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

Everton de Matos[1], Eduardo Viegas[1], Ramão Tiburski[2], and Fabiano Hessel[3]

[1] Technology Innovation Institute, Abu Dhabi, UAE
{everton.dematos,eduardo.viegas}@tii.ae
[2] Federal Institute of Education Science and Technology of Santa Catarina, Brazil
ramao.tiburski@ifsc.edu.br
[3] Pontifical Catholic University of Rio Grande do Sul (PUCRS), Porto Alegre, Brazil
fabiano.hessel@pucrs.br

Abstract. Security and privacy are hot topics when considering the Internet of Things (IoT) application scenarios. By dealing with sensitive and sometimes personal data, IoT application environments need mechanisms to protect against different threats. The traditional security mechanisms are usually static and were not designed considering the dynamism imposed by IoT environments. Those environments could have mobile and dynamic entities that can change their status at deployment time, needing novel security mechanisms to cope with their requirements. Thus a non-static approach to security provision becomes mandatory. Context-Aware Security (CAS) is a mechanism to provide dynamic security for those environments. CAS solutions can adapt the security service (e.g., authentication, authorization, access control, and privacy-preserving) provision based on the context of the environment. This work reviews the concepts around CAS and presents an extensive review of existing solutions employing CAS in their architecture. Moreover, we define a taxonomy for CAS based on the context-awareness area.

1 Introduction

The Internet of Things (IoT) has gained significant attention in academia and industry. By embedding mobile networking and information processing capability into a wide array of gadgets and everyday items, the Internet of Things has added new dimensions to the world of information and communication technology [6]. The global IoT Security Product market is estimated to grow from USD 12 Bn in 2017 to USD 48 Bn by 2027 [8], leading us to believe that efforts to provide novel security solutions for IoT environments will be needed by the market.

The traditional security mechanism usually provides static and non-aware security services. Considering the high dynamism of IoT scenarios, Context-Aware Security (CAS) appears as a suitable mechanism to provide dynamic security to IoT environments, as many recent works have been proposed in this regard

[21][18]. CAS uses context information to provide security. Context information can be considered any high-level (i.e., human-readable) information that characterizes an entity [19]. As the context of an entity (i.e., device, user, network) may change on the fly in IoT environments, it is crucial to care about those changes when providing security services.

The present work aims to shed light on CAS solutions for IoT environments. We present definitions of CAS, considering the four main security services that it can provide: (i) authentication, (ii) authorization, (iii) access control, and (iv) privacy-preserving. We also introduce a novel taxonomy based on the well-established context-awareness area to classify the CAS solutions. Moreover, we review recent works that employ CAS in their architecture. The review considers the possible security services provided by the works and also the requirements to provide CAS.

Recent works have extensively discussed and reviewed the available solutions in the context-aware domain, but just a few discuss the challenges in the CAS area [21][19]. Grimm et al. [11] present a survey on CAS for vehicles and fleets through a detailed analysis of the context information relevant to future vehicle security. Sylla et al. [26] conduct a survey of the CAS solutions that have been proposed for smart city IoT applications. In light of this, the present work shows its novelty by providing an extensible review of CAS characteristics and requirements, introducing a novel taxonomy for CAS, and analyzing a significant amount of CAS solutions considering different application areas.

The remainder of the paper is structured as follows: Section 2 presents an overview of CAS concepts. Section 3 presents a taxonomy on CAS. Section 4 presents the requirements of CAS solutions. Section 5 introduces available solutions for CAS. Section 6 presents a discussion on CAS solutions. Finally, Section 7 concludes the paper.

2 Context-Aware Security

Traditionally, security requirements are assumed to be relatively static since security decisions do not change with context, nor do they account for changing conditions in the environment [2]. However, the use of context information to provide security decisions is a key feature to mitigate some security problems [19][29]. The CAS does not remove the need for traditional security mechanisms. It adds a layer of security and privacy, focusing on the dynamism of such IoT environments.

The Context-Aware Security (CAS) is defined by Mostéfaoui, and Brézillon [7][20] as: "*a set of information collected from the user's environment and the application environment and that is relevant to the security infrastructure of both the user and the application.*" Also, CAS can be defined as a situation where a security solution considers a set of information (context) while making a specific security decision. For example, while detecting an intrusion during communication, the security mechanisms may adapt to a strong authentication method. The context-unaware mechanisms can be inadequate for the Internet of

Things due to its dynamic and heterogeneous environment. Context information can be used to reconfigure security mechanisms and adjust security parameters. The contextual information can be integrated into various security mechanisms such as authentication, access control, encryption, etc. [13].

While the notion of context awareness has been well spread through the scientific community [1], currently, there is a lack of security and privacy-preserving mechanisms that take into account dynamic context conditions for the IoT [24][19]. For the implementation of CAS in IoT environments, four main security services can be provided: (i) authentication, (ii) authorization, (iii) access control, and (iv) privacy-preserving. The next items present an overview of each security service [2][13][29].

