Intelligent risk management framework

Wissam Abbass, Zineb Bakraouy, Amine Baina, Mostafa Bellafkih
National Institute of Posts and Telecommunication INPT, Madinat Al Irfane, Rabat, Morocco

Article Info

Article history:

Received May 11, 2019
Revised Jul 29, 2019
Accepted Aug 12, 2019

Keywords:

ArchiMate
Artificial intelligence
Convolutional neural network
Internet of things
Mobile agents
Nessus
PDCA cycle
Risk management

ABSTRACT

The Internet of Things (IoT) is rapidly increasing and enhancing today's world by introducing a large set of interconnected devices. Several beneficial services are produced by these devices as for area monitoring and process control. However, IoT security is still a major problem. In fact, IoT' security beggings largely whith an effective Risk Management process. However, the essense of this process is to acquire a risk inventory cibling the IoT devices. Nevertheless, it is quite difficult to obtaining this latter which significantly adds complication issues to the Risk Management. Without the ability of holisticly identify the IoT critical devices, inaccurate Risk Management is achieved which leads unfortunately to novel risk exposures. Traditional Risk-based approaches fails drastically at apprending IoT' potential attacks. The dynamic structure, the heteregouns nature of devices, the various security objectives and infrastructure pervasiveness are key factors impacting the overall perfomance. Thus, a holistic Risk Management witihin the IoT is indispensable. Accordingly, we propose an intelligent Risk Management framework using Mobile Agents in order to deliver preventive and responsive assessment.

Corresponding Author:

Wissam ABBASS,
National Institute of Posts and Telecommunication INPT,
Madinat Al Irfane, Rabat, Morocco.
Email: abbass@inpt.ac.ma

1. INTRODUCTION

In the actual interconnected era, IoT has gradually attracted wide interest for smart management and monitoring. IoT refers to the ubiquitous network of everyday objects embedded with computing devices. It merges different technologies, standards and services in order to support intelligent decision making [1]. IoT is the key to delivering smart services, as for environment monitoring, devices tracking, smart buildings and trafficc optimization [2]. It tolerates remote control of these objects wherefore the integration of diverse architectures, design methodologies and middleware. Actually, IoT' objects collect data using distributed sensors and transmit it thanks to Internet protocols to an IoT platform for processing and storage [3]. IoT' devices are often contracted with storage issues which is a source of diverse attacks. One vulnerability is likely to be exploited by attacks which allows gaining privileged access to the entire network [4]. Moreover, due to Internet connection and the lack of security various data breaches occur leading consequently to several security concerns [5]. Back in 2016, a massive distributed denial-of-service (DDoS) attack had managed to make thousand of the Internet's top destinations inaccessible [6]. Considering the highly interconnection of these devices, one exploited vulnerability grants whole access to data, rendering it unusable [7]. Subsequently, as everyday objects become more connected, IoT security becomes crucial.

Managing risks affecting the IoT is reflected complex as regard for the large scale of the connected devices. Moreover, with the perpetual interaction of these devices novel threats are on the rise [8]. In fact, considering the interconnected infrastructure of the IoT' devices, a distributed Risk Management solution in highly required. Accordingly, this paper proposes an intelligent Risk Management framework using Mobile Agents in order to deliver preventive and responsive assessment. Indeed, using Mobile Agents is practically suitable for distributed systems such as the IoT. The proposed Framework considers two main components: preventive and responsive. On one hand, the preventive component applies Convolutional Neural Network for risk identification and classification. On the other hand, a responsive comoenent dealing with the IoT dynamic environment. Indeed, the combination of preventive and responsive approaches delivered valuable results. In fact, the Responsive Risk Analysis investigates all the relevant risks earlier, so accordingly before their potential occurrence. This investigation is then tailored as a Model-base, which a mobile agent is responsible for its management. Mobile Agents technology is the key combining the preventive and responsive approaches, shifting thus risk countermeasures decisions from the preventive approach to the responsive one. Our contribution grants security for Cloud of things without influencing its performance. The papers layout is organized accordingly into four sections: the first section reviews the Risk Management components, includes related work and introduces the research method. The second section details the proposed framework. The third section highlights an experimental analysis clarifying the key value of the proposed framework. Finally, constructive findings are pinpointed.

