# Response to the Editor and to the Reviewers

**Title: Security Analysis of a Proposed Internet of Things Middleware**

## We would like to thank the Editor and the two reviewers for their insightful comments and suggestions that have greatly improved the quality of our work. Below are our point-to-point responses to the comments and suggestions.

1. EDITOR
2. **COMMENT:** *Based on the advice received, your manuscript could be accepted for publication should you be prepared to incorporate minor revisions*.

## **REPLY:** We thank the Editor for the time, work, and positive evaluation of our paper.

1. REVIEWER 2
2. **COMMENT:** *Authors claim to present a security model for UIoT, a previously proposal from the same authors. Nevertheless, the security proposal in the paper is too vague and still needs further development. But, as the general ideas presented are admissible, it may be accepted and some review suggestions follow.*

## **REPLY:** We thank this reviewer for her/his stimulating comments and for appreciating the contribution of our paper, as well as for her/his review suggestions. We modified and added content to our paper in order to give more precisions and development details. Specifically, we have reviewed and extended our introduction for a better contextualization of the problem and introduced two new figures (1 and 5), with their description text, intended respectively to elucidate the security issues for IoT users, devices, applications and middleware (Section 1), and to give a new perspective on our proposed model (Section 4.4).

1. **COMMENT:** *Please clarify (page 1, line 40) - "unique identification for objects is also a problem due to ever-limited availability of IPv4 addresses"; what about IPv6? why do you ignore IPv6 (and 6lowpan)? Should discuss!.*

## **REPLY:** We thank the reviewer for this constructive comment. We have rewritten this part of the text and changed it t: “since IoT presupposes the Internet as its main data exchange infrastructure, issues related to the Internet architecture are also a challenge, including the unique identification for communicating, and possibly moving, objects, applications and users”. Also, we added new text to explain this issue in our Proposed Model (Section 4), stating that: “this is more than a question of IP addresses, but a more general identification question considering mobility and the possible participation of devices and users in different IoT instances. For this reason, we adopt the idea of the middleware attributing the identification to each device and the security model to having the structure and processes for this identification and the corresponding subsequent authentication and authorization, as required in our attack models (Section 3) and integrated in the abstraction of devices and users for purposes of authentication and access control list described in Section 4.3.”

1. **COMMENT:** *(Page 2, line 31) - "World Wide Web (Internet)"... Clarify, www and Internet are not the same concept!.*

## **REPLY:** This has been corrected. Thank you.

1. **COMMENT:** *(Page 2, line 55) - "this research intends to use existing solutions to serve as base for \*\*\*its\*\*\* esperimentation". Rephrase and clarify: \*\*\*its\*\*\* is referring what?.*

## **REPLY:** This has been corrected. Thank you.

1. **COMMENT:** *Justify better the reasons that led you not to use any of the solutions presented, appart from yours! Clarify better WHY NOT: LinkSmart, IoT-A, iCore... Presented reasons are too fragile! Why not compare their chars with UIoT?.*

## **REPLY:** In the revised manuscript, the explanation was rewritten for each case of these relevant initiatives. The reasons to not using them were related to either these solutions do not providing an operational prototype or the respective source code. Also, we have added in Section 2.1.4 the following texts about the choice of UIoT: “*Despite it was developed independently of other proposed architectures, UIoT presents many similarities to them*” and “*Since it has an operational prototype and its architecture responds to general requirements common to other IoT middleware, UIoT was considered appropriate to be used in this paper study without any loss of generality. Besides, since its security model was yet to be proposed, it was chosen as the base middleware for this work.*”. Indeed, the source code of UIoT is available as open source in www.uiot.org, but we have considered that it was not appropriate to put a reference to this site in a research paper.

1. **COMMENT:** *(Page 5, line 35) - please develop further on how do you propose to " previously share the network key" with devices; manually and for each single device? any other (semi)automated proccess?.*

## **REPLY:** We thank the reviewer for this constructive comment. We have developed further on this subject changed and, specifically in Section 4.1, we now added the following: “*There is the possibility of performing the automatic initialization of the network keys, for example, using a reliable key distribution and certification entity (certificate authority) or obtaining a validation by a subset of peer entities able to generate a key from a subset of key parts each belonging to a pair entity (threshold cryptography). In both cases, there is an initial process of discovery of trusted entities, which is quite complex and always requires availability of connection with such entities, possibly located outside the IoT network instance. Even so, each device would have to be produced with a certified key. For these reasons, we opted for manual key sharing, by initiative of the owners of devices. In this way, we avoid both the complexity of the automatic startup and the possible new security loopholes in the automated exchange of keys. Since the device already has to be inserted in the physical environment by an administrator, at that time this administrator can add the key to the device abstraction in the middleware, simplifying the process and initializing the correct key exchange process.*”

1. **COMMENT:** *(Pafe 6, line 4-8) - discussion is too generic! How do yiu plan to use those technologies for external security?.*

## **REPLY:** We thank the reviewer for this comment. We apologize for the confusion, since we do not intend to use our proposal for external security. To remove this ambiguity we have rewritten the text to make it clear that we propose to secure the external interfaces of the IoT middleware, in the following terms in Section 4: “*This section covers the middleware internal security aspects, and those regarding its interfaces to the external world, as well as authentication procedures and the smart objects access control list (ACL). Internal security comprehends communication between master and slave controllers, while external interfaces security encompasses communication between the master controller and applications or between the master controller and system users.*”. Consequently, we renamed the concerned Subsection as “4.2 *Security of External Interfaces*”.

1. **COMMENT:** *(Page 6, line 8) - reference is missing (Ref:ddos).*

## **REPLY:** The correction of this reference has been done. Thank you.

1. **COMMENT:** *Please revise references. Do not use accentuated chars (for instance at [26]); identify clearly and in an uniform way the RFCs cited (identify proposed standards)”.*

*s*

## **REPLY:** We revised all references and the whole manuscript bibliography. Thank you.

1. REVIEWER 3
2. **COMMENT:** *The paper describes a method to add security and privacy into a middleware for Internet of Things, named UIoT. The contribution relies on a simple survey of possible security attacks and a new security model for UIoT. However, the authors should explain very well why and where the security model is new. Although the paper makes a comprehensive explanation of the security problems related with IoT and a good description of the proposed solution.*

## **REPLY:** We thank this reviewer for appreciating the contribution of our paper and for the constructive comments. During this journal evaluation process, we have maintained our attention to new developments in this paper domain, which allowed us to put forward new perspectives on the context of IoT middleware. Also, and more importantly, we have been able analyze new references on IoT security. For this reason, we have rewritten the Introduction of our paper (Section 1) to take into consideration these new contributions including contributions by ourselves. We then have strong indicators to sustain that “*To our best knowledge this is the first comprehensive published model that can be extended for any IoT middleware*” as we state in section “4.Proposed Security Model”. Accordingly, we have updated this paper references/bibliography with recent developments in the area.

1. **COMMENT:** *The colours used in figure Fig.3 are not appropriate for a journal paper.*

## **REPLY:** This figure has been corrected. Thank you.

1. **COMMENT:** *A major revision of English is required, the text presents several failures. For instance: Pag.1 ln 46, col 1: trhough->through; Pag.4 ln 22, col 2: tcp/ip ->TCP/IP.*

## **REPLY:** The whole text has been broadly and carefully revised, including the cited typos. Thank you.