Authentication: Traditional authentication methods require much user interaction in the form of manual log-ins, logouts, and file permissions. Today, passwords are the most common form of authentication. However, passwords are also a major source of vulnerabilities, as they are often easy to guess, re-used, forgotten, shared with others, and susceptible to social engineering. Moreover, well-known authentication technologies, such as face recognition, iris scanner, and biometric technology, can be used. Besides those examples of technologies, context information strengthens the authentication process by providing a second-factor authentication.

Authorization and Access Control: Allow means granting access when the user or device credential matches with pre-stored credentials, and deny means blocking access when the user or device credential does not match with pre-stored credentials. This type of system can be considered static in nature because it does not take into consideration other factors, such as contextual information from the user or device environment, while making allow and deny decisions. But the IoT has a dynamic environment where flexible security policies using contextual information can potentially increase the effectiveness of security decisions.

Privacy-Preserving: Since information reflects users' daily activities (e.g., travel routes, buying habits), it is considered by many users as private, it would be no surprise that one of the requirements to ubiquitous applications would be privacy preservation. For example, users may not be willing to provide their current location to the Location-based service (LBS) server due to concerns about location privacy. Context information can be used to determine when or not to keep user information private.

3 Taxonomy of Context-aware Security in IoT

Taking into account widespread published research in the context-awareness area [21][13][19], and considering particular features of heterogeneous IoT environments, such as processing power, storage capacity, network conditions, and different users/applications, we defined a taxonomy of CAS in IoT. The present taxonomy is derived from a previous work on context-aware domain [19]. The taxonomy presents the main characteristics of CAS solutions alongside the possible deployment variations. It is depicted in Figure 1. The taxonomy is divided into three parts: (i) Context Modeling (i.e., how to manage with context), (ii) Key Architectural Components (i.e., architectural characteristics), and (iii) Applicability (i.e., in which way the CAS is provided).

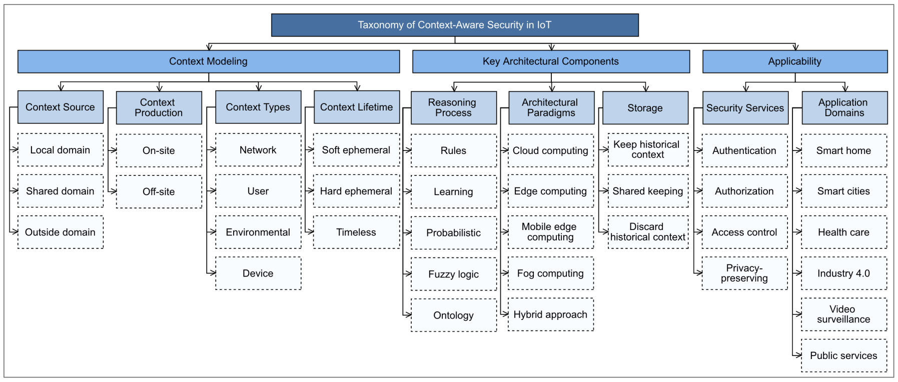

Fig. 1. A taxonomy representation of Context-Aware Security in IoT.

3.1 Context Modeling

Context Source: CAS solutions need context information to provide security services. It can be acquired from different sources, such as *local domain*, *shared domain*, and *outside domain*. The domain relates to the physical place where the solution is deployed (e.g., healthcare, smart city, industry 4.0). In the *local domain*, the CAS solution only has access to context information from its deployed domain. In the *shared domain*, a context can come from the same domain of the solution but in another deployment site (e.g., two instances of the same healthcare solution). Finally, the *outside domain* refers to a context from a different domain of the deployed one.

Context Production: The context can be produced in two different ways: *on-site* or *off-site*. The *on-site* context production happens when the solution providing CAS is also responsible for producing the context information by acquiring the raw data from the IoT entities and turning them into context information. The *off-site* process happens when a third-party software entity is responsible for context production.

Context Types: The Context Type is defined by the characteristics of the source that the context was acquired. The different Context Types of the context information are: *network* (e.g., bandwidth situations, congestion, fault nodes), *user* (e.g., location, activities, paths, preferences), *environmental* (e.g., weather, crowding), and *device* (e.g., battery life, possible errors). A CAS solution can have context information of one or more context types.

Context Lifetime: Context can be time-sensitive information depending on the deployment environment. If context information becomes old, it can lose value, as IoT environments tend to be highly dynamic, and the data can change in a minimal amount of time. The Context Lifetime can be classified in: *soft ephemeral*, *hard ephemeral*, and *timeless.* The *soft ephemeral* context information is useful for a specific period. The *hard ephemeral* context information can vary in each interaction. The *timeless* context information represents the ones that may not change over time. The amount of time for a context to become useless depends on the deployment environment and must be set by the CAS solution.