2. MATERIALS AND METHODS

2.1. IoT’ risk management

IoT’ Risk Management process is a countinous process of modeling the exposure of the connected devices to risk [9]. It allows identifiying, assessing and mitigating the potential risks that may potentially harm the overall performance [10]. Figure 1 depicts Risk consists of a potential threat launching an attack againt a device’s vulnerability in order to negatively impact its performance. Accodirngly, Risk Management is commonly applied in order to apply effcient countermeasures strengthening devices’ vulnerabilities. IoT’ Risk Management process consists of four main steps: risk identification, assessement, mitigation and moniroting [11]. As depicted in Figure 2, the first step considers identifying the critical devices and the related security objectives. Risk assessment is the core step of the whole process as it determines the risk’s probability of occurrence and impacts. Risk Mitigation allows deciding the adequate countermeasure while Risk Monitoring tolerates checking the adequacy pf the chosen countermeasures and serves as a key essence of launching a new Risk Identification. Risk Monitoring aims to guarantee the reliability of each Risk Management step.

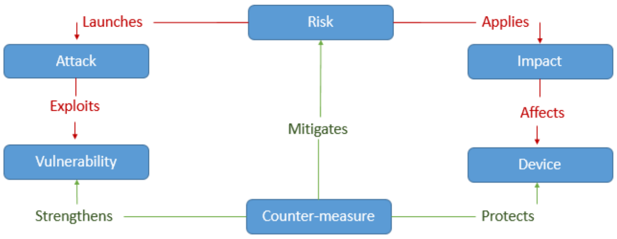


Figure 1. IoT’ Risk Management core concepts

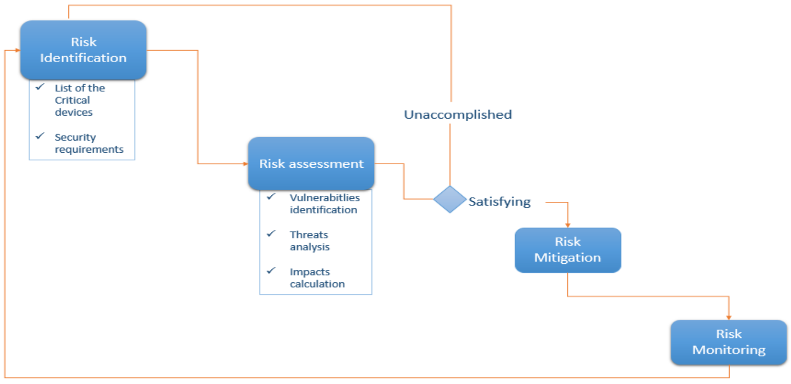


Figure 2. IoT’ Risk Management main steps

IoT' dynamic structure complicates Risk Management process. In fact, IoT devices are continuously interacting which gives rise to novel risk exposures [12]. Moreover, the interconneted devices are not managed as the traditional devices where the fact as they are often deignated as automate entities [13]. However, the absence of a common framework emerged an inconsistency at assessing risk [14].

Various challenges facing IoT Risk Mangement exist:

1. Increased number of devices.
2. Perpetual devices' communication incorporating sensitive data sharing.
3. Impotent devices' inventory.
4. Devices' complexity at determining a vulnerability impact.
5. Convoluted perception of a risk's attack expansion.

Risk Management within the IoT allows assessing the potential threats threatening the devices security. Indeed, SRA within the IoT is convulted, well mainly due to the external data storage and processing functions between IoT'heterogeneous devices. The goal of our research method is:

1. Determining IoT devices inventory,
2. Assuring IoT devices security,
3. Identifiyinf security profiles,
4. Defining efficient vulnerability reports,
5. Outlining real-time monitoring.

