-aware access control in smart city IoT applications.

As a first step, research should be conducted to better implement. mechanisms that enable the user to define his preferences and this with high granularity. These mechanisms must also preserve privacy and be appropriate for low-resource IoT devices. With regard to

adequate access control mechanisms for IoT devices, several proposals were made, including access control based on cryptography. Several variants of these mechanisms have been implemented and have proven their effectiveness. For example, in (Claeys et al., 2017), a token-based secure access control system is implemented. The main advantage of such a system is that it can be used in unsecured network environments.

Secondly, research must be carried out on the awareness of these mechanisms to the context. For example, it may be possible to define contextual authorization tokens as proposed in the MCIASIoTE project but based on the solution implemented in (Claeys et al., 2017). Indeed, unlike the mechanism proposed in the MCIASIoTE project, the mechanism proposed in (Claeys et al., 2017) is based on ACE (Shaad et al., 2018) and OAuth2 and does not require a secure connection for token management. However, this mechanism does not enable the user to have the ability to define and manage permissions. Moreover, it should be noted that the use of contextual authorization tokens could solve the problem of ACL complexity raised in the DCASTBISPF project.

Thirdly, research should be conducted to propose mechanisms that will allow the user to assign or revoke contextual authorizations on the fly. Then, the availability of these tokens to the receiving entities could be carried out safely and in a distributed manner using distributed registers such as the blockchain (Dorri et al., 2017; Alkurdi et al., 2018; Zheng et al., 2018; junaid jami Gul et al., 2019; Paillisse et al., 2019). Indeed, the blockchain will allow the user to remain anonymous while ensuring the confidence that only the entities for which the tokens are intended will be able to use them.

Finally, research must also focus on scaling up the solutions that will be proposed. This will allow the solution to be effective a user's devices number increases.

5.4 Communication security

When creating threat models for the IoT, attackers target network communication channels first. This targeting is due to the many vulnerabilities present in the different layers of the architecture. As a result, communications will have to be secured to counter attacks that threaten the system and applications. Communication security includes the confidentiality and integrity of data as well as the authentication of their origin. The studied projects have addressed little or no communication security. This security is very important when sensitive data flows between different devices, equipment, actors and storage locations. Table 6 compares the studied projects in terms of securing communications in a context-aware way.

5.4.1 Confidentiality

Confidentiality is essential to ensure the safe transmission of data and contributes to the protection of privacy in the IoT when private or identity-related data are transmitted.

5.4.1.1 Critical analysis of the studied projects

The confidentiality of communications was very poorly addressed in the studied projects. Apart from the CBSPHIoT and MCIASIoTE projects, confidentiality was not addressed in any of the other studied projects. In the CBSPHIoT project, the authors proposed the use of the IEEE 802.15.6 standard to ensure the confidentiality of data transmitted outside the sensors (IEEE, 2012; Kwak et al., 2010; Salehi et al., 2016; Ullah et al., 2013). This standard is used in Wireless Body Area Network (WBAN) communications. The range of WBAN communications is limited to the carrier's body, in this case to a gateway very close

Table 6 Comparison of work that has proposed mechanisms to ensure communication security in IoT

Projects	Contributions	Limits
MCIASIoTE (Ramos et al., 2015)	• Confidentiality of transmission in a WBAN network	• Confidentiality does not extend beyond the WBAN network • Confidentiality of communications is not end-to-end and is not context-aware • Not evaluated
CBSPHIoT (Alagar et al., 2018)	• Confidentiality of Internet communications by tunnelling	• The confidentiality of communications is not end-to-end and is not context-aware. • Not evaluated

to the person carrying devices.

The CBSPHIoT scheme main advantage is the implementation of patients' data confidentiality. Nevertheless, it has some limits. On the one hand, the limitation of such an approach is that data confidentiality is not ensured at the level of network, transport or application protocols as WBAN network is limited to the carrier's body. On the other hand, extra-WBAN communications will not be confidential. However, the confidentiality of communications will have to be ensured between the communication endpoints, i.e., end-to-end confidentiality. As a result, the CBSPHIoT project proposal is insufficient.

The architecture proposed in the MCIASIoTE project is based on the IoT-A ARM components. Indeed, IoT-A ARM architecture proposed an end-to-end communication security scheme which uses tunnelling system. The advantage of this scheme is the use of Virtual Private Network (VPN). Compared to the CBSPHIoT project, this scheme offers a better solution, which consists in ensuring end-to-end confidentiality with the tunnel concept (Bassi et al., 2013). However, although this solution may be safe, it is not always feasible due to the limited energy and computational resources of IoT devices.

5.4.1.2 Research directions

Despite the importance of communications confidentiality threats, it has not been given priority in the studied projects. The lack of confidentiality of communications in the IoT exposes users' data to attacks from the Internet and also from local networks. On the other hand, context-aware communications confidentiality has not been addressed in the studied projects. The research to be carried out on this service in order to ensure secure communications in IoT networks and applications should cover the following areas.

