Article

Security Capabilities and Vulnerabilities of Internet of Things Architectures and the Necessity of Using Dynamic Security for IOT

Seyyed Yasser Hashemi * and Fereidoon Shams
Department of Computer Engineering, Shahid Beheshti University, Tehran, Iran; hashemi.uni@gmail.com
* Correspondence: Y_Hashemi@sbu.ac.ir; Tel.: +98-914-180-3495

Abstract: Internet of things is a dynamic global network infrastructure based on standard and interoperable communication protocols where physical and virtual ‘things’ integrated into the information network. The Internet of Things links the objects of the real world with the virtual world, thus enabling anytime, anyplace connectivity for anything and not only for anyone. It refers to a world where physical objects and beings, as well as virtual data and environments, all interact with each other in the same space and time. It is natural that many risks associated with the creation of such a network. In this environment Security challenges are very important. The unique properties of the IOT such as "uncontrolled environment", "Heterogeneity", "Scalability" and "Constrained resources" makes unusable the previous solutions for security, privacy and trust. In this paper, different IOT architectures will be introduced and the security strategies will be compared. Our analysis shows the necessity of dynamic security for the Internet of Things.

Keywords: Internet of Things; security; privacy; trust; IOT architecture; dynamic security

1. Introduction

Internet of Things (IoT) is an integrated part of Future Internet and could be defined as a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual “things” have identities, physical attributes, virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network. In the IOT, "things" are expected to become active participants in business, information and social processes where they are enabled to interact and communicate among themselves and with the environment by exchanging data and information “sensed” about the environment, while reacting autonomously to the “real/physical world” events and influencing it by running processes that trigger actions and create services with or without direct human intervention [1].

Internet that is universalized many years ago still has many security weaknesses that led to threat to humans’ property and even lives as well. In such circumstances, securing a global network of things with its own characteristics and limitations that communicate together and with humans naturally will be more complicated. New environmental conditions and features of the various devices, causes the security of Internet of Things is considered specifically and various architectures are provided [2-10]. Also, due to the ownership of things, as well as privacy of humans, attention to safety tips related to identifying and exploring, availability, access control, privacy and trust in the Internet of Things will be more important. Internet of Things technology is such that, if exploited, there is even the possibility of endangering lives. Thus, the security of the Internet of Things is a key element in the implementation of this technology.

Considering the importance of security in the Internet of Things, in this paper, proposed architectures for Internet of things is reviewed and their ability to meet the security needs of the Internet of Things is compared. Accordingly, we express shortcomings in Internet of things security and the necessity of using Dynamic Security for Internet of Things will be clear.
The rest of the paper is organized as follows: Section 2 describes the characteristic of Internet of Things. The security requirements for IoT are presented in section 3. Section 4 Provides an overview of the IoT architectures as well as a security and privacy analysis of them with respect to our requirements. Finally, IoT architectures compared with a focus on the fulfillment of the requirements and concluded the paper in Section 5.

2. IoT Characteristic Based on Security

The most important characteristic of the Internet of Things in the literature [11-17] are the following:

- Uncontrolled environment: Environment is very widespread and uncontrolled. Things are part of the environment and in many cases without supervision and control, are moving in the environment. In this uncontrolled and widespread environment, malicious manipulation of things by people or other things is possible. Uncontrolled environment refers to three categories of requirements in general:
  - Mobility: IoT devices are mobile and often generally connect to the Internet via a large set of providers. In this environment permanent network connectivity and constant presence cannot be expected.
  - Physical accessibility: The sensors and things are available publicly on the Internet of Things and malicious manipulation of things by people or other things is possible. As result of the physical access the attacker can gain full access to the persistent storage of the affected component.
  - Trust: Trust has various aspects, such as the "Multidimensional", "Contextual", "Mutable", "Revocable" and etc. In this environment and considering the large number of devices and users interact with each other, so priori trust relationship is to require review and automatic mechanism for measuring and managing trust of things, services, and users to the Internet of Things to be developed or adapted.
  - Governance: Governance is the amount of actual security control on the network of things. Wherever there is more control and monitoring, there is more safety. This also applies to IoT networks. If every interaction is monitored, then it would be much easier to track a malicious activity to the attacker. Thus, this security control can be a very positive aspect. However, if it exceeds some limit, it can turn into a nuisance as a high level of monitoring can be a threat for every user's privacy.