Actually, IoT devices include no embedded security which is quite appeling for attacks. As a matter of a fact, IoT' security beggings largely whith an effective Risk Management process. However, the essense of this process is to acquire a risk inventory cibling the IoT devices. Nevertheless, it is quite difficult to obtaining this latter which significantly adds complication issues to the Risk Management. In fact, in order to fully acnkowldge IoT benefits, it is mandatory to apply a deep analysis of the potential risks that may influence the overall security.

2.2. Related work

Using Artificial Intelligence in a quest for enhancing Risk Management is the focus of various research work. Ziegler & al. [15] relied on Mobile Agents in order to provide a security and privacy approach. However, their approach fail at holisticly enhance public trust. Game theory has been the key focus of Abie & al. [16] at estimating and predicting risk impacts within an ehealth IoT. Deng & al. [17] used machine learning methods in order to determine the network's intrusion risks. Liu & al. [18] proposed a dynamical risk assessment by relying on Artificial Immune System in order to deduce suspicious events. Nurse & al. [19] builded an impact assessment model by considering the dynamics and uniqueness of the IoT environement. We have in previous work used Deep Learning alogirthm for classifying IoT' risks [20]. Artificial intelligence enhandes significantly risks identifying and analysis [20].

3. INTELLIGENT RISK MANAGEMENT FRAMEWORK

As shown in Figure 3, the proposed framework' follows a "Do-Act-Check" cycle:

1. A preventive Risk Analysis framework which is the "Do" phase. It supports implementing security measures before risk symptoms manifest. The preventive management delivers an inventory of the risk profiles that allow identifying the critical devices. It detects and stymies IoT-based attacks. It does identify risk but does not explicitly address it. Moreover, it describes the key factors that would drive risks and provides guidance for deciding security countermeasures, viewpoints, and patterns that would help security managers better develop security models.
2. Mobile Agents are considered as the "Act" phase. Used as risk sensors embedded at IoT devices, these agents help report risk asynchronously and autonomously. Due to their autonomous aspect within the IoT infrastrucutre, they are mainly used for their ability to operate asynchronously and autonomously of the process responsible for crafting it. Indeed, they are considered as a risk sensors that collect relevant real time data.
3. A responsive Risk Analysis framework which is the "Check" phase, it responds to risks after they have happened.

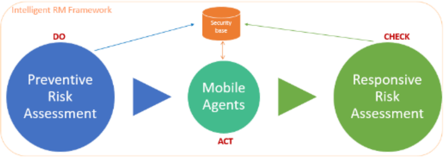


Figure 3. Intelligent Risk Management framework

Using the PDCA cycle allows matching IoT' dynamic infrastructure. In fact, it starts with a "Plan phase" which considers:

1. Scope definition,
2. Gathering a devices inventory,
3. Critical devices identification.

The planning phase represents a key element promoting the critical devices which would consist the main target. The "Do phase" considers perceiving and predicting risk occurence. As related in Figure 4, it launches two agents: the Collector Agent "Nessus" collecting data related to vulnerabilities and the Analyser Agent "ArchiMate" analysezinng this data in order to identify the potential risks and their countermeasures.