3.2 Key Architectural Components

Reasoning Process: The Reasoning Process is responsible for transforming raw data into context and turning the context information into security services by the CAS solutions. The most popular reasoning techniques are *rules*, *learning*, *probabilistic*, *fuzzy logic*, and *ontology. Rules* are simple to use and are one of the most lightweight options, which should be considered for resource-constrained IoT environments. *Rules* are based on IF-THEN-ELSE conditions. The *learning* techniques, such as Bayesian Networks and Decision trees, require a significant amount of data for more accurate reasoning. *Probabilistic* reasoning also needs an extensive data set to produce satisfactory results. However, it reasons numerical values only using past acquired data/context. *Fuzzy logic* allows a more natural representation of the environment. Even so, it can be error-prone, considering it is manually defined. The use of *ontologies* allows complex reasoning and representations. However, the input data should be modeled in a compatible format (e.g., Web Ontology Language (OWL), Resource Description Framework (RDF)), and it tends to have low performance by requiring more computational effort than usually found in resource-constrained IoT environments.

Architectural Paradigms: The CAS solutions can follow different architectural paradigms depending on diverse requirements, such as resource availability, storage space, network conditions, and processing power. These architectural paradigms can be categorized in *cloud computing*, *edge computing*, *mobile edge computing*, *fog computing*, and *hybrid approach. Cloud computing* focuses on performing the essential processing tasks in the cloud and also using it to store information if necessary. Oppositely, both *edge computing* and *mobile edge computing* paradigms focus on processing the more critical tasks at the edge of the network directly on the data sources devices. These paradigms help decrease network latency and tend to be more scalable. The difference between edge and mobile edge approaches is mobility since the mobile edge entities can change their location frequently. The *fog computing* paradigm extends cloud computing into an intermediate layer physically close to data sources devices [12]. Finally, some solutions integrate more than one architectural paradigm described, being characterized as *hybrid approaches.*

Storage: The CAS solutions can *keep historical context*, perform a *shared keeping*, or *discard historical context.* The ones that *keep historical context* store internally all the context information used for the security services provisions. The history can also be used alongside the CAS reasoning for probabilistic processing. A different way of storage is the *shared keeping.* These solutions can also have access to previously used context information but in a shared way. The context is stored in another instance, different from the one performing the CAS process. Finally, some solutions may only use the context information during the execution time and then *discard historical context*.

3.3 Applicability

Security Services: CAS solutions can be used to provide different Security Services in the security and privacy area, such as *authentication*, *authorization*, *access control*, and *privacy-preserving*. The solutions use the Reasoning Process to reason about the context and provide a Security Service. A solution can provide one or more Security Services, it will depend on the deployment environment, and the Reasoning Process used. An example of a Security Service is the Context-Aware Role Based Access Control (CARBAC) scheme proposed by Hosseinzadeh et al. [14]. It controls the access of the users to the system following their role, as the traditional Role-based Access Control (RBAC), but it also considers the current context information for granting access.

Application Domains: A number of different application domains can use CAS solutions. Some examples are *smart home*, *smart cities*, *health care*, *industry 4.0*, *video surveillance*, and *public services*. For instance, in a smart city, privacy-preserving can be achieved when the people may share their personal context with a city infrastructure only at a determined context (e.g., out of the home). Also, context-based access control policies can be defined in an industry 4.0 environment to the employees only access some rooms depending on the context. Those are some examples of Security Services being applied in different domains.

4 Key Requirements of Context-aware Security in IoT

The taxonomy presented in Section 3 showed the main characteristics of CAS solutions in IoT and how their application may vary. Taking this into account, the present section defines the mandatory features for a smooth provision of security services using context information [21][15].

Context acquisition: The acquisition comprises three characteristics of the defined taxonomy (see Figure 1): Context Source, Context Production, and Context Types. It is crucial that the CAS solution maintain a source to acquire context. Moreover, the context information could be acquired from different sources (e.g., network, user, environmental, device). For example, a CAS solution deployed in a smart city can acquire context from a traffic light by publish/subscribe and from an ambulance by web service at the same time.

Context processing: This component can also be called reasoning or security services inference. It is strictly linked to the Reasoning Process, which examples can be seen in Figure 1. Context processing is responsible for providing secure decisions using context information as input. There is no definition of how much context information can be processed to provide a secure decision, it can vary depending on the reasoning technique and the application domain.

Context processing needs to adapt depending on the IoT environment in which it is inserted. Thus, the design of this component should consider the resource restrictions imposed by the IoT environment in order to have a smooth and functional CAS solution.

