Assessing the Internet of Things Security Risks

Wissam Abbass, Zineb Bakraouy, Amine Baina, and Mostafa Bellafkih
National Institute of Posts and Telecommunication INPT, Madinat Al Irfane, Rabat, Morocco
Email: {abbass, zineb, baina, bellafkih}@inpt.ac.ma

Abstract —The Internet of Things (IoT) has extensively altered the IT landscape, allowing thus no human requirements in order to fluently communicate. However, it has introduced uncertainty which led to the emergence of a myriad of security risks. As coping with these security risks is becoming more and more challenging, the need of a new Security Risk Assessment (SRA) approach dealing with the IoT heterogeneous and dynamic paradigm is needed. Indeed, SRA is the primary means preserving the business services' confidentiality, integrity and availability. Different SRA approaches exist but applying them to the pervasive paradigm of the IoT is commonly agreed as impotent. Therefore, we provide a novel approach based on the Elasticsearch Stack Solution (ELK) and the Plan, Do, Check, Act (PDCA) cycle aimed at efficiently assessing IoT' security risks. As a result, the provided approach has skillfully dealt with the IoT dynamic environment. Furthermore, a benchmark of our novel approach and the existing approaches is successfully realized highlighting eventually the main findings.

Index Terms—Security risk assessment, IoT security risks, elasticsearch stack, PDCA cycle, attack graph, Risk register, risk management

I. Introduction

Today's organizations are largely based on an IoT infrastructure which relatively encompasses a large set of interconnected devices requiring inherently no human intervention. Actually, every device includes physical/virtual sensors and an IP address in order to connect to the Internet [1]. The IoT simply designates the bright future of our modern interconnected world [2]. However, due to its pervasive computing paradigm, security is usually neglected. In fact, serious security risks ate associated with to the IoT infrastructure. Each connected device combines serious vulnerabilities which lead to various security breaches to be launched. These security breaches include loss of sensitive data causing significant financial and reputational damage, massive distributed Denial-of-Service (DDoS) for instance the famous Mirai botnets attack. Therefore, conducting an efficient Security Risk Assessment (SRA) is of a greater value. Indeed, SRA tolerates analyzing security risks in order to act on it as quickly as possible. Yet, today's SRA must mandatory face the IoT' scalability feature, devices' diversity and the infrastructures' interrelation. Consequently, traditional SRA approaches do not sustain resistance, tolerance and resilience towards security risks occurrence. Indeed, various SRA approaches exist including standards and methods. In one hand, SRA standards (ISO/IEC 27005 and ISO 31000) include mainly best SRA practices [3]. In the other hand, SRA methods including, EBIOS [4], MEHARI [5], CRAMM [6] and OCTAVE [7], have their main security goals and processes. These SRA methods encompass mainly an empirical formalization of the SRA standards and provide practically qualitative security risks assessment based on subjective experiences, checklists and brainstorming. Both of SRA standards and methods provide an informal assessment and the obtained results are often criticized due to their subjective basis. Moreover, they are unable to adapt to the IoT dynamic infrastructure, leveraging thus a gap between risks identified at the initial state and new ones occurring later on the running state. Indeed, adopting them would adversely affect the IoT performance and security. Considering the IoT' interrelated infrastructure and its interconnected and heterogonous devices [8], the focus is accordingly shifted into a flexible approach able to extract SRA related information from different sources and act on it as quick as possible. Furthermore, risk knowledge must latterly be acknowledged [9]. Thus, resulting to the need of a novel SRA approach able to proactively and reactively assess IoT' security risks and instantly alleviate their spreading impacts.