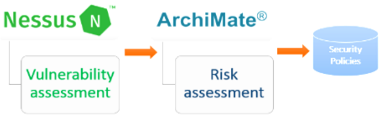


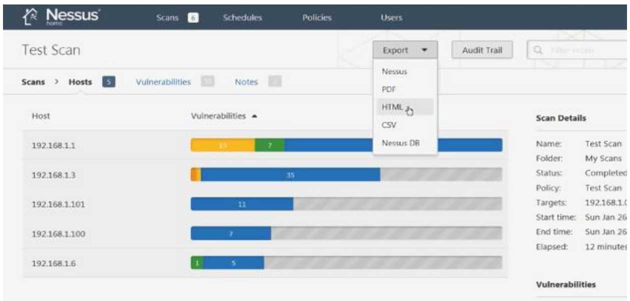
Figure 4. Preventive Risk Assessement

The Nessus tool helps beneficially detect vulnerabilities that would exploit an infrastructure. Choosing Nessus is based on the fact that it uses agents that perform scanning instructions and report it to a central Nessus Manager. Nessus cumulates the security models, which are further scrutinized by ArchiMate. The Security Model-base includes risk scenarios and the security policies. All the risk identification and analyses made by the Preventive Risk Assessment phase are represented as security models. In fact, it allows understanding and evaluating security risk exposures. It is considered as a risk inventory that contains the critical IoT devices.

4. COMPUTATIONAL ANALYSIS

Figure 5 show Nessus Vulnerability. In order to highlight the feasibility of the proposed framework, we perform firstly a Preventive Risk Assessment, which includes:

1. Vulnerability assessment: First, we have performed the vulnerability assessment using Nessus. It has beneficially helped understanding all the existing vulnerabilities and their impact. It has also supported where best to focus security controls.
2. Risk assessment: ArchiMate identifies the threats that would target the critical IoT devices.



Host	Vulnerabilities
192.168.1.1	15 7
192.168.1.3	35
192.168.1.101	11
192.168.1.100	7
192.168.1.6	1 5

Name: Test Scan
Folder: My Scans
Status: Completed
Policy: Test Scan
Targets: 192.168.1.0
Start time: Sun Jan 26
End time: Sun Jan 26
Elapsed: 12 minutes

Figure 5. Nessus Vulnerability report export

After importing the Nessus output file which the extinction is ".csv", ArchiMate interprets it with its own Enterprise Architecture Management concepts. Figure 6 pinpoints the ArchiMate interpretation of the Nessus ".csv" output.

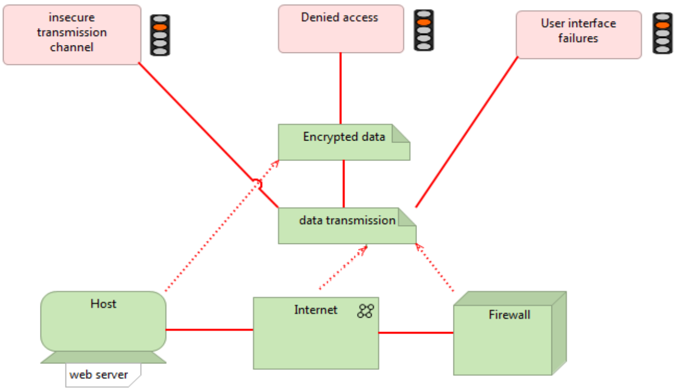


Figure 6. ArchiMate vulnerabilities assessment

After the vulnerabilities identified by Nessus are modelled by ArchiMate, the identification of risk scenarios is thus accomplished as described in Figure 7.