Interoperability: Context information can vary in many ways, such as format, data type, size, and representation. Thus, CAS solutions for IoT should be interoperable by ensuring that different context information is compatible to be used as input for the security services provision. Also, there is no standard for context information representation [21], making this requirement more crucial and hard to implement.

Privacy: As most IoT systems, CAS solutions also deal with sensitive information. For example, if a CAS solution is placed at a hospital, it will deal with the sensitive health context of the patient (e.g., health status). Thus, keeping all the context information protected from possible attacks trying to steal or modify them is essential. These attacks can happen when the context information is stored or even when it is on the network. The communication channels must be protected with secure protocols to ensure data integrity and privacy. Also, authentication and access control methods should be used to protect the stored information and cryptography/anonymization.

Reliability: As the CAS solutions provide security and privacy for IoT environments and can be used in many application domains, it is a requirement to be reliable. It is essential to ensure reliability to foster the users/applications usage and improve the entire solution's security level.

5 Projects considering Context-Aware Security in IoT

The CAS concept has been on researchers' radar since the pervasive computing era [15][13]. They have introduced important definitions of the area that have been carried over the years. Due to the technological limitations of that time, CAS solutions were used to have very specific applicability. However, with the recent popularization of IoT applications, the CAS topic become more likely to be applied. Nowadays, many efforts are providing CAS solutions in different ways considering the characteristics of IoT environments.

Table 1 analyzes CAS systems based on possible security services provided by the solution: (i) authentication, (ii) authorization, (iii) access control, and (iv) privacy-preserving. A dash (—) symbol is used across all columns to denote that the feature is either missing or not mentioned in related publications that are available. The symbol (✓) is used to denote the feature employed by the analyzed work from some perspective. We choose the solutions by searching for the terms *Context-Aware Security* and *context-aware + privacy + secure + authentication + authorization + access control* on academic repositories (i.e., Google Scholar, IEEE Xplore, ACM Digital Library, Springer). We focused on solutions developed in recent years, and deployed for embedded systems applications.

In **SocIoTal**, the authors present a framework developed under the foundations of the EU FP7 SocIoTal project [24]. The proposed framework has two

Table 1. Overview of Context-Aware Security Solutions by Security Service Provided.

Solutions	Ref	Year	Authentication	Authorization	Access Control	Privacy-Preserving	Scope
SocIoTal	[24]	2015	✓	✓	✓	✓	IoT
Rachid et al.	[23]	2015	—	—	—	✓	IoT
Gansel et al.	[9]	2015	✓	—	✓	—	Automotive
SVM-CASE	[17]	2015	✓	—	—	—	VANET
CAS RBAC	[29]	2016	—	✓	✓	—	User
CARBAC	[14]	2016	✓	✓	✓	✓	WSN
ContexIoT	[16]	2017	—	✓	✓	—	IoT
CAPP	[30]	2017	—	—	—	✓	Smartphones
CRBAC	[4]	2018	✓	✓	✓	✓	Healthcare
CSIP	[3]	2018	✓	—	✓	—	Industrial IoT
Aegis	[25]	2019	—	✓	✓	—	Smart Home
Gheisari et al.	[10]	2019	—	—	—	✓	Smart City
Psarra et al.	[22]	2020	—	✓	✓	—	Healthcare
SETUCOM	[27]	2021	✓	✓	✓	✓	IoT
STAC	[5]	2021	✓	✓	✓	✓	IoT

main modules: Group Manager and Context Manager. The former is responsible for dealing with data sharing within a group of devices. The latter is responsible for the CAS provision by a Complex Event Processing (CEP) technique.

Rachid et al. propose a context-aware architecture for privacy preservation in IoT [23]. It has the possibility of offering an ontology as a service that can be used for privacy processing. **Gansel et al.** present a solution focused in automotive scenarios [9]. They propose an access control model that is inherently aware of the context of the car and its applications. Their model grants permissions to exclusively access certain display areas to applications depending on the current context. The SVM-based Context-Aware Security Framework (**SVM-CASE**) [17] uses the Support Vector Machine (SVM) learning technique to automatically determine the boundary between the misbehaving nodes and well-behaved nodes in VANETs. SVM-CASE uses the vehicle's context information, such as velocity, temperature, and altitude, to detect malicious nodes in a network.

Trnka et al. propose a solution that extends role-based access control (RBAC) with certain context awareness elements [29]. It is based on the usage of security levels, which are granted to the user based on his context. In **CARBAC**, the authors propose a Context-Aware Role Based Access Control (CARBAC) scheme [14]. CARBAC access control scheme is modeled using ontological techniques and Web Ontology Language (OWL) and implemented via the CLIPS business rules tool. **ContexIoT:** is a context-based permission system for IoT platforms that provides contextual integrity [16]. It is a smartphone app developed using the Samsung SmartThings platform that is able to analyze the context data flow.