We therefore acknowledge a novel SRA approach based on the ELK stack in order to effectively tackle these aforementioned issues. The ELK stack is highly recommended for its high availability and scalability [10]. It would provide objective assessment of the IoT security risks. The large knowledge gap about the IoT interrelated devices along with the challenge of the dynamic environment, shows that the use of the ELK stack would allow rapid assessment of the security risks. A set of the potential security risks are all indexed on the ELK stack. Considering IoT' need of great performance, ELK stack would smoothly extract reports and enable risk statistics [11]. We further strengthen our proposed approach by practically incorporating the Plan, Do, Check, Act (PDCA) cycle which perfectly matches the requirements of the IoT' ever evolving infrastructure [12]. The proposed approach focuses mainly on minimizing the IoT' tangible and intangible security risks by:

- Gathering, parsing and storing effectively SRA related information,
- Identifying the IoT devices' vulnerabilities,
- Depicting security risks' graphs.

The paper's layout is organized into four sections: the first section reviews the SRA in general and particularly

Manuscript received March 6, 2019; revised September 2, 2019.
doi:10.12720/jcm.14.10.958-964

within the IoT infrastructure. The second section introduces the proposed approach and then we highlight its utility at assessing the security risks targeting an IoT environment. Finally, section 4 summarizes our contribution and provides the key findings.

II. SRA within the IoT

Considering the continuous IoT development, a major highlight should be shed on the fact that its promotion shall not be outpaced by security risks occurrence [12]. Therefore, the key point to boost IoT' promotion is by appropriately addressing SRA. As a matter of a fact, SRA allows better designating the security measures that would suitably mitigate risks occurrence resulted from devices interconnection over the Internet [13]. Moreover, IoT' architecture is implicitly based upon an interconnected infrastructure, including:

- **The perception layer** comprising various types of sensors interacting and collecting data within the physical environment,
- **The network layer** transmitting the collected data to any specific processing system through an Internet network,
- **The transport layer** simply taking care of the data transport (the famous TCP and UDP protocols),
- **The application layer** managing data's integrity, authenticity and confidentiality.

Resulting consequently to a myriad of heterogeneous security risks [14]. Therefore, we advocate applying SRA to the IoT interconnected infrastructure as depicted below in Fig. 1.

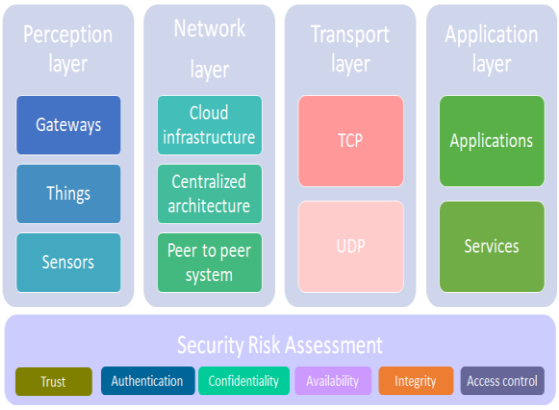

Fig. 1. SRA within the IoT

SRA within the IoT layers requires undertaking Trust, Integrity, Authentication, Availability, Privacy and Access control management [15]. An attacker would easily affect these layers by easily targeting a physical vulnerability as altering parameters of the routing protocols or launching malicious applications [16]. We classify IoT' security risks into three main categories: physical, network and application attacks, as shown in Table I. In fact, the main goal of our research work is to apprehend networks attacks within IoT network layer.

TABLE I. SECURITY RISKS TARGETING IOT LAYERS

IoT layers	IoT Security risks
Perception	Node jamming and tampering, malicious Node Adware.
Network	DoS/DDoS, Sinkhole, selective forwarding, Packets altering and Worm.
Application	DoS/DDoS, Viruses, Malicious scripts, Phishing and Man in the Middle.

Our main goal is to capture all the IoT' SRA related information which basically concerns the security risks' three basic factors: threats, vulnerabilities and impacts [17]. Actually, the existing SRA approaches only target one specific factor leading thus to inadequate and insufficient SRA [18]. Furthermore, these approaches differ from each other in terms of the targeted scope and the conducted analytical process [19]. As a matter of a fact, security risks are inherently present anywhere at any time and are able to quickly evolve [20]. Unfortunately, the existing SRA approaches are unable to deal with the IoT' dynamic infrastructure [21]. In fact, they systematically identify the critical devices as static objects and do not take into consideration the devices complexity and pervasiveness or neither the environment where they evolve [22]. Consequently, this leverages a gap between risks identified at the initial state and new ones occurring later on the real time [23-24]. The main goal of our research work is to provide SRA in real time. Accordingly in this paper, we acknowledge providing a novel SRA approach that suits the dynamic feature of the IoT in order to accurately prioritize and treat risk [25]. Our contribution is mainly based on the ELK stack and PDCA cycle in order to effectively tackle the aforementioned challenges. ELK has efficiently showed its ability to analyze security logs analysis which is highly beneficial for conducting SRA in real time [26]. The provided approach focuses on providing objective and rapid assessment of the IoT security risks.

