Modelling Dynamic Risks in Internet-of-Things Applications

Javeria Samad
School of IT, Faculty of SEBE
Deakin University
Melbourne, Australia
jsamad@deakin.edu.au

Seng W. Loke
School of IT, Faculty of SEBE
Deakin University
Melbourne, Australia
seng.loke@deakin.edu.au

Karl Reed
Dept. of CS and IT
La Trobe University
Melbourne, Australia
k.reed@latrobe.edu.au

Abstract

Internet of things (IoT) while providing virtually unlimited opportunities, is also prone to many "risks". Risk analysis is therefore a mandatory action for any IoT system to ensure security, privacy, performance and reliability. Moreover, the complexity and structural dynamism of these mobile cloud/IoT systems further adds to the need for specialized, systematic and automated risk analysis and mitigation as well as the context awareness of risk management. This paper represents a part of our ongoing work towards creating a quantitative context-aware risk management system, suitable for dynamic mobile cloud and IoT environments, which would use the current context parameters to predict/identify potential risks and where possible, manage risks autonomously.

Keywords

context aware; risk analysis; mobile cloud; IoT

I. INTRODUCTION

The term context-aware means being alert of present surroundings (i.e. locations, environment etc.) and situations continuously, and making use of these most-current context parameters for calculating risks at any given time, which is vital given the potentially dynamic nature of mobile clouds and IoT systems. Our research [1],[2] shows that there has been little progress towards the development of cloud-enabled IoT and mobile systems risk management approaches or tools. To address this issue, we have tried to come up with a quantitative context aware risk management approach suitable for dynamic IoT environment, which will help identify as well as predict potential risks based on context information, generate respective alarms and where possible, manage risks autonomously.

The paper is organised as follows. Section II discusses briefly our Context Aware Risk Management (CARM) methodology along with corresponding risk state machine diagrams in the background of a respective case study. Section III presents an overview of application prototype and demonstrates the prototype in the light of run-time risk monitoring for selected risks items from the case study. Section IV provides conclusions and future work.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the Owner/Author.
MobiQuitous 2017, November 7–10, 2017, Melbourne, VIC, Australia
© 2017 Copyright is held by the owner/author(s).
ACM ISBN 978-1-4503-5368-7/17/11.
https://doi.org/10.1145/3144457.3144514

II. CARM METHODOLOGY

The proposed methodology CARM is designed to create a quantitative risk-aware system for mobile/IoT cloud computing that can be used for organized, timely and effective risk identification, risk assessment and mitigation for diverse cloud based mobile/IoT systems. The proposed methodology uses initial cloud based IoT system characteristics and the risk requirements to produce a risk profile as well as derive the functionalities necessary for implementation of a context aware risk management system.

The mandatory activities of CARM include planning, risk identification, risk assessment & treatment and evaluation. Some of these activities are standard to risk management procedures prevalent in other areas like finance, insurance, project management and engineering etc. [3,4,5,6] and we are intending to use these as basis of our CARM methodology.

Case Study:

To see that how these risks can affect any application, we have taken an example of a cloud based e-health application proposed in [7]. They have designed a scalable real-time health monitoring and analysis system. This prototype system collects patient data (e.g., pulse and heart beat rates) through an ECG sensor device attached to a patient's body. This sensor device transmits the data to the patient's mobile device via Bluetooth without manual intervention. A client-software on a mobile device then transfers the data to an ECG Analysis Web-service hosted on a cloud computing stack, either using Wi-Fi or mobile device's 3G network. The software then analyses the patient's data, generates results and appends the latest findings to the patient's medical record. Depending on analysis, the data could be sent to patients, doctors or emergency services as needed. Further details of the prototype system as well as the identified risks and risk scenarios, can be seen in [1]. It's a time-critical application that requires extreme levels of reliability for the data being generated and needs to be always up-to-date with the latest findings.

To demonstrate that how CARM will work, we have taken example of most basic but extremely important risk factor "resource limitations" of mobile devices. Further complex scenarios involving multiple risk factors will be presented in future works. As this app will depend on mobile devices of patients and the wrist-wearable monitor, it is crucial extremely

important to always keep those devices well powered, the failure to do which can result in life threatening consequences.

In figure 1, the functioning of CARM is represented by means of risk state machine (RSM) diagram. It shows that how any identified risk factor will go through multiple states depending on its acceptable threshold value, priority, relevance to domain, impact on overall system reliability and functioning and net risk value. How the Net risk value will be calculated for each risk item is presented in [2]. Here we will only focus on different risk states and how this state machine along with quantitative risk calculation formulas from [2] will be implemented into an actual running system for context aware autonomous risk management system.