- Heterogeneity: Heterogeneity is one of the natural features of the Internet of Things. Create an ecosystem of diverse things that are provided by different manufacturers and proper communication between them is one of the goals of the Internet of Things. It also integrates the different things is a concern for the Internet of Things. Therefore compatibility and interoperability have to be considered.

- Scalability: The number of IoT devices is growing every day and more devices are getting connected with the global information network. Current security schemes lack of the scalability property; therefore, such schemes are not suitable for IoT devices. Also, The vast amount of contiguous things in the Internet of Things will require highly scalable protocols.

- Constrained resources: resources have many Restrictions on Internet of Things such as energy limitations, low computation power and memory limitations. Thus, heavy computational algorithms cannot be applied to all things.

3. Security Requirements

The most important Security Requirements for Internet of Things in the literature are in the following categories (Figure 1):

- Network Security: An IoT device might join or leave a network at anytime from anywhere. The IoT requires architectures to deal with the heterogeneity of things. Interconnecting things may require confidentiality, authenticity and integrity. Also, IoT architectures should ensure that link handover is possible. Availability ensures that the connectivity of a thing or service persists
even under link failures. Thus confidentiality, authenticity, integrity and availability are subsets of Network Security.

- **Identity Management**: Due to the number of devices, and also because of the complex relationship between devices, services, owners and users, there are certain challenges for identity management on the Internet of Things. Hence, special attention to authentication, authorization includes the revocation or non-repudiation (the assurance that someone cannot deny something) and accountability (every action is clearly bound to an authenticated entity) is essential.

- **Privacy**: The pervasiveness of the Internet of Things raises many privacy issues. Privacy, including data privacy, anonymity (hiding data source), pseudonym (temporary identities of subjects which can be used instead of the real ones in anonymous interactions) and unlinkability (specific actions of the same person must not be linked together).

- **Trust**: Trust is included data trust, entity trust and device trust. Establishing entity trust is much more difficult than device trust.

- **Resilience**: Resilience is classified into two categories, robustness against attacks and resilience in defeat.

- **Dynamic Security**: Due to the nature of the Internet of Things, dynamic security affects the other security categories. According to the characteristic of the Internet of Things such as “uncontrollable and dynamic environment”, “the diversity of things” and “limited resources”, static security solutions alone will not be able to meet the security needs of the Internet of Things and dynamic Security have very important role in Internet of Things security. We define dynamic security with four subcomponents: Runtime Behavior Based Security (Designing systems security according to runtime behavior), Context-Driven Security, Freshness (Freshness guarantees that the data is very much recent and no old messages have been replayed) and Adaptation (Adaptive (active-defense) systems).

---

**Figure 1** Security Requirements for Internet of Things

Security requirements and characteristic of the Internet of things affect each other. This effect is shown in Table 1. In Table 1 the ”●” symbols represent the level of influence in a scale from one (low) to three (high).
Table 1. Security requirements with characteristic of Internet of Things relationship

<table>
<thead>
<tr>
<th></th>
<th>Network security</th>
<th>Identity management</th>
<th>Privacy</th>
<th>Trust</th>
<th>Resilience</th>
<th>Dynamic Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uncontrolled environment</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●●●</td>
<td>●</td>
<td>●●●</td>
</tr>
<tr>
<td>Mobility</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●●●</td>
<td>●</td>
<td>●●●</td>
</tr>
<tr>
<td>Physical accessibility</td>
<td>●●●</td>
<td>●</td>
<td>●●●</td>
<td>●</td>
<td>●●</td>
<td>●</td>
</tr>
<tr>
<td>Trust</td>
<td>●●●</td>
<td>●●●</td>
<td>●</td>
<td>●●●</td>
<td>●</td>
<td>●●●</td>
</tr>
<tr>
<td>Governance</td>
<td>●●●</td>
<td>●●●</td>
<td>●</td>
<td>●●●</td>
<td>●</td>
<td>●●●</td>
</tr>
<tr>
<td>Heterogeneity</td>
<td>●</td>
<td>●●●</td>
<td>●</td>
<td>●●●</td>
<td>●</td>
<td>●●●</td>
</tr>
<tr>
<td>Scalability</td>
<td>●</td>
<td>●●●</td>
<td>●</td>
<td>●●●</td>
<td>●</td>
<td>●●●</td>
</tr>
<tr>
<td>Constrained Resources</td>
<td>●●●</td>
<td>●</td>
<td>●●●</td>
<td>●</td>
<td>●</td>
<td>●●●</td>
</tr>
</tbody>
</table>

4. Review IOT Architectures in Security Perspective

In this section eight main architectures proposed for internet of thing in recent years are reviewed and security solutions are detailed.


