ISSN 2278-3091

Volume 9, No.5, September - October 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse315952020.pdf

https://doi.org/10.30534/ijatcse/2020/315952020

Security Risk Assessment for Internet Of Things based Forest Fires Detection System

Ghizlane Benzekri[1], Omar Moussaoui[2], Ali El Moussati[3], Idrissi idriss[4]

[1]MATSI Lab ESTO, Mohamed First University, Oujda, Morocco, ghizlane.benzekri@gmail.com

[2]MATSI Lab ESTO, Mohamed First University, Oujda, Morocco, o.moussaoui@ump.ac.ma

[3]Department of Electronics, Informatics and Telecommunications, ENSAO, Mohamed First University, Oujda, Morocco, a.elmoussati@ump.ac.ma

[4]MATSI Lab ESTO, Mohamed First University, Oujda, Morocco, idrissi@ump.ac.ma

ABSTRACT

The Internet of Things (IoT) refers to all physical devices or objects that receive and transfer data over wireless networks, without human intervention. Actually, various applications have adapted IoT technology. Among this application is the IoT-Forest Fires Detection System, which aims to provide 24/7 forest fire monitoring and detection. So, the adaptation of IoT technology poses new security challenges, which make Forest Fires Detection System being insecure and extremely vulnerable to different types of security attacks. Therefore, it is necessary to develop a complete vision of the security status of Forest Fires Detection System by identifying the possible security risks. In this context, this article applies the (OCTAVE) Operationally Critical Threat, Asset, and Vulnerability Evaluation methodology, to specify the security risks, to highlight the various security vulnerabilities and to propose adequate countermeasures to mitigating the identified risks. Hence, we can use the research result for developing the security policy and the security requirements of Fires Detection System.

Key words: The Internet of Things (IoT); IoT Forest Fires Detection System; Security risk; Security threats; Security vulnerabilities; OCTAVE methodology.

1. INTRODUCTION

The 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.

The IoT Forest Fires Detection System is one of the services based on IoT technology. This system reduces the cost and time of human resources and can save lives and reduce loss of property: if a fire is detected at an early stage and immediate action is taken.

Nevertheless, the deployment of IoT technology for building the Fire Detection System, taking into consideration the process of automation and control processes, presents new security challenges. Thus, IOT Forest Fires Detection System requires a good visibility about security requirements: an IoT-Forest Fires Detection System is highly vulnerable to attacks via the Internet. If the system is hacked, the attacker can invade the system operation, access or alter sensitive information and causes system Failure.

Therefore, this article describes the application of the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology [1] to identify security risks originating from IoT-Fire Detection System. After that, several countermeasures are proposed for mitigating the identified security risks. This contribution should be used to ameliorate the security policies for IOT Forest Fires Detection System.

The rest of this paper is structured as follows: Background section introduces essential concepts to understand this work: The Forest Fires Detection System, security risk assessment concept and risk assessment methodologies. Section 3 present related works and the motivation for choosing Octave methodology. After that, in Section 4 explain the application of the methodology to the addressed problem, these section concern research findings, discussion in terms of possible threats and identified risks. Finally, conclusion and planned future work are provided in Section 5.

2. BACKGROUND

2.1 Forest Fires Detection System

The IoT forest fire system [2] aims to provide 24/7 forest fire monitoring and detection “Fig. 1”. It reduces the cost and time of human resources and can save lives and reduce loss of property: if afire is detected at an early stage and immediate action is taken.

As we can see in “Fig. 1”. There are four main components in this system: sensor nodes, gateways, internet servers and end users (for example, firefighters and the public, etc.). In order to detect a fire, IoT sensors must be distributed around the forest. However, the communication between sensors and receivers to exchange data is made by LoRa suitable for long-range communication [3].

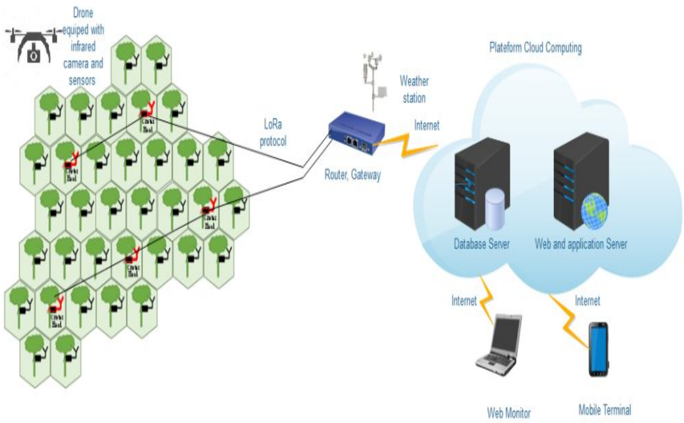

Figure 1: Structure of the proposed Forest Fire detection system

After collecting the data, the gateways push the data to the Internet using the MQTT communication protocol via the cellular network. The data is then stored on the Internet server with open-source IoT platform, and is displayed in an online dashboard “Fig. 2”, In addition, gateways issue alarms to users via Telegram instantly if they determine that a fire is happening somewhere.