The first focus is on implementing robust wireless communication protocols for IoT devices to eliminate vulnerabilities (Zhang et al., 2017). These protocols should use lightweight, efficient cryptographic systems adapted to IoT devices to ensure the confidentiality of data exchanged in wireless networks. For example, among the cryptosystems available for IoT, Elliptic Curve Cryptography (ECC) takes the lead due to the security provided and its low resource consumption (Dubois, 18.03.18).

In the near future, quantum computers will be able to break public-key cryptography schemes (e.g ECC). Therefore, researches should be done to mitigate this threat in IoT by

proposing lightweight post-quantum schemes and research efforts like (Cheng et al., 2017; Guneysu and Oder, 2017; Liu et al., 2018) must continue.

In smart city IoT applications, some devices use a gateway to communicate over the Internet while others can communicate directly over the Internet. However, these communications can pass through several networks and are thus exposed to several attacks. That is why the second axis focuses on implementing context-aware data confidentiality in these communications. Some work has tried to find a solution to this problem. For example, in (Granjal et al., 2014; Wang and Mu, 2017; Glissa and Meddeb, 2019), the various authors drew inspiration from the IPSec protocol by proposing protocols similar to the VPN (Virtual Private Network), i.e., implementing communication confidentiality at the network layer level. However, the implementation of these protocols is not context-aware.

Another solution is security at the payload level of the application layer message. Given the limited resources of many devices, the use of lightweight encryption protocol and cryptographic signature mechanism to encrypt and sign application layer messages can allow these devices to communicate over unsecured networks. For example, in OSCAR (Vučinić et al., 2015), the authors proposed a mechanism for sending and receiving encrypted CoAP data packets over an unsecured network. However, the solution is based on the use of a trusted server. In (Alphand et al., 2018), the authors used OSCAR as a basis for proposing IoTChain, unlike OSCAR, trust is decentralized and managed by the Blockchain. However, the implementation of these solutions are not context-aware.

As previously described, in a smart city, the inhabitants (users) are mobile. This results in a frequent change of network used for communications. Indeed, a mechanism to ensure the confidentiality of communications in a local network (home/business) is no longer sufficient as soon as communications pass through a public network (café, airport, etc.). This is why the third axis should focus on the sensitivity of communication confidentiality to the context. Thus, depending on the user's context and risks, a confidential communication channel could be established.

5.4.2 Data integrity and authentication of data origin

The security of communication requires the implementation of mechanisms to verify the integrity and origin of data. In the following subsections, we will provide a detailed comparison of the studied projects in terms of proposed or implemented integrity mechanisms. We will also compare these projects in terms of proposed mechanisms for verifying the authentication of data origin. Then we identify a number of research tasks to be carried out to ensure data integrity and origin authentication when communicating in the IoT.

5.4.2.1 Critical analysis of the studied projects

Data integrity ensures that the data has not been altered during the exchanges, i.e. that the recipient has received the data sent by the sender without alteration. Apart from the CBSPHIoT project, none of the studied projects proposed or implemented mechanisms to ensure data integrity during communications. This is due to the fact that most projects focused on the implementation of one context-aware security service. In the CBSPHIoT project, the authors propose the use of the IEEE 802.15.6 standard to ensure the integrity of the data exchanged within the WBAN (IEEE, 2012). WBANs represent only a fraction of the networks used among smart city IoT applications. Thus, the proposed solution in CBSPHIoT project, i.e IEEE 802.15.6 is very limited.

Data authentication ensures the authenticity of the origin of the data received. However,

this security service was not addressed in the studied projects. This is due to the fact that most of these projects do not take into account the communications security.

5.4.2.2 Research directions

Data integrity and authentication mechanisms are essential for enabling secure communications. Generally, protocols deployed to ensure data confidentiality also ensure data integrity and verify the authenticity of data origins. For example, the IEEE 802.15.4 standard ensures data integrity and confidentiality through the following mechanisms: AES-CBC-MAC-X, AES-CCM-MAC-X, where X represents 64, 128 or 256 depending on the variant of the encryption suite used.

The proposed mechanisms so far in the studied projects to ensure data integrity and authentication only concern the data link layer. These services will have to be provided in network layer communications. Mechanisms to ensure data integrity and authentication are included in the IPv6 protocol specifications (Deering and Hinder, 1998). However, they are proposed as extensions and they can be fully implemented to provide IP AH (Authentication Header) and ESP (Encapsulating Security Payload) (Atkinson and Kent, 1998). This requires the establishment of a secure communication tunnel. Since 6LoWPAN is the protocol used for routing packets in the IoT, research will need to be conducted to enable the implementation of mechanisms, for example, those provided in the IPv6 specifications to ensure data integrity and authentication, even in the absence of an IPSec secure communication tunnel. These mechanisms will be implemented by unconstrained IoT objects that generally serve as intermediaries in communications.