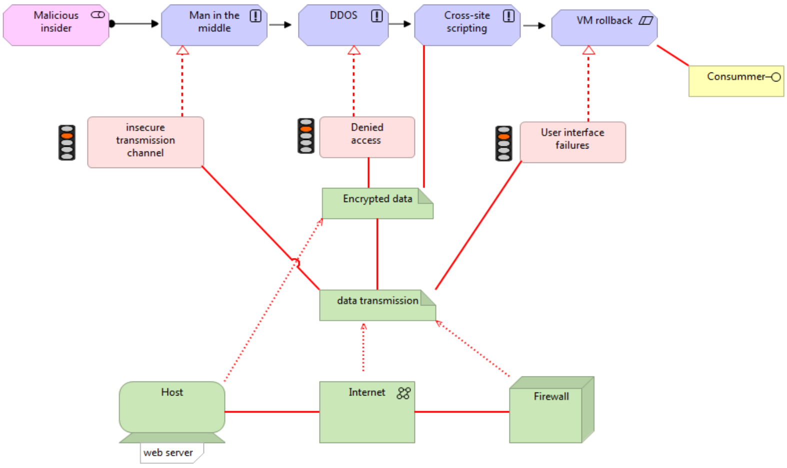


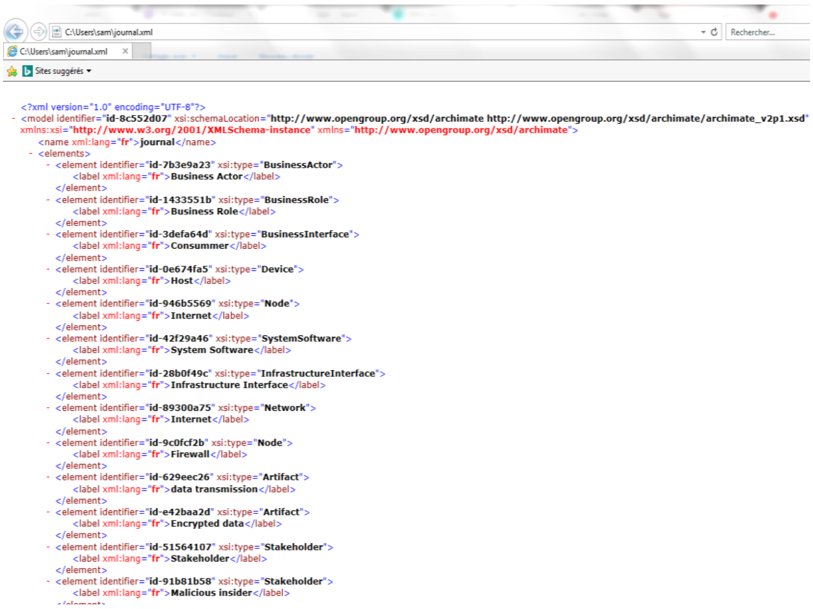
Figure 7. ArchiMate risk assessment

3. Security Model-Base: this activity stores the security measures taken in order to prevent risk occurrence. It also details the decisions made for real-time risk situations. It simply encounters the potential risks. Furthermore, the security Model-base encompasses consistent data of the entire IoT infrastrucutre.

Figure 8 shows the ArchiMate Risk Assessment output which has the ".xml" extinction. This extinction would allow us thus to a further conception of security policies. As a complement of our computational analysis, we perform then a responsive risk analysis, which comprises:

– Real-time risk mitigating: Mobile agents withstand risks as fault-tolerant systems. In fact, they work as sensors that instantly block malicious traffic. The main reason of choosing Mobile Agents is due to their swiftness to sync and transfer messages between IoT devices. Responsive Risk Assessment allows a continuous monitoring, assessment and optimizing. Nevertheless, it does not perform Risk Analysis on a daily basis but instead treats the output given by Preventive Risk Assessment, which is stored in the security Model-base and is available in real-time. Thus, Preventive Risk Assessment digest this output and correlate with Mobile Agents in order to, decide risk mitigation without delay. It convenes the