The context-aware privacy-preserving algorithm (**CAPP**) [30] was designed for smartphone applications to decide in which way the context of a user can be disseminated. In **CRBAC**, the authors propose a context-sensitive role-based access control (CRBAC) [4]. The CRBAC model defines context conditions involving roles and attributes to describe policies that can be applied in critical situations. Context-sensitive seamless identity provisioning (**CSIP**) is a mutual authentication framework for the Industrial Internet of Things (IIoT) [3]. The authors define the inhabitants of IIoT scenarios as people, devices, services, systems, sensors, and 5G smartphones. CSIP builds an inhabitant profile by using their activities' history and usage patterns of the environment's resources, based on that, it can create an identity proxy to perform the verification required during the interaction for the authentication process.

Aegis is a CAS framework to detect malicious activity in Smart Home Systems (SHS) [25]. Aegis captures sensor-device data in smart home scenarios to understand the user activity context. With this data, it is possible to detect malicious behavior and alter users about it. **Gheisari et al.:** first equip IoT-based smart city with Software Defined Networking paradigm (SDN). Then, they mount a privacy-preserving method on top of it that manages flowing data packets of IoT devices' data [10]. The SDN classifies all connected IoT devices' data based on the context.

Psarra et al. [22] present a CAS model that can serve as background knowledge for creating and enforcing access control rules for electronic health records (EHR) using a combination of the Attribute Based Access Control (ABAC) and Attribute Based Encryption (ABE) models. **SETUCOM** [27] secures context information exchange by using a hybrid encryption system adapted to IoT devices and manages trust through artificial intelligence techniques such as Bayesian networks and fuzzy logic. **STAC** [5] uses ontologies to provide CAS of data regarding patient context, such as treatment history, test description, current location, or cause of the disease.

Although all the analyzed works provide solutions related to CAS, they may differ in their architecture and how they provide security. Each work has its focus, as ones have the objective of protecting the whole infrastructure, and there are systems with a specific goal. By using context information to provide security, most of the systems were deployed for dynamic situations, where the location and status are important elements.

6 Summary of Context-Aware Security Solutions

A comparative summary of recent context-aware solutions focused on IoT environments is presented in Table 2, a dash (—) symbol is used across all columns to denote that the feature is either missing or not mentioned in related publications that are available. The CAS requirements (See Section 4) are considered for the analysis. For all the requirements, we analyze the characteristics implemented by the CAS solution and not the specific technologies that it uses. For example, a solution can address the Privacy requirement if it has a process in its architecture for hiding the user data in some context. If a solution only uses a secure communication protocol (e.g., DTLS, TLS, wolfSSL) for protecting data, it is not considered as meeting the Privacy requirement.

Some of the analyzed works act in the CAS field by the detection of anomalies [17][16][25]. Such approaches use context both from users and the environment to detect abnormal network/system activity based on historic data and/or unusual behavior. When properly implemented, anomaly detection can deliver significant security improvements to IoT environments. However, it represents a subset of the security provision possibilities achieved by the use of CAS solutions. In a CAS solution, anomaly detection can act as a trigger for providing different Security Services.

The only two requirements performed by all the analyzed works were *Context acquisition* and *Context processing*. It is expected for the solutions to do that, as the CAS solutions should get the context from a source (i.e., Context acquisition) and process it for taking the security decisions. A considerable amount of analyzed works performs the Context acquisition by getting context from the user's mobile device [14][16][3]. Rachid et al. [23] propose a different approach by getting context through a sensing layer from a wireless sensor network. Gheisari et al. [10] have defined a Software-Defined Networking (SDN) for acquiring context. On the Context processing requirement, the use of rules is the most popular technique [9][29][14][16][10][22][5]. Rules are simple to define, easy to use, and lightweight, being popular in the context-aware field [21]. The usage of both ontologies and machine learning techniques can be considered a trend in this field [23][14][27]. Moreover, such techniques can help in providing interoperability.

The *Interoperability* requirement is related to the solution effort in dealing with different entities (e.g., data, devices). Some analyzed works provide interoperability only with the same kind of entities [17][16][30]. SocIoTal [24] and Aegis [25] work in providing a common data format, making easy interoperability after parsing processing. Rachid et al. [23] and CARBAC [14] perform similar processing, using an ontology to create a common vocabulary between the entities.

Privacy and *Reliability* are the less addressed requirements by the analyzed works. For *Privacy*, most of the analyzed works perform a kind of processing, either by rules or different condition manager, to set the privacy level of context data [24][23][14]. CRBAC [4] performs an anonymization privacy processing by replacing some elements of the context information for unique data, keeping it private. Aegis [25] does not store user data from smart home devices, reducing privacy risks and concerns from prior solutions. There are different approaches employed by the analyzed works to ensure the *Reliability* requirement. Most works perform a redundancy processing to minimize failures [16][3][10].