Finally, research can be conducted to enable the implementation of mechanisms to ensure data integrity and authentication at the application layer level depending on user context, for instance, when communications are not secured. In the presence of secured communications, i.e., secured context, applications layer payload will stay clear. These mechanisms will have to be adapted to the low-resource IoT devices. Indeed, protecting data at the application layer is a secure and lightweight way to ensure the security of communications in the IoT, even if communications take place over an unsecured network.

5.5 Security of the stored data

Data is a core element of the IoT systems and applications. They need data to be stored before any analytics. So, data security needs to be ensured at the storage level. It can be done by implementing proper confidentiality and integrity mechanisms.

5.5.1 Critical analysis of the studied projects

The security of the stored data has been given very little consideration in the studied projects. It must be ensured at the time of collect, transmission and until storage. Apart from the CBSPHIoT project, none of the studied projects proposed or implemented a mechanism to ensure data security at the storage level.

In the CBSPHIoT project, data is encrypted and stored in the cloud. According to the authors, data encryption is performed using the key pair (PID, DID). The PID (Patient IDentifier) represents the patient's identifier and the DID (Device IDentifier) represents the identifier of the object that is the source of the data.

The benefits of such a scheme are that only the hospital system will be able to decrypt patient's data in a given context (e.g. inside the hospital). However, the authors did not

specify the used encryption system and how the encryption keys were managed. Moreover, the overall system has not been evaluated.

5.5.2 Research directions

Based on the foregoing, a number of tasks remain to be done to ensure the security of the stored data. The mechanisms to be implemented to ensure the security of the stored data must also ensure the integrity and confidentiality of the data. In this context, research will need to be conducted to find robust, effective and less time-consuming and resource-intensive encryption suites to ensure the confidentiality of stored data.

The solutions to be proposed must also ensure the integrity of the data stored by hashing and time-stamping. Current data privacy mechanisms implement crypto-systems such as AES and ECC (Ammar et al., 2018; Goyal and Sahula, 2016; Mahajan and Sachdeva, 2013; Mustafa et al., 2018; Singh et al., 2017). However, the efficient management of encryption/decryption keys remains one of the challenges. Keys are generally hard-coded in different devices. Often these devices do not have a mechanism for updating these keys. In this context, research must be done to allow a secure update of the various cryptographic keys. Research will also be required to ensure the physical security of IoT devices. This will prevent attacks targeting the extraction of cryptographic keys.

Further research must be conducted to allow access to the user's encrypted data without prior decryption. Indeed, it takes a considerable amount of time to decipher large amounts of data. One possible solution is the use of a homomorphic encryption system. Homomorphic encryption is a cryptographic system that allows operations on encrypted data to be performed without prior decryption. Thus, the data will always be in an encrypted state when processed. However, homomorphic encryption is complex to implement and very resource-intensive. Lightweight homomorphic encryption has been proposed in (Baharon et al., 2015) for mobile cloud services. Thus, research must be conducted for homomorphic encryption adapted to the IoT to allow access to encrypted data without prior decryption.

Attribute-Based Encryption is very promising encryption techniques used in a cloud storage environment (Kaaniche and Laurent, 2017). In this sense, research needs to be done for adapting such a technique to IoT device.

5.6 Heterogeneity and Scalability

Heterogeneity and scalability are important characteristics of IoT. In the following subsections, we will make a detailed comparison of the studied projects in terms of heterogeneity support and scaling up. Finally, we will identify a number of research projects that need to be carried out to enable heterogeneity and scalability in smart cities IoT applications.

5.6.1 Critical analysis of the studied projects

The IoT system devices have various communication systems, computing and memory capacities. Among the studied projects, only DCASTBISPF and ECSA considered heterogeneity and scalability.

With regard to heterogeneity, the DCASTBISPF project allows the implementation of a PEP (Policy Enforcement Point) specific to each device group. This allows the solution to support various types of devices. In the ECSA project, the authors also announced the support of heterogeneity. Since the ECSA architecture is focused on context sharing, heterogeneity is managed in the Semantic Manager module. However, the mechanism proposed

in the DCASTBISPF project allows better support of heterogeneity than that of the ECSA project, because the Semantic Manager of the latter only manages context sharing between objects. However, this mechanism does not manage the application of security rules provided in the architecture.

Scalability is one of the challenges for an IoT system, as the number of devices present in the architecture can be very dense (106 devices per km2). Scalability was poorly addressed in the studied projects and was not identified as a criterion to be taken into account.

5.6.2 Research directions

IoT devices number is continuously increasing and according to forecasts, it will reach a number at seven devices per user without industrials and others business devices. Research will need to be conducted to enable scalability in the aforementioned applications while ensuring the same level of security and privacy protection.

Heterogeneity is a fundamental feature that any security architecture in the IoT must support. Research will need to be conducted to address heterogeneity in the implementation of security. Software Defined Networking (SDN) and Network Function Virtualization (NFV) could solve the problem of heterogeneity in application of security rules at the device level (Ojo et al., 2016). Indeed, SDN could be used to enforce security policies. In addition, the distribution/hierarchisation of the SDN architecture should facilitate scalability (Omnes et al., 2015). NFV could allow dynamic service function chaining (SFC) for dynamic network traffic steering in order to allow the security analysis of the traffic (Medhat et al., 2017; Yong Li and Min Chen, 2015; Cheng et al., 2018).