This architecture is the result of IoT-A Project in the European Lighthouse Integrated Project. The source of the need for a comprehensive architecture for the Internet of Things is the issue of integrity. In the present world, smart networks are designed and each of which has based on its own architecture and incompatible with the other. In fact, smart networks are great but distinct subsets of Internet of Things that actually instead of its original purpose have formed the Internet of Things. To achieve the main goal, there is need for a comprehensive architecture to implement Internet of Things that different networks, based on uniform platform implemented (Similar to the leaves of a tree, but the trunk unique; Figure 2). In this case different smart networks can be compatible with each other, support each other and communicate with each other. For this reason, IoT-A was implemented to provide reference architecture (ARM) for the Internet of Things.

ARM architecture can be seen in the form of a matrix that is an ideal starting point for all architectures. To provide such a matrix, all mechanisms, functions and protocols used to make it must be specified and linking them must be expressed. Although no system will not use all of these at once, but a comprehensive architecture like ARM must cover all cases. Therefore, a system designer, determine the own architecture by selecting protocols, functional components and other items in comprehensive architecture.
4.1.1. Security in ARM

ARM architecture can be seen in the form of a matrix that is an ideal starting point for all architectures. To

In ARM, Security is investigated of the four dimensions [3]. For each dimension by specifying "expected features", requirements are extracted and accordingly activities and strategies have been predicted. Four security dimensions in the ARM are: Security, Privacy, Trust and Availability.

Functional view of ARM reference architecture is shown in Figure 3. As shown in Architecture, four security dimensions have been implemented in five components:

- **Key Exchange and Management (KEM):**
  - Cryptographic key management for confidentiality and integrity combined with originality.
  - Failing to address constrained devices and unprotected gateways connections.
  - As well as failing to address availability in network communications.

- **Authorization (AuthZ):**
  - Services and infrastructure Access Control, for the purpose of access control to services, data confidentiality, data integrity, privacy and service availability using of RBAC (Role Based Access Control) and ABAC (Attribute Based Access Control).

- **Authentication (AuthN):**
  - Authentication Services and humans with the purpose of authentication and accountability using of biometric-based methods.

- **Identity Management (IM):**
  - This component is included identity management, pseudonyms and access policies related to user and service privacy.

- **Trust and Reputation (TRA):**
Collecting user trust scores and calculating level of services trust to measure the reliability of service and level of service trust.

In this architecture Confidentiality, Integrity, Authenticity, Authentication, Authorization, Revocation, Pseudonymity, Unlinkability, Device trust, Entity trust, Robustness and Resilience aspects have been considered and the aspects of Availability, Data privacy and Freshness are investigated partially. In this architecture not paid sufficient attention to aspects of Accountability, Anonymity, Data Trust, Runtime Behavior Based Security, Context-Driven Security and Adaptation.

4.2. MGC Architecture [4]

MGC architecture is a proposed architecture for the IoS Based on cloud computing which is scheduled to be extracted from Secure Internet of Things Project (SITP). The duration of the project is 5 years (since 2014) and 12 professors of the universities of Stanford, Berkeley and Michigan, are responsible for it. This Group believes that, in fact, Massive amounts of data obtained through IoT devices must be processed and it is clear that this process needs powerful processors that are available through the cloud. Therefore, MGC was proposed architecture to be able to respond IoT processing requirements.

4.2.1. Security in MGC

Security in MGC is including data security and system security. MGC Security architecture is shown in Figure 3.

The most important aim in data security is to analyze and develop new cryptography computing models responsible for data analysis and using them in multiple data streams in compact systems data security. For security, the goal is end to end security. For this purpose, these cases should be:

- Devices produce encrypted data
- Only end applications are able to do fully decode and view data
- Ports and cloud must be able to operate on the data, without being aware of the nature of the information.

Data security Strategies are:

- Using Homomorphic cryptography methods to ensure end to end security
- Do the protocols in a distributed manner. In this case, the cloud garnering results, but the cloud is unaware of what data produce results.
In system Security the aim is analyzing and implementing a secure open-source hardware/software framework that simplify developing Internet of Things applications using new computing models. For data processing the following steps are needed. Security and privacy should be considered in all of them:

- Complex models to describe data when storing data
- Transfer data between models
- Those models are limited to devices
- Observations can represent models
- Controllers specify how the data is transferred

The system creates a code structure for the entire process.