III. The Proposed Approach

The proposed approach is primarily based on the ELK stack, as we acknowledge being commonly compatible with the IoT' infrastructure scalability. We have chosen it in order to provide fast and objective assessment of the IoT security risks. By fast assessment, we highlight as quickly as possible collecting SRA related information and depicting it in reports and statistics. In fact, considering the interconnected infrastructure of the IoT, ELK stack would allow analyzing large amounts of data from different sources of devices' location for later security risks processing and treatment. ELK stack is a beneficial approach for providing real-time security risks analysis.

Therefore, our approach core concepts include three basic components:

- **Logstash** which the component responsible for simultaneously collecting data from multiple sources and transferring it to a specific destination which is the core component "Elasticsearch". As IoT devices are located in different location, this component would collect their log files.
- **Elasticsearch**, an open source information retrieval library written in Java, will serve as a data storage, search and analytics engine. It is considered the key component of the whole approach. The output of Logstash serves as input for the Elasticsearch and then stores it in order to subsequently decide the suitable security controls measures (as to whether ignore the risk or plan and implement control policies.
- **Kibana** entails a web-based interface that eventually provides search queries for the controls measures and display the assessment of the security risks related information. It simply tolerates visualizing data from Elasticsearch in order to make sense of it.

Indeed, the main goal of the approach is to extract and visualize logs files thanks to Logstash and to later store it in the Elasticsearch in order to later act on the SRA timestamping information. These three basic components have a key role in the real time workflow of parsing, analyzing and displaying the IoT' SRA related information. ELK stack is mainly chosen thanks to its reliability, customized dashboards and adequate security regarding these tasks. Furthermore, our approach allows acknowledging a Risk Register serving subsequently for security policies retrieving. Moreover, in order to better use these key components we have incorporated the PDCA cycle. Fig. 2 highlights the proposed approach main terminology.

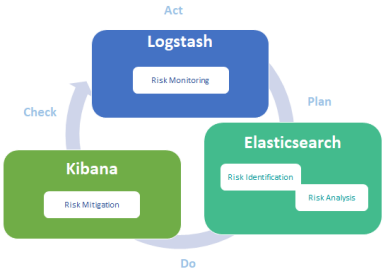

Fig. 2. The proposed approach main terminology

It entails:

- **A Planning phase** in order to effectively designate the organizational vision. This phase would primarily identify the critical assets and the potential risks that may target the global security.
- **A "Do" phase** formulating the needed security controls to be implemented.
- **A checking phase** that would inspect the feasibility of the chosen security controls. It mainly reviews the security risks' level.
- **A monitoring phase** checking the security controls in order to be extended and integrated into corporate policies. This phase basically triggers preventative actions (ACLs, countermeasures) and maintains a display of the SRA related information.

The PDCA cycle adds a significant advantage to the ELK tack as it allows our approach to be systematically documented, communicated and continually improved. Accordingly, our work tolerates responding to changes, displaying SRA related information and emphasizing security risks knowledge. It basically promotes translating the security risks assessment into elementary controls. Thanks to the Logstash, the proposed approach performs basically logs collection allowing thus risk knowledge and situational awareness. Elasticsearch serves accordingly as a Risk Register while Kibana assists creating risk profiles. For each critical asset is assigned a graph depicting the related risks, their probability of occurrence, their level of severity and risk history with the used countermeasures back then.