Nessus vulnerability assessment data with the network behavioural data, which relates to a genuine real-time picture of the possible occurring attacks.



```
  <?xml version="1.0" encoding="UTF-8"?>
- <model identifier="id-8c552d07" xsi:schemaLocation="http://www.opengroup.org/xsd/archimate http://www.opengroup.org/xsd/archimate/archimate_v2p1.xsd"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://www.opengroup.org/xsd/archimate">
     <name xml:lang="fr">journal</name>
   - <elements>
       - <element identifier="id-7b3e9a23" xsi:type="BusinessActor">
            <label xml:lang="fr">Business Actor</label>
         </element>
       - <element identifier="id-1433551b" xsi:type="BusinessRole">
            <label xml:lang="fr">Business Role</label>
         </element>
       - <element identifier="id-3defa64d" xsi:type="BusinessInterface">
            <label xml:lang="fr">Consummer</label>
         </element>
       - <element identifier="id-0e674fa5" xsi:type="Device">
            <label xml:lang="fr">Host</label>
         </element>
       - <element identifier="id-946b5569" xsi:type="Node">
            <label xml:lang="fr">Internet</label>
         </element>
       - <element identifier="id-42f29a46" xsi:type="SystemSoftware">
            <label xml:lang="fr">System Software</label>
         </element>
       - <element identifier="id-28b0f49c" xsi:type="InfrastructureInterface">
            <label xml:lang="fr">Infrastructure Interface</label>
         </element>
       - <element identifier="id-89300a75" xsi:type="Network">
            <label xml:lang="fr">Internet</label>
         </element>
       - <element identifier="id-9c0fcf2b" xsi:type="Node">
            <label xml:lang="fr">Firewall</label>
         </element>
       - <element identifier="id-629eec26" xsi:type="Artifact">
            <label xml:lang="fr">data transmission</label>
         </element>
       - <element identifier="id-e42baa2d" xsi:type="Artifact">
            <label xml:lang="fr">Encrypted data</label>
         </element>
       - <element identifier="id-51564107" xsi:type="Stakeholder">
            <label xml:lang="fr">Stakeholder</label>
         </element>
       - <element identifier="id-91b81b58" xsi:type="Stakeholder">
            <label xml:lang="fr">Malicious insider</label>
         </element>
```

Figure 8. Archimate Risk Assessment XML output

Figure 9 show the framework's class diagram. The main objects of the framework's class diagram are:

– "Mobile_Agent" class is the general class which models a Mobile Agent. "Collector"class is dedicated to perform vulnerabilities detection. "Analyser" class achieves risk assessment. "Locator" class is dedicated to security policies collection. "Monitor" class controls all the Mobile agents and keeps a track of an agent transit time and its tasks. In case a Mobile Agent had stopped, it launches another one to keep the work going.

– "Host_Agent" class goal is to facilitate the Mobile_Agent class objects work in the Host. It provides instance discovery and lifecycle hosting.

– "Query" class serves as an identification of the different tasks handled and controlled by the Mobile Agents.

– "Security_Policies" is a directory of all the approved security policies.

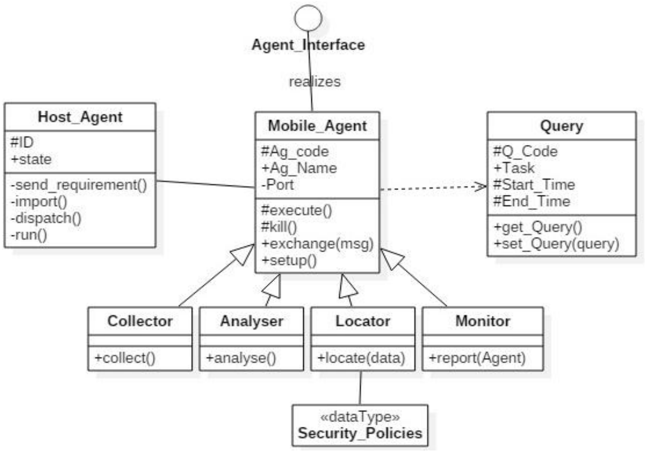


Figure 9. The framework's class diagram

Figure 10 describes the interaction between the main objects of ASRAaaS.