III. APPLICATION PROTOTYPE

For the purpose of demonstration of CARM implementation, let's have a look at application prototype (focusing only on the selected risk factor from RSM above for the moment). For this particular risk, the CARM will periodically be capturing remaining battery percentage and using it as input, will be continuously comparing it against agreed upon threshold value for this particular risk. The RSM diagram pretty much represents the functioning of CARM in terms of different states this risk factor will go through before entering "mitigation" state. Its during these states that the quantitative part will be applied for risk calculations for statistical decision making. During mitigation state, the previously agreed upon risk mitigation strategies will be applied, either manually or automatically, depending on nature of risk factor. In this case, the risk treatment solution will be combination of both automatic mitigation (by deploying some pre-defined strategies) as well as manual intervention. This scenario is represented in the screen shots from sample application prototype implementation of this particular risk factor in figure 2.

Most of these calculations will be done in background and not visible to CARM user unless requested. For example, while moving from one risk state to another (depending on current context parameters and resultant risk values) , certain methods will be called that will each carry out necessary tasks to either generate alarms for manual intervention or where possible, carry out mitigation tasks automatically.

IV. CONCLUSIONS

From our previous research it's evident that there is a need for a formal risk management framework that can help in effective risk mitigation for mobile cloud computing and IoT systems. Our target is to design such an autonomous system that can deal with risks at multiple stages of the mobile cloud and IoT infrastructure, while taking into consideration the current context situations for more proactive risk mitigation. In this paper, we have presented an application prototype based on risk management ontology that can help in proactive risk assessment and mitigation in context aware manner. In future we intend to enhance this prototype further to include more risk situations from different Mobile/IoT systems.

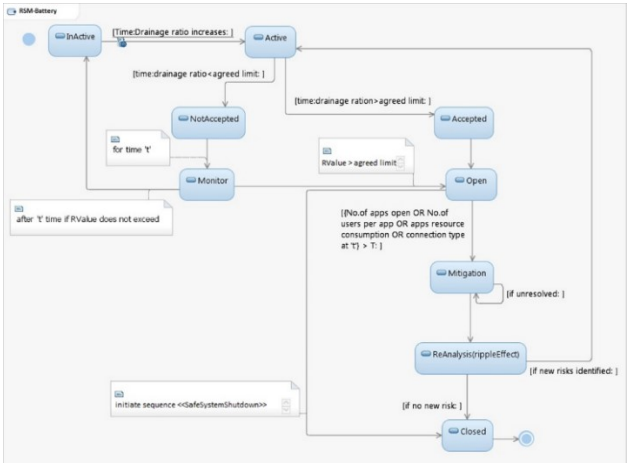

Figure 1 Risk state machine diagram for risk factor 'battery resource limitation' with respect to case study

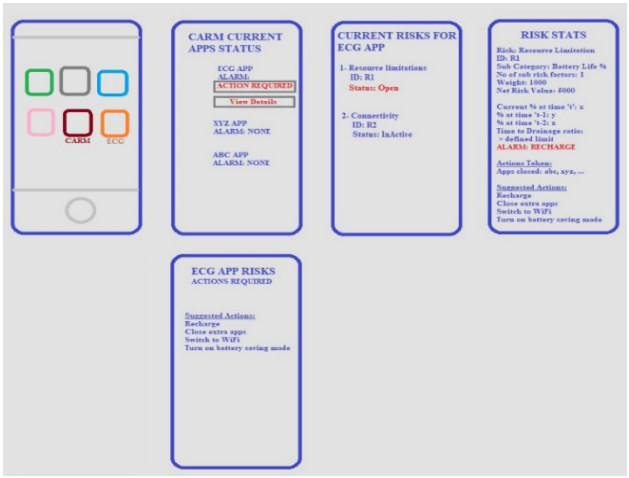

Figure 2 Sample Application prototype for risk factor 'battery resource limitation'

REFERENCES

[1] Samad, J., Loke, S. W. and Reed, K. "Mobile Cloud Computing, in Cloud Services, Networking, and Management" John Wiley & Sons, Inc, Hoboken, NJ. DOI: 10.1002/9781119042655.ch7, 2015

[2] Samad, Javeria, Seng W. Loke, and Karl Reed. "Quantitative risk analysis for mobile cloud computing: a preliminary approach and a health application case study." Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on. IEEE, 2013.

[3] Samad J., Ikram N., Usman M. "Managing Risks: An Evaluation of Risk Management Processes". IEEE International Multi-topic Conference, p.281-287, 2007.

[4] ACTIA, "Guide to Risk Management: Insurance and Risk Management Strategies", Report by Australian Capital Territory Insurance Authority, 2004.

[5] "IEEE Standard for Software Life Cycle Processes-Risk Management". Software Engineering Standards Committee of the IEEE Computer Society, (IEEE Std. 1540-2001), IEEE-SA Standards Board

[6]Standards Australia OB-007. Risk Management- Principles and Guidelines. AS/NZS ISO 31000:2009 Standards Australia and Standards Newzealand, ACT Australia, 2009.

[7] Pandey S., Voorsluys W., Niu S., Khandoker A., Buyya R. "An Autonomic Cloud Environment for Hosting Ecg Data Analysis Services". Elsevier Future Generation Computer Systems 28: p.147-154, 2012.