Our work's feasibility has been proved within an end-to-end system where its main business services include daily interactions between different devices. The daily interactions are considered critical and highly beneficial to the overall performance wherefore the compulsory needs of a new SRA approach securing these dynamic interactions. The conducted SRA comprises an excel file depicting a large set of the main security risks. These security risks are commonly identified through questionnaires. The implementation has consisted at first for processing the collected logs with Logstash. These collected logs were handled by Logstash as events and shipped off to Elasticsearch. Then, we have parsed this storage engine in order to determine the gaps between the current state and the target state which always designated the secure state. In case of differences preventative actions would be triggered. Otherwise, the new risks would be stored and the new statistics would be altered in order to add the new level of severity. The main added value of ELK stack is its ability to specify timers for every step. Accordingly, the implementation has incorporated:

- **The initial step** which as related in Fig. 3 consist of collecting logs. Actually, logstash mainly was selected as it allows obtaining and analyzing data in real time.

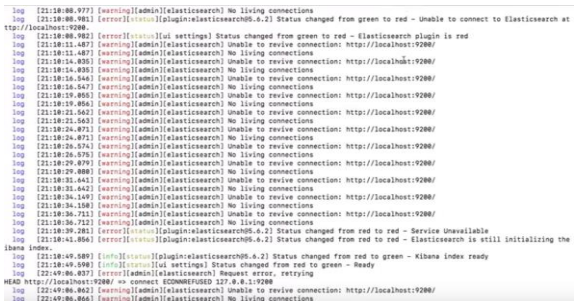

Fig. 3. Risk logs

Indeed, collecting the risk logs is a critical task which is considered as the main trigger influencing the start of the SRA process. Capturing these logs allows perceiving what is being processed within the dynamic infrastructure. It results accordingly into beneficially integrating the real time execution within the SRA process.

- **The core phase** storing the risks logs in order to usefully act on it and make sense of it. (Fig. 4).

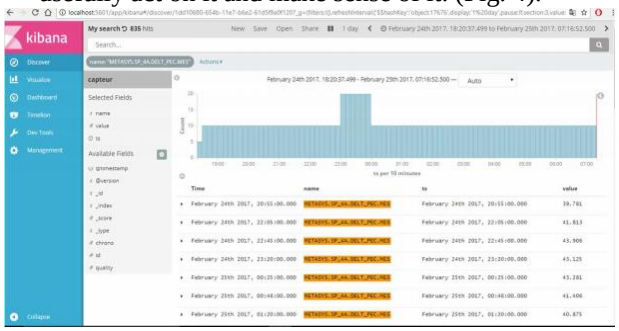

Fig. 4. SRA related information storage

Furthermore, as already mentioned the SRA related information storage is basically done as a JSON format which is highlighted in Fig. 5.

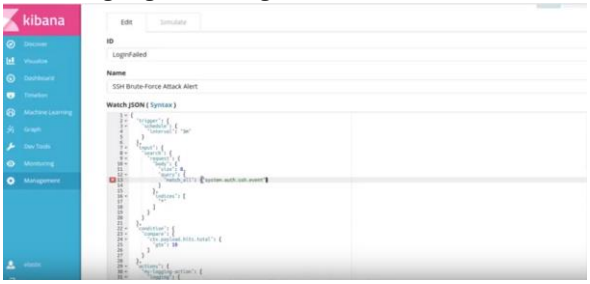

Fig. 5. SRA related information JSON format

The JSON format is a key factor that is meaningfully contributing to the reasoning, evolution and traceability of the SRA related information. Actually, thanks to the ELK stack open source feature, the JSON format file can be adapted with new features allowing further analysis and enhancement.

Fig. 6 reflects the Elasticsearch ability to parse its Risk Registry.

Fig. 6. Security risks registry

- **The finale phase** displaying SRA reports and statistics. (Fig. 7)

Fig. 7. Kibana's display of the SRA related information

As depicted in Fig. 8, Kibana displays the security risks related information. In fact, each risk has been associated with the exploited vulnerabilities.