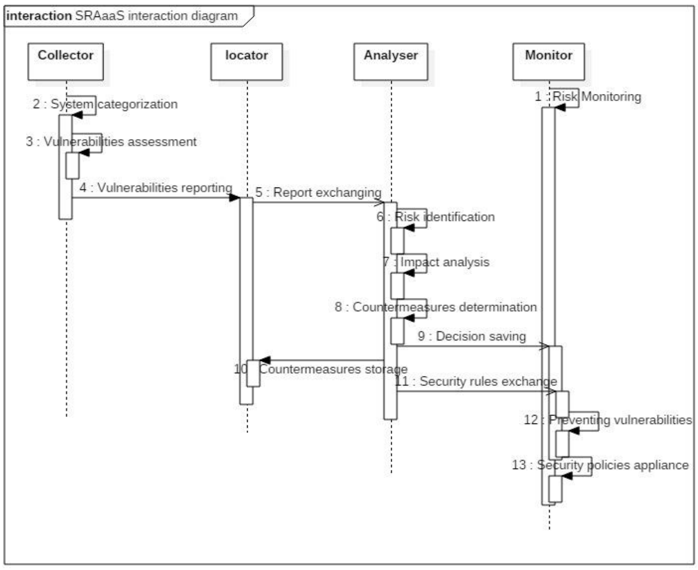

interaction SRAaaS interaction diagram
Collector
locator
Analyser
Monitor
1 : Risk Monitoring
2 : System categorization
3 : Vulnerabilities assessment
4 : Vulnerabilities reporting
5 : Report exchanging
6 : Risk identification
7 : Impact analysis
8 : Countermeasures determination
9 : Decision saving
10 : Countermeasures storage
11 : Security rules exchange
12 : Preventing vulnerabilities
13 : Security policies appliance

Figure 10. The Framework's sequence diagram

In one hand, the main advantages offered by the intelligent Risk Management framework are:

1. An Early detection of DDOS attacks owing to the Preventive Risk Assessment.
2. A flexible mitigation of the known SQL injections attacks with the Responsibe Risk Assessement.
3. Real-time monitoring with Mobile Agents detecting suspisous changes.

In the other hand, the limitations are:

1. A semi-quantitative (combining quantitative and qualitative) Risk Analysis approach should also be considered.
2. Responsive Risk Assessment only acts on the attacks identified by the Preventive Risk Assessment.
3. Only stored attacks in the security Model-base can be mitigated.
4. No experimental results are provided.
5. A continuous manually reflection must be considered.

5. CONCLUSION

The IoT has elevated the modern world to a newer level of satisfaction and evolution. In this paper, we have presented an intelligent Risk Management framework for the IoT. Usefully, it considers data history and acts taking into account the security Model-base. The framework provides idyllic solutions to preserve the confidentiality, integrity and availability of the IoT devices against malfunction behaviours. The key element is the use of Mobile Agents. In fact, they did not have an inclusive control to their data synchronization since they were operating in the IoT dynamic infrastructure. Moreover, the security Model-base has granted the Mobile Agents with a common interpretation of the IoT infrastructure and the security policies. The intelligent framework is practically based on collaborative Mobile Agents that collect data, analyze it and act on it according to the security strategy. Nevertheless, our work also includes limitations. In fact, no risk profile is generated by the Preventive Risk Analysis, no insight on how the critical devices were assessed or neither not how statistical data was captured.

Future work should consider sensors aggregating real-time data in order to be automatically analysed by the Mobile Agents. The general idea is to consider a security Model-base, which incorporate security rules accomplished by the Preventive Risk Assessment. It would evidently allow supporting a continuous Risk Assessment. From the security Model-base, the Mobile Agent will be able to determine the security state and would further perform a Responsive Risk Assessment by taking into consideration historical data. This easily triggers protective measures. Another research task is to inspect Mobile Agents reliability. The provided intelligent Risk Management framework is indeed suitable for assessing the risks facing the IoT' devices, but is tactlessly not the ultimate security solution. It is a conceptual foundation investigating the combination of preventive and responsive risk assessment in order to preserve data confidentiality, integrity and availability.

REFERENCES

[1] J. Bhattacharjee, A. Sengupta, M. S. Barik, et C. Mazumdar, « An Analytical Study of Methodologies and Tools for Enterprise Information Security Risk Management », *Information Technology Risk Management and Compliance in Modern Organizations*, IGI Global, p. 1-20, 2018.

[2] M. Gupta, R. Sharman, J. Walp, et P. Mulgund, Éd., *Information Technology Risk Management and Compliance in Modern Organizations:* IGI Global, 2018.