It is essential to research, study, and develop Context-Aware Security solutions for the evolution and consolidation of the IoT. The analyzed solutions provide Context-Aware Security in different ways in their applications. The most common drawbacks of Context-Aware Security solutions are related to data protection (i.e., context information). It is important to follow the new legal regulations such as the General Data Protection Regulation (GDPR) [28] to ensure

Table 2. Overview of Context-Aware Security Solutions by Requirements.

Solutions	Ref	Context acquisition	Context processing	Interoperability	Privacy	Reliability
SocIoTal	[24]	Gets context from internal or external device‘s sensors	Uses key-value pairs and markups for modeling and Complex Event Processing for reasoning	Translates raw context data into a proprietary common format	A repository of privacy rules is used to define privacy preferences of users	It has a component that allows smart objects to obtain data from other entities in a reliable way
Rachid et al.	[23]	Gets context trough a sensing layer from a WSN	Uses an ontology-based reasoning technique	An ontology acts as a common vocabulary for the context across the various system components	Uses an ontology that describes the privacy of users	—
Gansel et al.	[9]	Gets context about the status of the car, the environment, and user	Uses rules for a dynamical access control	—	An application requires a permission restricted to certain contexts	It uses a microkernel based hypervisor
SVM-CASE	[17]	Gets context from network and nodes/devices	Uses the Support Vector Machine (SVM) algorithm to classify nodes	Provides interoperability between different automotive nodes	—	Verifies if a node becomes misbehaving using context information
CAS RBAC	[29]	Uses both real-time and historical users context (e.g., location, time)	Uses rules to determine access control levels	It is interoperable with solutions using Role-based Access Control (RBAC)	—	It has mechanisms to validity check the context information
CARBAC	[14]	Gets context from users devices (e.g., smartphone)	Uses OWL and CLIPS rules to perform reasoning	By using ontologies, it is able to deal with generic data	Provides data privacy by security rules	—
ContexIoT	[16]	Collects context from the smartphone in installation and runtime	Uses rules to compare contexts in a key-value pair	It uses the Samsung SmartThings platform to prototype the solution	—	It keeps a runtime logging for the context events
CAPP	[30]	It acts as a middleware for the smartphone and can get context directly from smartphones sensors	It uses Markov Chain for both model and reasoning on context to provide privacy	It can be used by different smartphones	It protects user‘s privacy context from untrusted smartphone apps	It performs check methods before release the context of a user
CRBAC	[4]	Gets context from previously connected devices	Uses a rule-based processing for access control	—	Replaces the original data identities with unique privacy labels	It records the history of every data exchange between the entities
CSIP	[3]	Gets the context from sensors/smartphones of medical domain	Uses data mining techniques to extract patterns for future reasoning by comparison	Synchronizes data blocks with a cloud-based side	Uses a secure session-key for access to private data	Stores the processed data for learning purposes
Aegis	[25]	Collects the state of smart home devices and sensors (active or inactive) autonomously	A Markov Chain-based machine learning model is used to detect malicious activities	It has a data array format for parsing the collected context	It assigns an anonymous ID for each user to ensure privacy	—
Gheisari et al.	[10]	It has a Software-Defined Networking (SDN) for getting the device‘s data	It uses rules to determine the sensitivity level of each data	Different devices can participate a defined SDN	It defines that sensitive data not be disclosed unintentionally	It splits sensitive data and sends split parts through a secure route
Psarra et al.	[22]	Gets plaintext from medical records and attribute values from the environment	Uses a rule-based approach with ontologies for vocabulary	An ontology acts as a common vocabulary for the healthcare domain	—	—
SETUCOM	[27]	Acquisition through MQTT protocol. Subscription is also available	Uses fuzzy logic for the reasoning process	Context modeler module to help in interoperability	Modules to deal with devices trust and network security	Device trust module responsible for the reliability of the context information
STAC	[5]	Collected data is transferred between various devices to the knowledge base	Semantic rules applicable on OWL ontologies	—	Provides data privacy by security rules	—

that privacy-sensitive data is not leaked. Also, most Context-Aware Security solutions do not care about the high heterogeneity of IoT environments by providing a complete interoperable mechanism for context information.

7 Conclusion

Context-Aware Security solutions play a key role in providing dynamic security in IoT environments. Even though there are various solutions deployed with different characteristics, there are challenges to be overcome. In this review, we presented essential requirements for the development of Context-Aware Security solutions. We also introduced a novel taxonomy for Context-Aware Security. Finally, we presented various existing Context-Aware Security solutions and discussed their features in detail that can lead to the challenges and open issues for such platforms and the potential enhancements for them. In conclusion, we believe this work can contribute to the research community by comparing Context-Aware Security solutions and helping readers to develop new solutions which address Context-Aware Security in IoT.