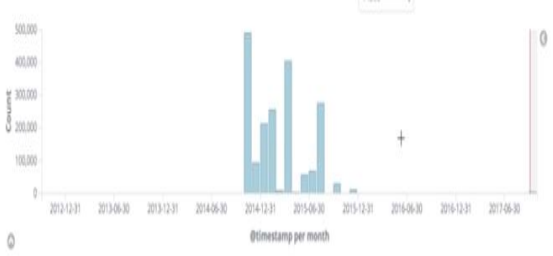

Fig. 8. Security Risks statistics

Moreover, every critical asset is associated with security risks statistics which eventually shows the risks that may threaten its security.

SRA standards remain the main SRA drivers upon which every approach rely on. Semi-quantitative and quantitative methods are unfortunately not security oriented but rather focus on quantifying the risk's occurrence (either with values or numbers). Our main goal is to also quantify risk but to correspondingly allow a dynamic display SRA related information. On one hand, Security modeling languages are beneficially useful when modeling cost-effective decisions related to the overall security. Additionally, they are often used for modeling risk impact and probability at the initial system conception. ArchiMate on the other hand is advantageously integrating the Enterprise architecture within the SRA process. It is mainly used for aligning the IT/business services. The qualitative approaches discussed earlier have been over the years the key tools used for conducting SRA. EBIOS is commonly the most chosen method. It is simple at use, fits perfectly to any type of infrastructure. The Octave and CRAMM methods differ basically from EBIOS by being mainly dedicated to large infrastructures. However, the main focus when choosing an approach relies largely on the formalized input. Moreover, the primary goal of using these approaches is to be able to gain knowledge about risk occurrence. Most of security risks analysts apprehend questionnaires and result creating CSV Excel file gathering risk knowledge. Actually, the existing SRA approaches do provide that but each one with its own sophisticated output. Yet, this output is commonly considered acceptable and practically every organization is relying on it and only focusing efforts on applying countermeasures. Indeed, applying countermeasures without a deep dynamic analysis allows the emergence of new types of security risks. Moreover, considering the output's format each approach results lack formality. Actually, their results consist mainly on table and natural language text. Consequently, these approaches are insufficient at proving reasoning, evolution and traceability of the SRA related information. The main disadvantage of the aforementioned SRA approach is their resulted output. Accordingly, the proposed Enterprise SRA offers a solution to address these

limitations. The work presented in this paper has consolidated efforts in order to be able to significantly share SRA related information, to realize security risks' statistics and to safeguard every security actions. The proposed enterprise SRA approach has provided a SRA with document oriented format schema free. It has contributed at changing the SRA results from tables into JSON documents. This change contributes meaningfully to the reasoning, evolution and traceability of the SRA related information.

Moreover, the provided approach has been tested in practice and SRA has been successfully improved within an end-to-end system. It has effectively dealt with the traditional approaches' underlined limitations.

IV. Conclusion

Our main idea has consisted of using Logstash as a collector, Elasticsearch as a streaming component and Kibana as a user interface displaying security risks' statistics. Using this approach has beneficially allowed examining different risk reports, stats and dashboards. It has fundamentally acknowledged translating the analysis of security risks into elementary controls. Thanks to the approach's modules, dynamic risk knowledge can be gathered which would later allow developing a situational awareness. ELK stack benefits SRA by:

- Displaying the critical assets' vulnerabilities;
- Analyzing logs and making sense of it;
- Classifying the security risks;
- Depicting the attack's graphs;
- Displaying the SRA related information.

SRA within the IoT is currently considered as a critical concern which allows highly gaining a competitive advantage. It has tremendously heightened the attention thanks to its ability to deal with the tangible and intangible security risks.