In this architecture Confidentiality, Authenticity, Authentication and Authorization aspects have been considered and the aspects of Integrity, Robustness and Resilience are investigated partially. In this architecture not paid sufficient attention to aspects of Availability, Accountability, Revocation, Data privacy, Anonymity, Pseudonymity, Unlinkability, Device trust, Entity trust, Data trust, Runtime Behavior Based Security, Context-Driven Security, Freshness and Adaptation yet.

4.3. BETaaS Architecture [5]

Building the Environment for the Things as a Service (BETaaS) is an FP7 STREP project co-funded by the European Commission under the ICT theme of DG CONNECT. BETaaS architecture is based on the Thing as a Service (TaaaS) reference model (Figure 4) and by strengthening IOT-a architecture is proposed (Figure 5).
Figure 4. Functional view of Thing as a Service Reference Model

Figure 5. BETaS layered architecture and functions of each layer
4.3.1. Security in BETaaS

Security is implemented in Security Management Component. Security Management Component is shown in Figure 6. Abilities and shortcomings of Security Management component are:

- For network security, key management component Provides "Components Communication", "authentication", "user sessions Management" and "encrypted communication".
- Security Management component using from the authentication level, gate-level and application or service level for Identity Management.
- The need for accountability remains unclear.
- Privacy, anonymity and pseudonym are not addressed practically.
- To calculate the final trust, security mechanisms values such as trust performance, battery load and stability on the provided information collecting and on the basis of them the final trust is calculated.
- The resilience aspect is applied by defect prevention, removal, tolerance and prediction.

![Figure 6. Security Management Component BETaaS architecture](image)

In BETaaS architecture Confidentiality, Integrity, Authenticity, Authentication, Authorization, Device trust, Data trust, Robustness, Resilience and Adaptation aspects have been considered and the Context-Driven Security aspect is investigated partially. In this architecture not paid sufficient attention to aspects of Availability, Accountability, Revocation, Data privacy, Anonymity, Pseudonymity, Unlinkability, Entity Trust, Runtime Behavior Based Security and Freshness.

4.4. OpenIoT Architecture [6]

Open Source cloud solution for the Internet of things Building (OpenIoT) is based on IOT-a and cloud-based. Figure 8 is shown OpenIoT architecture in functional view.
4.4.1. Security in OpenIoT

OpenIoT has two security Modules: Security and Privacy Module (Figure 7) as well as trust module (Figure 8). Abilities and shortcomings of Security modules are:

- Security and Privacy Module has secure messaging, authentication and authorization sub modules.
- However, as mentioned privacy in module name but Features of privacy is neglected.
- "Trust Module" does trust evaluation of the sensor's inputted data (data trust)
In OpenIoT architecture Confidentiality, Integrity, Authenticity, Authentication, Authorization, Device trust, Entity trust and Resilience aspects have been considered. In this architecture not paid sufficient attention to aspects of Availability, Accountability, Revocation, Data privacy, Anonymity, Pseudonymity, Unlinkability. Data trust, Robustness, Runtime Behavior Based Security, Context-Driven Security, Freshness and Adaptation.

4.5. IoT@Work Architecture [7]

Internet of thing at work (IoT@Work) architecture is developed with the purpose of creating IOT architecture for the areas of industrial automation. IoT@Work developed during the 36-month project that started in 2010 in EU by Siemens and several other companies and with the support of European Microsoft Innovation Centre (EMIC). IoT@Work breaks functions into a layered structure which guarantees independence and thus increases the flexibility of various aspects. IoT@Work layered Architecture is shown in Figure 9. Security strategies are grouped in “Security plane” box.

4.5.1. Security in IoT@Work

In Figure 9, security strategies are grouped in "Security plane" box. Security strategies are applied in layers. Noteworthy Tips are:

- Known protocols used to create “network security”.
- "Extensible Authentication Protocol (EAP)” is used For Authentication and “Capability-Based Access Control (CBAC)” is used for Authorization
- Privacy is not considered significant because of the nature of industrial automation.
• Flexibility is a basic requirement for IoT@Work and is implemented with a focus on failure handling.

In IoT@Work architecture Confidentiality, Authenticity, Authentication, Authorization, Accountability, Revocation, Anonymity and Pseudonymity aspects have been considered and the aspects of Availability, Data privacy, Robustness, Resilience and Freshness are investigated partially. In this architecture not paid sufficient attention to aspects of Integrity, Unlinkability, Device trust, Entity trust, Data trust, Runtime Behavior Based Security, Context-Driven Security and Adaptation.