6 Conclusion

IoT is an ubiquitous technology that provides several value-added services in people's daily lives: trade, industry, environmental management, etc. This survey focused on the implementation of context-aware security in smart city IoT applications. Context-awareness is a feature of IoT that can be used to provide efficient and adapted security and privacy protection in smart city IoT applications. The studied projects have the same principle in terms of using context-awareness to provide optimal security in these applications. However, these projects have applied different approaches to the implementation of this principle.

We have conducted a critical review of the solutions/architectures proposed in these projects based on context-awareness management, privacy protection and security services (authentication, access control, confidentiality, integrity, etc.). We have highlighted the challenges to be met and proposed research directions for context-aware security that can benefit from the advantages provided by new network architectures in the smart city's IoT applications. Future research directions have to carefully consider the user's needs and specificities (digital divide, high mobility, usability, etc.) for user-centric security and privacy protection. They must also consider the challenges of security and privacy raised by the evolution of the new network's architectures such as Fog computing, Software Defined Networking, Network Function Virtualization and 5G Network, for anytime and anywhere security and privacy.

References

A. A. Abi Sen, F. A. Eassa, K. Jambi, and M. Yamin. Preserving privacy in internet of things: A survey. *International Journal of Information Technology*, pages 189–200, Feb. 2018.

G. D. Abowd, A. K. Dey, P. J. Brown, N. Davies, M. Smith, and P. Steggles. Towards a Better Understanding of Context and Context-Awareness. In *HUC '99 Proceedings of the 1st International Symposium on Handheld and Ubiquitous Computing*, pages 304–307, Karlsruhe, Germany, 1999. Springer-Verlag. ISBN 3-540-66550-1.

V. Alagar, A. Alsaig, O. Ormandjiva, and K. Wan. Context-Based Security and Privacy for Healthcare IoT. In *2018 IEEE International Conference on Smart Internet of Things (SmartIoT)*, pages 122–128, Xi'an, China, Aug. 2018. IEEE. ISBN 978-1-5386-8543-3. doi: 10.1109/SmartIoT.2018.00-14.

F. Alkurdi, I. Elgendi, K. S. Munasinghe, D. Sharma, and A. Jamalipour. Blockchain in IoT Security: A Survey. In *2018 28th International Telecommunication Networks and Applications Conference (ITNAC)*, pages 1–4, Sydney, NSW, Nov. 2018. IEEE. ISBN 978-1-5386-7177-1. doi: 10.1109/ATNAC.2018.8615409.

O. Alphand, M. Amoretti, T. Claeys, S. Dall'Asta, A. Duda, G. Ferrari, F. Rousseau, B. Tourancheau, L. Veltri, and F. Zanichelli. IoTChain: A blockchain security architecture for the Internet of Things. In *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6, Barcelona, Apr. 2018. IEEE. ISBN 978-1-5386-1734-2. doi: 10.1109/WCNC.2018.8377385.

M. Ammar, G. Russello, and B. Crispo. Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, 38:8–27, Feb. 2018. ISSN 22142126. doi: 10.1016/j.jisa.2017.11.002.

Y. Ashibani, D. Kauling, and Q. H. Mahmoud. A context-aware authentication service for smart homes. In *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pages 588–589, Las Vegas, NV, USA, Jan. 2017. IEEE. ISBN 978-1-5090-6196-9. doi: 10.1109/CCNC.2017.7983179.

R. Atkinson and S. Kent. IP Authentication Header. https://tools.ietf.org/html/rfc2402, Nov. 1998.

L. Atzori, A. Iera, and G. Morabito. The Internet of Things: A survey. *Computer Networks*, 54(15):2787–2805, Oct. 2010. ISSN 13891286. doi: 10.1016/j.comnet.2010.05.010.

M. R. Baharon, Q. Shi, and D. Llewellyn-Jones. A New Lightweight Homomorphic Encryption Scheme for Mobile Cloud Computing. In *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, pages 618–625, LIVERPOOL, United Kingdom, Oct. 2015. IEEE. ISBN 978-1-5090-0154-5. doi: 10.1109/CIT/IUCC/DASC/PICOM.2015.88.

M. Barhamgi, C. Perera, C. Ghedira, and D. Benslimane. User-centric Privacy Engineering for the Internet of Things. *arXiv:1809.00926 [cs]*, Sept. 2018.

A. Bassi, M. Bauer, M. Fiedler, T. Kramp, R. van Kranenburg, S. Lange, and S. Meissner, editors. *Enabling Things to Talk*. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013. ISBN 978-3-642-40402-3 978-3-642-40403-0. doi: 10.1007/978-3-642-40403-0.