The work presented in this paper has produced a novel approach that can be used as a tool for the SRA within the IoT. It is designed to complement the existing SRA approaches and not replacing it. The obtained results have shown our contribution's feasibility within the IoT scalable infrastructure. Indeed, it has flawlessly depicted security risks' statistics that successfully lead to an effective security effort. The approach is distinguished by the PDCA cycle integration which largely emphasizes and enhances SRA knowledge. The ELK approach has allowed using various modules for risk mapping and analysis. It has consisted of assisting security analysts in capturing logs, storing then parsing and displaying them in order to output security risks' statistics. The inputs were risks logs which approximates the real time execution integration. The output is customizable and can be filtered in order to match the need. An implementation of the proposed approach has been depicted in order to illustrate its feasibility. Although the approach emphasizes SRA knowledge, it lacks a systematic knowledge protection strategy. Moreover, one of the main key of constructing the enterprise SRA approach was the opportunity to leverage access list from the collected and stored data. Yet, no clue has been conceived. This context is a main factor bearing a highly concern to focus on. Indeed, the idyllic is to act on the identified risks as quickly as possible. Thus, the proposed approach should mandatory include a proactive side in order to patently differ from the existing approaches.

As Future research, we plan focusing on adding authentication and authorization. Indeed, we consider connecting an Active directory or LDAP in order to attribute roles to users and restrict access. SRA is always followed by reports we therefor intend to further explore the need of on-demand and scheduled risk reports. Moreover, we suggest controlling the ELK's performance and its influence upon the IoT' overall security.

References

[1] F. Wortmann and K. Flüchter, "Internet of things," *Business & Information Systems Engineering*, vol. 57, no. 3, pp. 221-224. 2015.

[2] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10-28, 2017.

[3] J. Mcdonald, N. Oualha, A. Puccetti, A. Hecker, and F. Planchon, "Application of EBIOS for the risk assessment of ICT use in electrical distribution sub-stations," 2013.

[4] A. Syalim, Y. Hori, and K. Sakurai, "Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide," in *Proc. International Conference on Availability, Reliability and Security*, 2009, pp. 726-731.

[5] B. Corcoran, "A qualitative risk analysis and management tool – CRAMM," 2002, p. 13.

[6] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing OCTAVE allegro: Improving the information security risk assessment process," Carnegie-Mellon Univ. Pittsburgh PA Software Engineering INST, CMU/SEI-2007-TR-012, 2007.

[7] J. Tupa, J. Simota, and F. Steiner, "Aspects of risk management implementation for Industry 4.0," *Procedia Manuf.*, vol. 11, pp. 1223-1230, 2017.

[8] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266-2279, 2013.

[9] S. Lins, S. Schneider, and A. Sunyaev, "Trust is good, control is better: Creating secure clouds by continuous auditing," *IEEE Trans. Cloud Comput.*, vol. 6, no. 3, pp. 890-903, 2018.

[10] J. Eriksson, *Threat Politics: New Perspectives on* Security, *Risk and Crisis Management: New Perspectives on Security, Risk and Crisis Management*. Routledge, 2017.

[11] K. Liu, M. Wang, W. Zhu, J. Wu, and X. Yan, "Vulnerability analysis of an urban gas pipeline network considering pipeline-road dependency," *Int. J. Crit. Infrastruct. Prot.*, 2018.