4.6. WSO2 Architecture [8]

WSO2 Company in the United States of America provides a reference architecture that includes both the devices and the cloud server architecture for interaction and management of these devices. The main goal of this architecture is provide an effective starting point for architects and designers who are able to cover most of the requirements of the Internet of Things in the system and development projects. However, this architecture is not limited to a specific set of technology and does not emphasize on client-server, hardware or cloud architecture and architecture is independent of specific providers. WSO2 architecture is shown in Figure 10.

4.6.1. Security in WSO2

Security as a vertical layer is provided in WSO2 architecture. Various security operations by "IDENTIFY AND ACCESS MANAGEMENT LAYER" are performed at different layers of the architecture. In device layer declared each device normally requires an identifier. Identifier may be one of the following:

- A unique identifier (UUID) connected to the device (usually part of the system-on-chip, or provided by a secondary chip)
- A UUID provided by the radio subsystem (eg Bluetooth ID, MAC address of the Wi-Fi)
- An OAuth2 Refresh / Bearer token (in addition to the ones above)
An identifier is stored in non-volatile memory such as EEPROM. The reference architecture is recommended that each device has a UUID (preferably an hardware unchangeable ID) and as well as an encryption a OAuth2 Refresh / Bearer token stored in the EEPROM is used.

The aggregation/bus layer carried two important security tasks. This layer should be OAuth2 source server and also be the access policies execution point.

In general, the most important features of identify and access management layer are:

- Using from OAuth2 to provide authentication, emission, revocation and management of tokens.
- Support for separate registration (individual), including SAML2 SSO and support OpenID communications
- Supports identity protocols such as WS-Federation (Passive), OpenID 2.0, Kerberos, Integrated Windows Authentication (IWA), and others
- Full support for the XACML and acting as PDP and PIP and PAP
- the ability to integrate between different identity providers and service providers including brokering identity
- Support for the provisioning of identity such as SPML and support of SCIM.
- Support for policy-based access

In WSO2 architecture Confidentiality, Authentication and Device trust aspects have been considered and the aspects of Integrity, Authorization, Robustness and Resilience are investigated partially. In this architecture not paid sufficient attention to aspects of Authenticity, Availability, Accountability, Revocation, Data privacy, Anonymity, Pseudonymity, Unlinkability, Device trust, Entity trust, Data trust, Runtime Behavior Based Security, Context-Driven Security, Freshness and Adaptation.

4.7. BUTLER Architecture [9]

BUTLER is a Europe Union FP7 projects focusing on research on Internet of things. Four layer of architecture to cover all the necessary features and fulfill the requirements are communications, data and context management, system and devices management and service management. BUTLER systems is established at three entity including BUTLER SmartObject, BUTLER SmartServer and BUTLER SmartMobile. BUTLER architecture is shown in Figure 11.

4.7.1. Security in BUTLER

Security is applied in BUTLER SmartServer entity using Authorization SmartServer (TrustManager) component:

- BUTLER has provided a security and privacy framework by offering risk analysis model.
- In the BUTLER security framework, main idea is separating security management (granting users, manage profiles, key management, manufacturing encryption, access control, etc.) of application domains and access to resources.
- Security management is handled by a dedicated server is the name of authorization server. In the case of authorization server will not have access to data sources and is not involved in the transfer of data and business logic are shown in Figure 12.
- BUTLER security framework provides end-to-end security.
- OAuth 2.0 protocol used for security.
- Awareness of the context is an essential part of the architecture is emphasized.
Figure 11. BUTLER architecture

Figure 12. BUTLER authorization server will not have access to data sources and is not involved in the transfer of data and business logic
In BUTLER architecture Confidentiality, Integrity, Authenticity, Authentication, Authorization, Data privacy, Device trust, Entity trust, Robustness, Resilience and Context-Driven Security aspects have been considered and the aspects of Availability, Unlinkability, Data trust, Runtime Behavior Based Security, Freshness and Adaptation are investigated partially. In this architecture not paid sufficient attention to aspects of Accountability, Revocation, Anonymity and Pseudonymity.

4.8. Microsoft Azure Architecture [10]

This reference architecture is a guide to create, secure, scalable and devices-based solutions to connect devices, analysis, and integration with Backend Systems that focused on the public cloud (on private cloud is also applicable). This architecture is provided by Microsoft. Figure 13 shows the architecture.