References

1. Abowd, G.D., Dey, A.K., Brown, P.J., Davies, N., Smith, M., Steggles, P.: Towards a Better Understanding of Context and Context-Awareness. In: Proceedings of the 1st International Symposium on Handheld and Ubiquitous Computing. pp. 304–307. HUC '99, Springer-Verlag, London, UK, UK (1999)
2. Al-Muhtadi, J., Ranganathan, A., Campbell, R., Mickunas, M.D.: Cerberus: a context-aware security scheme for smart spaces. In: Proceedings of the 1st IEEE International Conference on Pervasive Computing and Communications. pp. 489–496 (Mar 2003). https://doi.org/10.1109/PERCOM.2003.1192774
3. Al-Turjman, F., Alturjman, S.: Context-Sensitive Access in Industrial Internet of Things (IIoT) Healthcare Applications. IEEE Transactions on Industrial Informatics **14**(6), 2736–2744 (Jun 2018). https://doi.org/10.1109/TII.2018.2808190
4. Alagar, V., Alsaig, A., Ormandjiva, O., Wan, K.: Context-Based Security and Privacy for Healthcare IoT. In: Proceedings of the 2nd IEEE International Conference on Smart Internet of Things. pp. 122–128 (Aug 2018). https://doi.org/10.1109/SmartIoT.2018.00-14
5. and, A.N.: An ontology based approach for context-aware security in the internet of things (IoT). International Journal of Wireless and Microwave Technologies **11**(1), 28–46 (Feb 2021). https://doi.org/10.5815/ijwmt.2021.01.04, https://doi.org/10.5815/ijwmt.2021.01.04
6. Atzori, L., Iera, A., Morabito, G.: The internet of things: A survey. Computer Networks **54**(15), 2787–2805 (Oct 2010). https://doi.org/http://dx.doi.org/10.1016/j.comnet.2010.05.010
7. Brezillon, P., Mostefaoui, G.K.: Context-based security policies: a new modeling approach. In: Proceedings of the 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops. pp. 154–158 (Mar 2004). https://doi.org/10.1109/PERCOMW.2004.1276923

8. Future Market Insights: Global Internet of Things (IoT) Security Product Market Overview (2017), https://www.futuremarketinsights.com/reports/internet-of-things-security-products-market
9. Gansel, S., Schnitzer, S., Gilbeau-Hammoud, A., Friesen, V., Dürr, F., Rothermel, K., Maihöfer, C., Krämer, U.: Context-Aware Access Control in Novel Automotive HMI Systems, chap. 8, pp. 118–138. Springer International Publishing, Cham (2015). https://doi.org/10.1007/978-3-319-26961-0_8, https://doi.org/10.1007/978-3-319-26961-0_8
10. Gheisari, M., Wang, G., Khan, W.Z., Fernández-Campusano, C.: A context-aware privacy-preserving method for IoT-based smart city using Software Defined Networking. Computers & Security **87**, 101470 (Nov 2019). https://doi.org/https://doi.org/10.1016/j.cose.2019.02.006, http://www.sciencedirect.com/science/article/pii/S0167404818313336
11. Grimm, D., Stang, M., Sax, E.: Context-aware security for vehicles and fleets: A survey. IEEE Access **9**, 101809–101846 (2021). https://doi.org/10.1109/ACCESS.2021.3097146
12. Gupta *et al.*, H.: iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments. Software: Practice and Experience **47**(9), 1275–1296 (Jun 2017). https://doi.org/10.1002/spe.2509
13. Habib, K., Leister, W.: Context-Aware Authentication for the Internet of Things. In: Proceedings of the 11th International Conference on Autonomic and Autonomous Systems. p. 6 (2015)
14. Hosseinzadeh, S., Virtanen, S., Díaz-Rodríguez, N., Lilius, J.: A Semantic Security Framework and Context-aware Role-based Access Control Ontology for Smart Spaces. In: Proceedings of the 1st International Workshop on Semantic Big Data. pp. 8:1–8:6. SBD '16, ACM, New York, NY, USA (2016). https://doi.org/10.1145/2928294.2928300, http://doi.acm.org/10.1145/2928294.2928300
15. Hu *et al.*, J.: A Dynamic, Context-Aware Security Infrastructure for Distributed Healthcare Applications. In: Proceedings of the 1st Workshop on Pervasive Privacy Security, Privacy, and Trust. pp. 1–8. Citeseer (2004)
16. Jia, Y.J., Chen, Q.A., Wang, S., Rahmati, A., Fernandes, E., Mao, Z.M., Prakash, A., Unviersity, S.J.: ContexIoT: Towards Providing Contextual Integrity to Appified IoT Platforms. In: Proceedings of the 21st Network and Distributed System Security Symposium. pp. 1–15 (2017)
17. Li, W., Joshi, A., Finin, T.: SVM-CASE: An SVM-Based Context Aware Security Framework for Vehicular Ad-Hoc Networks. In: Proceedings of the 82nd IEEE Vehicular Technology Conference. pp. 1–5 (Sep 2015). https://doi.org/10.1109/VTCFall.2015.7391162
18. de Matos, E., Tiburski, R.T., Amaral, L.A., Hessel, F.: Providing Context-Aware Security for IoT Environments Through Context Sharing Feature. In: Proceedings of the 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications. pp. 1711–1715 (Aug 2018). https://doi.org/10.1109/TrustCom/BigDataSE.2018.00257
19. de Matos, E., Tiburski, R.T., Moratelli, C.R., Filho, S.J., Amaral, L.A., Ramachandran, G., Krishnamachari, B., Hessel, F.: Context information sharing for the Internet of Things: A survey. Computer Networks **166**, 1–19 (Jan 2020). https://doi.org/https://doi.org/10.1016/j.comnet.2019.106988, http://www.sciencedirect.com/science/article/pii/S1389128619310400