J. Bernal Bernabe, J. L. Hernández, M. V. Moreno, and A. F. Skarmeta Gomez. Privacy-Preserving Security Framework for a Social-Aware Internet of Things. In R. Hervás, S. Lee, C. Nugent, and J. Bravo, editors, *Ubiquitous Computing and Ambient Intelligence. Personalisation and User Adapted Services*, volume 8867, pages 408–415. Springer International Publishing, Cham, 2014. ISBN 978-3-319-13101-6 978-3-319-13102-3. doi: 10.1007/978-3-319-13102-3_67.

J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-Policy Attribute-Based Encryption. In *2007 IEEE Symposium on Security and Privacy (SP '07)*, pages 321–334, Berkeley, CA, May 2007. IEEE. ISBN 978-0-7695-2848-9. doi: 10.1109/SP.2007.11.

J. Biron and J. Follett. *Foundational Elements of an IoT Solution*. O'Reilly Media, Inc., United State of America, first edition edition, 2016. ISBN 978-1-4919-5097-5.

T. Borgohain, U. Kumar, and S. Sanyal. Survey of security and privacy issues of internet of things. *arXiv preprint arXiv:1501.02211*, 2015.

C. Bormann and P. Hoffman. Concise Binary Object Representation (CBOR). Technical Report RFC7049, RFC Editor, Oct. 2013.

C. Bormann, M. Ersue, and A. Keranen. Terminology for Constrained-Node Networks. Technical Report RFC7228, RFC Editor, May 2014.

P. Brézillon and G. Mostéfaoui. Context-based security policies: A new modeling approach. In *IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second*, pages 154–158, Orlando, FL, USA, 2004. IEEE. ISBN 978-0-7695-2106-0. doi: 10.1109/PERCOMW.2004.1276923.

C. Cheng, R. Lu, A. Petzoldt, and T. Takagi. Securing the Internet of Things in a Quantum World. *IEEE Communications Magazine*, 55(2):116–120, Feb. 2017. ISSN 0163-6804. doi: 10.1109/MCOM.2017.1600522CM.

H. Cheng, N. Xiong, L. T. Yang, and Y.-S. Jeong. Distributed scheduling algorithms for channel access in TDMA wireless mesh networks. *The Journal of Supercomputing*, 63 (2):407–430, Feb. 2013. ISSN 0920-8542, 1573-0484. doi: 10.1007/s11227-008-0244-7.

Y. Cheng, H. Jiang, F. Wang, Y. Hua, D. Feng, W. Guo, and Y. Wu. Using high-bandwidth networks efficiently for fast graph computation. *IEEE Transactions on Parallel and Distributed Systems*, 30(5):1170–1183, 2018.

T. Claeys, F. Rousseau, and B. Tourancheau. Securing Complex IoT Platforms with Token Based Access Control and Authenticated Key Establishment. In *2017 International Workshop on Secure Internet of Things (SIoT)*, pages 1–9, Oslo, Sept. 2017. IEEE. ISBN 978-1-5386-4541-3. doi: 10.1109/SIoT.2017.00006.

Council and Parliament of European Union. REGULATION (EU) 2016/679, april 2016. `http://data.europa.eu/eli/reg/2016/679/oj/fra` [Accessed:2018-12-11].

D. Darwish. Improved layered architecture for internet of things. *Int. J. Comput. Acad. Res.(IJCAR)*, 4:214–223, 2015.

E. de Matos, R. T. Tiburski, L. A. Amaral, and F. Hessel. Context Interoperability for IoT Through an Edge-Centric Context Sharing Architecture. In *2018 IEEE Symposium on Computers and Communications (ISCC)*, pages 00667–00670, Natal, Brazil, June 2018a. IEEE. ISBN 978-1-5386-6950-1. doi: 10.1109/ISCC.2018.8538491.

E. de Matos, R. T. Tiburski, L. A. Amaral, and F. Hessel. Providing Context-Aware Security for IoT Environments Through Context Sharing Feature. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pages 1711–1715, New York, NY, USA, Aug. 2018b. IEEE. ISBN 978-1-5386-4388-4. doi: 10.1109/TrustCom/BigDataSE.2018.00257.

S. E. Deering and R. Hinder. Internet Protocol, Version 6 (IPv6) Specification, RFC 2460. https://tools.ietf.org/html/rfc2460, Dec. 1998.

B. Di Martino, M. Rak, M. Ficco, A. Esposito, S. Maisto, and S. Nacchia. Internet of things reference architectures, security and interoperability: A survey. *Internet of Things*, 1-2: 99–112, Sept. 2018. ISSN 25426605. doi: 10.1016/j.iot.2018.08.008.

R. Di Pietro, X. Salleras, M. Signorini, and E. Waisbard. A blockchain-based Trust System for the Internet of Things. In *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies - SACMAT '18*, pages 77–83, Indianapolis, Indiana, USA, 2018. ACM Press. ISBN 978-1-4503-5666-4. doi: 10.1145/3205977.3205993.

A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram. Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 618–623, Kona, HI, Mar. 2017. IEEE. ISBN 978-1-5090-4338-5. doi: 10.1109/PERCOMW.2017.7917634.