[12] D. Sameer and K. Swaminathan, "Efficient surveillance and monitoring using the ELK stack for IoT powered Smart Buildings," in *Proc. 2nd International Conference on Inventive Systems and Control (ICISC)*, India, 2018.
[13] A. Cook, H. Janicke, L. Maglaras, and R. Smith, "An assessment of the application of IT security mechanisms to industrial control systems," *International Journal of Internet Technology Secured Transactions*, vol. 7, no. 2, p. 144, 2017.
[14] A. M. Ghiran, R. A. Buchmann, and C. C. Osman, "Security requirements elicitation from engineering governance, risk management and compliance," in *Proc. Springer International Working Conference on Requirements Engineering: Foundation for Software Quality*, Netherland, 2018, pp. 283–289.
[15] M. Panjwani, M. Jäntti, and J. Sormunen, "IT service management from a perspective of small and medium sized companies," in *Proc. 10th International Conference on the Quality of Information and Communications Technology*, Portugal, 2016, pp. 210–215.
[16] J. Tupa, J. Simota, and F. Steiner, "Aspects of risk management implementation for Industry 4.0," *Procedia Manuf.*, vol. 11, pp. 1223–1230, 2017.
[17] W. Abbass, A. Baina, and M. Bellafkih, "Survey on information system security risk management alignment", in *Proc. International Conference on Information Technology for Organizations Development*, Morocco, 2016, pp. 1–6.
[18] W. Abbass, A. Baina, and M. Bellafkih, "Improvement of information system security risk management," in *Proc. 4th IEEE International Colloquium on Information Science and Technology*, Morocco, 2016, pp. 182–187.
[19] H. Holm, T. Sommestad, M. Ekstedt, and L. Nordström, "CySeMoL: A tool for cyber security analysis of enterprises," in *Proc. 22nd International Conference and Exhibition on Electricity Distribution*, Sweden, 2013, pp. 1–4.
[20] S. Lins, S. Schneider, and A. Sunyaev, "Trust is good, control is better: Creating secure clouds by continuous auditing," *IEEE Trans. Cloud Comput.*, vol. 6, no. 3, pp. 890–903, 2018.
[21] M. A. Van Staalduinen, F. Khan, V. Gadag, and G. Reniers, "Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructure," *Reliability Engineering & System Safety*, 2017.
[22] A. Marrella, M. Mecella, B. Pernici, and P. Plebani, *Design-time Models for Resiliency*, InConceptual Modeling Perspectives, Springer, Cham, 2017.
[23] Z. Bakraouy, A. Baina, and M. Bellafkih, "Availability of web services based on autonomous classification and negotiation of SLAs," in *Proc. 6th International Conference on Multimedia Computing and Systems*, Morocco, 2018, pp. 1-6.
[24] Z. Bakraouy, A. Baina, and M. Bellafkih, "System multi agents for automatic negotiation of SLA in cloud computing," in *Proc. International Conference on Innovations in Bio-Inspired Computing and Applications*, Morocco, 2017, pp. 234-244.
[25] W. Abbass, Z. Bakraouy, A. Baina, and M. Bellafkih, "Classifying IoT security risks using Deep Learning algorithms," in *Proc. 6th International Conference on Wireless Networks and Mobile Communications*, Morocco, 2018.
[26] Son, S. Jun, and Y. Kwon, "Performance of ELK stack and commercial system in security log analysis," in *Proc. the 13th Malaysia International Conference on Communications (MICC)*, Malaysia, 2017.

Wissam Abbass was born in Rabat, Morocco. In 2012, she received her B.S. degree from the University of Science of Tetouan (USTC), in Software and network engineering and in 2014 her M.S. degree from the University of Science of Marrakech in Information systems security. She is currently pursuing a Ph.D. degree at the National Institute of Posts and Telecommunications (INPT) in Rabat. Her research interests include Computer networking, Web development, Network and software security, risk management and A.I.

Zineb Bakraouy was born in Rabat, Morocco. She obtained her DUT in 2012 at ENSET Rabat in software engineering and networks, and Bachelor's degree in 2013 at ENSET Mohammedia in computer system and network, then Engineer degree in 2015 at ENSA El Jadida in Telecommunications and Networks Engineering. She is currently in her fourth year of her PhD in networking studies at INPT Rabat. Her research interests center around the availability in critical infrastructures. Her current research is how to use Multi agent system for negotiation of SLA and to build an Available system: infrastructures, platforms and services.

Amine Baina received the PhD thesis in Computer Science from the National Institute of Applied Sciences (INSA) in Toulouse, France, in 2009. He is an Assistant Professor in computer science at the National Institute of Posts and Telecommunications (INPT) in Rabat, Morocco 2010. His research interests are critical infrastructures protection, Electrical Grid, Information Security.

Mostafa Bellafkih was born in Oujda, Morocco. He received the PhD thesis in Computer Science from the University of Paris 6, France, in June 1994 and Doctorat Es Science in Computer Science (network field) from the University of Mohammed V in Rabat, Morocco, in May 2001. He is a professor at the National Institute of Posts and

Telecommunications (INPT) in Rabat, Morocco since 1995. His research interests include network management, Systems security, knowledge management, A.I., Data mining and Software Engineering.