![Microsoft Azure Architecture](image)

**Figure 13.** Microsoft Azure Architecture

4.8.1. Security in Microsoft Azure

- Privacy Protection using Microsoft privacy standard and Microsoft’s security development lifecycle (SDL)
- Confidence infrastructure is developed.
- multi-factor authentication
- Role-based access control
- Access Monitor
- encrypted communications

In Microsoft Azure architecture Confidentiality, Integrity, Authenticity, Authentication, Authorization, Data privacy, Device trust, Entity trust, Data trust, Robustness and Resilience aspects have been considered and the aspects of Availability and Freshness are investigated partially. In this architecture not paid sufficient attention to aspects of Accountability, Revocation, Anonymity, Pseudonymity, Unlinkability, Runtime Behavior Based Security, Context-Driven Security, Freshness and Adaptation.

5. Discussion and Conclusions

In this article, is tried consider and investigate architectures that primarily, supported by the competent and well-known organizations and secondly documentation is printed and published and publicly available. On this basis eight of prominent architecture for the Internet of Things which are developed or are in development in recent years is selected. The selected architectures are examined and their shortcomings and capabilities for covering security requirements in uncontrolled, widespread and heterogeneous IOT environment are analyzed. As Table 2 shows, in general, on aspects of Confidentiality, Integrity, Authenticity, Authentication, Authorization, Device trust, Robustness and Resilience many researches are done and appropriate strategies are provided but on aspects of Availability, Accountability, Revocation, Data privacy, Anonymity, Pseudonymity, Unlinkability, Entity trust, Data trust, Runtime Behavior Based Security, Context-Driven Security, Freshness and Adaptation more effort is needed and should be considered and appropriate
strategies provided or available strategies are adapted for the Internet of Things. In Table 2 it is clear that dynamic security is the most important requirement for the architectures of the Internet of Things and should be considered particularly. Because dynamic security-related aspects have more affinity to the characteristics of the Internet of Things than other security aspects will have an impact on other aspects of security. Thus the importance and necessity of dynamic security for the Internet of Things becomes clear.

Table 2. Compare Security capabilities and vulnerabilities of internet of things architectures

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IoT-A</td>
</tr>
<tr>
<td><strong>Network security</strong></td>
<td></td>
</tr>
<tr>
<td>Confidentiality</td>
<td>✓</td>
</tr>
<tr>
<td>Integrity</td>
<td>✓</td>
</tr>
<tr>
<td>Authenticity</td>
<td>✓</td>
</tr>
<tr>
<td>Availability</td>
<td>≈</td>
</tr>
<tr>
<td><strong>Identity Management</strong></td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>✓</td>
</tr>
<tr>
<td>Authorization</td>
<td>✓</td>
</tr>
<tr>
<td>Accountability</td>
<td>x</td>
</tr>
<tr>
<td>Revocation</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Privacy</strong></td>
<td></td>
</tr>
<tr>
<td>Data privacy</td>
<td>≈</td>
</tr>
<tr>
<td>Anonymity</td>
<td>x</td>
</tr>
<tr>
<td>Pseudonymity</td>
<td>✓</td>
</tr>
<tr>
<td>Unlinkability</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Trust</strong></td>
<td></td>
</tr>
<tr>
<td>Device trust</td>
<td>✓</td>
</tr>
<tr>
<td>Entity trust</td>
<td>✓</td>
</tr>
<tr>
<td>Data trust</td>
<td>x</td>
</tr>
<tr>
<td><strong>Resilience</strong></td>
<td></td>
</tr>
<tr>
<td>Robustness</td>
<td>✓</td>
</tr>
<tr>
<td>Resilience</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Dynamic Security</strong></td>
<td></td>
</tr>
<tr>
<td>Runtime Behavior</td>
<td>x</td>
</tr>
<tr>
<td>Based Security</td>
<td></td>
</tr>
<tr>
<td>Context-Driven Security</td>
<td></td>
</tr>
<tr>
<td>Freshness</td>
<td>≈</td>
</tr>
<tr>
<td>Adaptation</td>
<td>x</td>
</tr>
</tbody>
</table>
References

8. PAUL FREMANTLE, A REFERENCE ARCHITECTURE FOR THE INTERNET OF THINGS, WSO2, VERSION 0.9.0 (OCTOBER 20, 2015).

© 2016 by the authors; licensee *Preprints*, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons by Attribution (CC-BY) license (http://creativecommons.org/licenses/by/4.0/).