C. Dubois. MIT's Encryption Chip Reduces Public-Key Encryption Power Consumption by 99.75%. https://www.allaboutcircuits.com/news/energy-efficient-public-key-encryption-chip-solve-iot-security-problems/ [Accessed:2018-09-23], 18.03.18.

Ericsson. Internet of Things forecast – Ericsson Mobility Report. https://www.ericsson.com/en/mobility-report/internet-of-things-forecast [Accessed: 2019-02-06], 2019.

O. Garcia-Morchon, S. Kumar, and M. Sethi. State-of-the-Art and Challenges for the Internet of Things Security. https://tools.ietf.org/id/draft-irtf-t2trg-iot-seccons-13.html, Apr. 2018.

G. Glissa and A. Meddeb. 6LowPSec: An end-to-end security protocol for 6LoWPAN. *Ad Hoc Networks*, 82:100–112, Jan. 2019. ISSN 15708705. doi: 10.1016/j.adhoc.2018.01.013.

T. K. Goyal and V. Sahula. Lightweight security algorithm for low power IoT devices. In *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pages 1725–1729, Jaipur, India, Sept. 2016. IEEE. ISBN 978-1-5090-2029-4. doi: 10.1109/ICACCI.2016.7732296.

J. Granjal, E. Monteiro, and J. S. Silva. Network-layer security for the Internet of Things using TinyOS and BLIP: Network-Layer Security For The IoT using TinyOS and BLIP. *International Journal of Communication Systems*, 27(10):1938–1963, Oct. 2014. ISSN 10745351. doi: 10.1002/dac.2444.

L. Guan, P. Liu, X. Xing, X. Ge, S. Zhang, M. Yu, and T. Jaeger. Trustshadow: Secure execution of unmodified applications with arm trustzone. In *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services*, pages 488–501. ACM, 2017.

J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29 (7):1645–1660, Sept. 2013. ISSN 0167739X. doi: 10.1016/j.future.2013.01.010.

T. Guneysu and T. Oder. Towards lightweight Identity-Based Encryption for the post-quantum-secure Internet of Things. In *2017 18th International Symposium on Quality Electronic Design (ISQED)*, pages 319–324, Santa Clara, CA, USA, Mar. 2017. IEEE. ISBN 978-1-5090-5404-6. doi: 10.1109/ISQED.2017.7918335.

W. Guo, J. Li, G. Chen, Y. Niu, and C. Chen. A PSO-Optimized Real-Time Fault-Tolerant Task Allocation Algorithm in Wireless Sensor Networks. *IEEE Transactions on Parallel and Distributed Systems*, 26(12):3236–3249, Dec. 2015. ISSN 1045-9219. doi: 10.1109/TPDS.2014.2386343.

E. Hayashi, S. Das, S. Amini, J. Hong, and I. Oakley. CASA: Context-aware scalable authentication. In *Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS '13*, page 1, Newcastle, United Kingdom, 2013. ACM Press. ISBN 978-1-4503-2319-2. doi: 10.1145/2501604.2501607.

IEEE. IEEE 802.15.6-2012 - IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks. https://standards.ieee.org/standard/802_15_6-2012.html, Feb. 2012.

J. ISO/IEC. Internet of Things (IoT), Preliminary report. https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/internet_of_things_report-jtc1.pdf [Accessed:2019-02-08], 2014.

ITU. ITU-T Recommendation Y.4000/Y.2060. https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060 [Accessed=2019-02-07], June 2012.

M. junaid jami Gul, A. Paul, A. Ahmad, M. Khan, and G. Jeon. Smart contract's interface for user centric business model in blockchain. In *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing - SAC '19*, pages 709–714, Limassol, Cyprus, 2019. ACM Press. ISBN 978-1-4503-5933-7. doi: 10.1145/3297280.3297347.

N. Kaaniche and M. Laurent. Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms. *Computer Communications*, 111: 120–141, Oct. 2017. ISSN 01403664. doi: 10.1016/j.comcom.2017.07.006.

A. Khan, A. Al-Zahrani, S. Al-Harbi, S. Al-Nashri, and I. A. Khan. Design of an IoT smart home system. In *2018 15th Learning and Technology Conference (L&T)*, pages 1–5, Jeddah, Feb. 2018. IEEE. ISBN 978-1-5386-4817-9. doi: 10.1109/LT.2018.8368484.

J. S. Kumar and D. R. Patel. A survey on internet of things: Security and privacy issues. *International Journal of Computer Applications*, 90(11), 2014.

K. S. Kwak, S. Ullah, and N. Ullah. An Overview of IEEE 802.15.6 Standard. *2010 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL 2010)*, pages 1–6, Nov. 2010. doi: 10.1109/ISABEL.2010.5702867.

W.-H. Lee, C. Liu, S. Ji, P. Mittal, and R. Lee. Quantification of De-anonymization Risks in Social Networks:. In *Proceedings of the 3rd International Conference on Information Systems Security and Privacy*, pages 126–135, Porto, Portugal, 2017. SCITEPRESS - Science and Technology Publications. ISBN 978-989-758-209-7. doi: 10.5220/0006192501260135.