20. Mostefaoui, G.K., Brezillon, P.: Modeling context-based security policies with contextual graphs. In: Proceedings of the IEEE Annual Conference on Pervasive Computing and Communications Workshops. pp. 28–32 (Mar 2004). https://doi.org/10.1109/PERCOMW.2004.1276900
21. Perera, C., Zaslavsky, A., Christen, P., Georgakopoulos, D.: Context Aware Computing for The Internet of Things: A Survey. IEEE Communications Surveys Tutorials **16**(1), 414–454 (First Quarter 2014). https://doi.org/10.1109/SURV.2013.042313.00197
22. Psarra, E., Verginadis, Y., Patiniotakis, I., Apostolou, D., Mentzas, G.: A context-aware security model for a combination of attribute-based access control and attribute-based encryption in the healthcare domain. In: Barolli, L., Amato, F., Moscato, F., Enokido, T., Takizawa, M. (eds.) Web, Artificial Intelligence and Network Applications. pp. 1133–1142. Springer International Publishing, Cham (2020)
23. Rachid, S., Challal, Y., Nadjia, B.: Internet of things context-aware privacy architecture. In: Proceedings of the 12th IEEE/ACS International Conference of Computer Systems and Applications. pp. 1–2 (Nov 2015). https://doi.org/10.1109/AICCSA.2015.7507247
24. Ramos, J.L.H., Bernabe, J.B., Skarmeta, A.F.: Managing Context Information for Adaptive Security in IoT Environments. In: Proceedings of the 29th IEEE International Conference on Advanced Information Networking and Applications Workshops. pp. 676–681 (Mar 2015). https://doi.org/10.1109/WAINA.2015.55
25. Sikder, A.K., Babun, L., Aksu, H., Uluagac, A.S.: Aegis: A Context-Aware Security Framework for Smart Home Systems. In: Proceedings of the 35th Annual Computer Security Applications Conference. p. 28–41. ACSAC '19, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3359789.3359840, https://doi.org/10.1145/3359789.3359840
26. Sylla, T., Chalouf, M.A., Krief, F., Samaké, K.: Context-aware security in the internet of things: a survey. International Journal of Autonomous and Adaptive Communications Systems **14**(3), 231–263 (2021). https://doi.org/10.1504/IJAACS.2021.117808, https://www.inderscienceonline.com/doi/abs/10.1504/IJAACS.2021.117808
27. Sylla, T., Chalouf, M.A., Krief, F., Samaké, K.: Setucom: Secure and trustworthy context management for context-aware security and privacy in the internet of things. Security and Communication Networks **2021**, 6632747 (Apr 2021). https://doi.org/10.1155/2021/6632747, https://doi.org/10.1155/2021/6632747
28. Tikkinen-Piri, C., Rohunen, A., Markkula, J.: EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review **34**(1), 134 – 153 (Feb 2018). https://doi.org/https://doi.org/10.1016/j.clsr.2017.05.015, http://www.sciencedirect.com/science/article/pii/S0267364917301966
29. Trnka, M., Cerny, T.: On Security Level Usage in Context-aware Role-based Access Control. In: Proceedings of the 31st Annual ACM Symposium on Applied Computing. pp. 1192–1195. SAC '16, ACM, New York, NY, USA (2016). https://doi.org/10.1145/2851613.2851664, http://doi.acm.org/10.1145/2851613.2851664
30. Zhang, L., Li, Y., Wang, L., Lu, J., Li, P., Wang, X.: An Efficient Context-Aware Privacy Preserving Approach for Smartphones. Security and Communication Networks **2017**, 1–11 (Apr 2017). https://doi.org/10.1155/2017/4842694