[3] B. Ali et A. Awad, « Cyber and physical security vulnerability assessment for IoT-based smart homes », *Sensors*, vol. 18, n^{o} 3, p. 817, 2018.

[4] T. Qiu, N. Chen, K. Li, M. Atiquzzaman, et W. Zhao, « How can heterogeneous Internet of Things build our future: A survey », *IEEE Commun. Surv. Tutor.*, vol. 20, n^{o} 3, p. 2011-2027, 2018.

[5] V. Adat et B. B. Gupta, « Security in Internet of Things: issues, challenges, taxonomy, and architecture », *Telecommun. Syst.*, vol. 67, n^{o} 3, p. 423-441, 2018.

[6] A. A. Diro et N. Chilamkurti, « Distributed attack detection scheme using deep learning approach for Internet of Things », *Future Gener. Comput. Syst.*, vol. 82, p. 761-768, 2018.

[7] S.-R. Oh et Y.-G. Kim, « Security requirements analysis for the IoT », *International Conference on Platform Technology and Service (PlatCon)*, p. 1-6, 2017.

[8] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, et S. Shieh, « IoT Security: Ongoing Challenges and Research Opportunities », in *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, Matsue, Japan, p. 230-234, 2014.

[9] J. Tupa, J. Simota, et F. Steiner, « Aspects of risk management implementation for Industry 4.0 », *Procedia Manuf.*, vol. 11, p. 1223-1230, 2017.

[10] W. Abbass, A. Baina, et M. Bellafkih, « Using EBIOS for risk management in critical information infrastructure », in *2015 5th World Congress on Information and Communication Technologies (WICT)*, Marrakech, Morocco, p. 107-112, 2015.

[11] P. Radanliev *et al.*, « Cyber Risk Management for the Internet of Things », 2019.

[12] P. Radanliev *et al.*, « Future developments in cyber risk assessment for the internet of things », *Comput. Ind.*, vol. 102, p. 14-22, 2018.

[13] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, et J. Lopez, « A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services », *IEEE Commun. Surv. Tutor.*, vol. 20, n^{o} 4, p. 3453-3495, 2018.

[14] D. E. Kouicem, A. Bouabdallah, et H. Lakhlef, « Internet of things security: A top-down survey », *Comput. Netw.*, vol. 141, p. 199-221, août 2018.

[15] S. Ziegler, A. Skarmeta, J. Bernal, E. E. Kim, et S. Bianchi, « ANASTACIA: Advanced networked agents for security and trust assessment in CPS IoT architectures », in *2017 Global Internet of Things Summit (GIoTS)*, Geneva, Switzerland, p. 1-6, 2017.

[16] H. Abie et I. Balasingham, « Risk-based adaptive security for smart IoT in eHealth », in *Proceedings of the 7th International Conference on Body Area Networks*, p. 269-275, 2012.

[17] L. Deng, D. Li, X. Yao, D. Cox, et H. Wang, « Mobile network intrusion detection for IoT system based on transfer learning algorithm », *Clust. Comput.*, 2018.

[18] C. Liu, Y. Zhang, J. Zeng, L. Peng, et R. Chen, « Research on Dynamical Security Risk Assessment for the Internet of Things inspired by immunology », *8th International Conference on Natural Computation*, Chongqing, Sichuan, China, p. 874-878, 2012.

[19] J. R. C. Nurse, S. Creese, et D. De Roure, « Security Risk Assessment in Internet of Things Systems », *IT Prof.*, vol. 19, n^{o} 5, p. 20-26, 2017.

[20] W. Abbass, Z. Bakraouy, A. Baina, et M. Bellafkih, « Classifying IoT security risks using Deep Learning algorithms », *6th International Conference on Wireless Networks and Mobile Communications (WINCOM)*, Marrakesh, Morocco, p. 1-6, 2018.

[21] M. Lu, *Artificial intelligence based risk and knowledge management*. Google Patents, 2019.