S. Li, L. D. Xu, and I. Romdhani. *Securing the Internet of Things*. Syngress, Cambridge, MA, 2017. ISBN 978-0-12-804458-2. OCLC: ocn972324781.

S.-W. Lin, B. Miller, a. Durand, G. Bleakley, A. Chigani, R. Martin, B. Murphy, and M. Crawford. The Industrial Internet of ThingsVolume G1: Reference Architecture. Technical Report IIC:PUB:G1:V1.80:20170131, IIC, 2017.

Z. Liu, K.-K. R. Choo, and J. Grossschadl. Securing Edge Devices in the Post-Quantum Internet of Things Using Lattice-Based Cryptography. *IEEE Communications Magazine*, 56(2):158–162, Feb. 2018. ISSN 0163-6804. doi: 10.1109/MCOM.2018.1700330.

P. Mahajan and A. Sachdeva. A Study of Encryption Algorithms AES, DES and RSA for Security. *Global Journal of Computer Science and Technology*, 2013. ISSN 0975-4172.

A. M. Medhat, T. Taleb, A. Elmangoush, G. A. Carella, S. Covaci, and T. Magedanz. Service Function Chaining in Next Generation Networks: State of the Art and Research Challenges. *IEEE Communications Magazine*, 55(2):216–223, Feb. 2017. ISSN 0163-6804. doi: 10.1109/MCOM.2016.1600219RP.

R. Mehta, J. Sahni, and K. Khanna. Internet of Things: Vision, Applications and Challenges. *Procedia Computer Science*, 132:1263–1269, 2018. ISSN 18770509. doi: 10.1016/j.procs.2018.05.042.

Y. Mowafi, D. Abou-Tair, T. Al-Aqarbeh, M. Abilov, V. Dmitriyev, and J. M. Gomez. A Context-aware Adaptive Security Framework for Mobile Applications. In *Proceedings of the 3rd International Conference on Context-Aware Systems and Applications*, Dubai, United Arab Emirates, 2014. ICST. ISBN 978-1-63190-005-1. doi: 10.4108/icst.iccasa.2014.257495.

G. Mustafa, R. Ashraf, M. A. Mirza, A. Jamil, and Muhammad. A review of data security and cryptographic techniques in IoT based devices. In *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems - ICFNDS '18*, pages 1–9, Amman, Jordan, 2018. ACM Press. ISBN 978-1-4503-6428-7. doi: 10.1145/3231053.3231100.

R. Neisse, G. Steri, G. Baldini, E. Tragos, I. N. Fovino, and M. Botterman. Dynamic Context-Aware Scalable and Trust-based IoT Security, Privacy Framework. In *Internet of Things - From Research and Innovation to Market Deployment*, River Publishers Series in Communication, pages 199 – 224. River Publishers, 2015a. ISBN 978-87-93102-95-8.

R. Neisse, G. Steri, I. N. Fovino, and G. Baldini. SecKit: A Model-based Security Toolkit for the Internet of Things. *Computers & Security*, 54:60–76, Oct. 2015b. ISSN 01674048. doi: 10.1016/j.cose.2015.06.002.

M. Ojo, D. Adami, and S. Giordano. A SDN-IoT Architecture with NFV Implementation. In *2016 IEEE Globecom Workshops (GC Wkshps)*, pages 1–6, Dec. 2016. doi: 10.1109/GLOCOMW.2016.7848825.

N. Omnes, M. Bouillon, G. Fromentoux, and O. Grand. A programmable and virtualized network & IT infrastructure for the internet of things: How can NFV & SDN help for facing the upcoming challenges. In *2015 18th International Conference on Intelligence in Next Generation Networks*, pages 64–69, Paris, France, 2015. IEEE. ISBN 978-1-4799-1866-9. doi: 10.1109/ICIN.2015.7073808.

A. Oracevic, S. Dilek, and S. Ozdemir. Security in internet of things: A survey. In *2017 International Symposium on Networks, Computers and Communications (ISNCC)*, pages 1–6, Marrakech, Morocco, May 2017. IEEE. ISBN 978-1-5090-4260-9. doi: 10.1109/ISNCC.2017.8072001.

J. Paillisse, J. Subira, A. Lopez, A. Rodriguez-Natal, V. Ermagan, F. Maino, and A. Cabellos. Distributed Access Control with Blockchain. *arXiv:1901.03568 [cs]*, Jan. 2019.

J. L. H. Ramos, J. B. Bernabe, and A. F. Skarmeta. Managing Context Information for Adaptive Security in IoT Environments. In *2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops*, pages 676–681, Gwangiu, South Korea, Mar. 2015. IEEE. ISBN 978-1-4799-1775-4. doi: 10.1109/WAINA.2015.55.

K. M. Sadique, R. Rahmani, and P. Johannesson. Towards security on internet of things: Applications and challenges in technology. *Procedia Computer Science*, 141:199–206, 2018.

S. A. Salehi, M. A. Razzaque, I. Tomeo-Reyes, and N. Hussain. IEEE 802.15.6 standard in wireless body area networks from a healthcare point of view. In *2016 22nd Asia-Pacific Conference on Communications (APCC)*, pages 523–528, Yogyakarta, Indonesia, Aug. 2016. IEEE. ISBN 978-1-5090-0676-2. doi: 10.1109/APCC.2016.7581523.

J. Schaad. CBOR Object Signing and Encryption (COSE). https://cose-wg.github.io/cose-spec/, Nov. 2016.

M. Scherling, A.-N. Huynh, M. Carlson, J. Strassner, S. Waldbusser, S. Herzog, A. Westerinen, J. Perry, B. Quinn, and J. Schnizlein. Terminology for Policy-Based Management. https://tools.ietf.org/html/rfc3198#page-17, Nov. 2001.

G. Selander, J. Mattsson, and F. Palombini. Object Security of CoAP (OSCOAP). https://tools.ietf.org/html/draft-ietf-core-object-security-00, Oct. 2016.

J. Shaad, R. Danyliw, and B. Kaduk. Authentication and Authorization for Constrained Environments (ace) -. https://datatracker.ietf.org/wg/ace/about/, Mar. 2018.

C. Shepherd, G. Arfaoui, I. Gurulian, R. P. Lee, K. Markantonakis, R. N. Akram, D. Sauveron, and E. Conchon. Secure and trusted execution: Past, present, and future-a critical review in the context of the internet of things and cyber-physical systems. In *2016 IEEE Trustcom/BigDataSE/ISPA*, pages 168–177. IEEE, 2016.

D. Singh, G. Tripathi, and A. J. Jara. A survey of Internet-of-Things: Future vision, architecture, challenges and services. In *2014 IEEE World Forum on Internet of Things (WF-IoT)*, pages 287–292, Seoul, Korea (South), Mar. 2014. IEEE. ISBN 978-1-4799-3459-1. doi: 10.1109/WF-IoT.2014.6803174.

M. Singh, M. Rajan, V. Shivraj, and P. Balamuralidhar. Secure MQTT for Internet of Things (IoT). In *2015 Fifth International Conference on Communication Systems and Network Technologies*, pages 746–751, Gwalior, India, Apr. 2015. IEEE. ISBN 978-1-4799-1797-6. doi: 10.1109/CSNT.2015.16.

S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park. Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing*, May 2017. doi: 10.1007/s12652-017-0494-4.

F. Staff. Internet of Things : Privacy and Security in a Connected World. Technical report, Federal Trade Commission, Jan. 2015.

O. Svet. IoT: User-Centric, Privacy Security - DZone IoT. https://dzone.com/articles/iot-user-centric-privacy-security [Accessed: 2019-02-26], Feb. 2019.

I. Torre, F. Koceva, O. R. Sanchez, and G. Adorni. A framework for personal data protection in the IoT. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 384–391, Barcelona, Spain, Dec. 2016. IEEE. ISBN 978-1-908320-73-5. doi: 10.1109/ICITST.2016.7856735.

A. Ukil, J. Sen, and S. Koilakonda. Embedded security for internet of things. In *2011 2nd National Conference on Emerging Trends and Applications in Computer Science*, pages 1–6. IEEE, 2011.

S. Ullah, M. Mohaisen, and M. A. Alnuem. A Review of IEEE 802.15.6 MAC, PHY, and Security Specifications. *International Journal of Distributed Sensor Networks*, 9(4): 950704, Apr. 2013. ISSN 1550-1477, 1550-1477. doi: 10.1155/2013/950704.

M. Vučinić, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti. OSCAR: Object security architecture for the Internet of Things. *Ad Hoc Networks*, 32:3–16, Sept. 2015. ISSN 15708705. doi: 10.1016/j.adhoc.2014.12.005.

X. Wang and Y. Mu. Communication security and privacy support in 6LoWPAN. *Journal of Information Security and Applications*, 34:108–119, June 2017. ISSN 22142126. doi: 10.1016/j.jisa.2017.02.003.

N. Woolf. DDoS attack that disrupted internet was largest of its kind in history, experts say, Oct. 2016.

X. Yao, Z. Chen, and Y. Tian. A lightweight attribute-based encryption scheme for the Internet of Things. *Future Generation Computer Systems*, 49:104–112, Aug. 2015. ISSN 0167739X. doi: 10.1016/j.future.2014.10.010.

Yong Li and Min Chen. Software-Defined Network Function Virtualization: A Survey. *IEEE Access*, 3:2542–2553, 2015. ISSN 2169-3536. doi: 10.1109/ACCESS.2015.2499271.

K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen. Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Communications Magazine*, 55(1): 122–129, Jan. 2017. ISSN 0163-6804. doi: 10.1109/MCOM.2017.1600267CM.

Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang. Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14(4):352, 2018. ISSN 1741-1106, 1741-1114. doi: 10.1504/IJWGS.2018.095647.