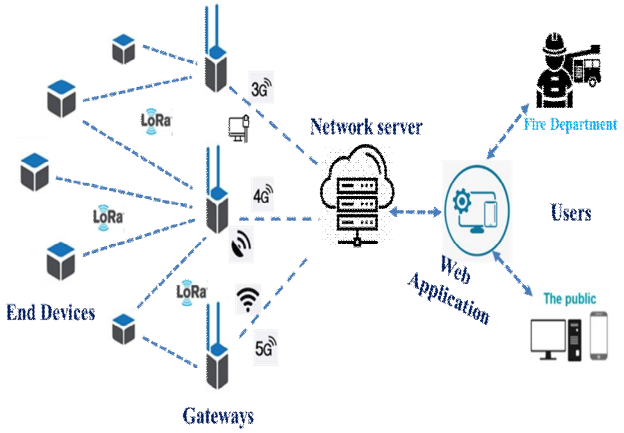

Figure 2 : IoT Fire Detetction system - Network architecture

2.2 Security risk assessment

There are several definitions given to the term of security risk assessment. According to NIST Standard, security risk assessment can be defined as the process of identifying, estimating, and prioritizing risks to organizational assets and operations [4]. Security risk assessment provides a basic vision to any security study. It gives the possibility to identify threats, impacts, vulnerabilities, and mechanism to mitigate the impacts.

The risk assessment process is based on four steps [5]:

Identification: in this step, all critical assets of the technology infrastructure are determined. Then specify sensitive data that is created, stored, or transmitted by these assets and create a risk profile for each asset.

Assessment: adopting assessment approach or methodology in order to analyze the correlation between assets, threats, vulnerabilities, and mitigating controls.

Mitigation: define a mitigation approach and enforce security controls for each risk.

Prevention: implement tools and processes to minimize threats and vulnerabilities.

2.3 Risk Assessment Methodologies

Several methodologies, standards and frameworks are used for conducting risk assessments; each of them has its own stages:

The NIST approach: National Institute of Standards and Technology’s approach [6] focuses on first steps which are: identifying threat sources and events, identifying the vulnerabilities and impact of threat events, before then specifying risks. Nevertheless, the NIST guidance is usually used for Federal Agencies and has needed more adaptations to be applicable to enterprises.

The International Organization for Standardization ISO [7] contains two important standards which are used in defining security and cyber security requirements which are ISO 27032 and ISO 27001.

The Capability Maturity Model Integrated (CMMI) [8] brings together several practices that enable the analysis and design of systems, software engineering and management. CMMI can generally improve the risks of the business production cycle. However, it can be difficult to develop CMMI measures.

The Common Vulnerability Scoring System (CVSS) [9] brings together practices, standards and guidelines useful in the industry. CVSS helps determine the severity and specifications of vulnerability by converting a qualitative input to a digital output.

Another approach is OCTAVE Operationally Critical Threat, Asset, and Vulnerability Evaluation method [10]. It’s a method which allows determining the risks, threats and vulnerabilities of a system by using worksheets for each step in order to clarify the different security aspects. It is an open source method that adapts to systems with limited resources. It can even be used to establish other risk identification methodology.

(

The Factor Analysis of Information Risk [11] is a standard quantitative risk analysis method for information security and operational risk. Indeed FAIR makes it possible to understand, measure and analyze the risk, but difficult to use given the lack of documentation and the lack of examples of the use of this methodology in concrete examples.

The Threat Assessment & Remediation Analysis (TARA) [12] is a qualitative analytical model that captures the most critical system threats and vulnerabilities. However, it cannot determine the impact of cyber risks.

CyVaR [13] a quantitative risk assessment method, but does not perform a full assessment due to the lack of required risk data. So, this makes CyVaR as a difficult method to implement, in order to assess risks and their impacts.

3. RELATED WORK AND MOTIVATION FOR CHOOSING OCTAVE METHODOLOGY

3.1 Related Work

In order to motivate the need for risk assessment security in IoT system, several works and efforts have been recently spent, in both literature and research academies. So various risk assessment studies are available:

The study in [14] discusses the risks of the agricultural supply chain under IoT and classifies and summarizes the risks of the current agricultural supply chain through qualitative analysis. The authors measure the size of the risk factors from a quantitative perspective based on a mathematical model. Finally, according to the calculations of the model, several measures of risk management and control are proposed for the agricultural supply chain under IoT.

In [15], the authors introduce an innovative risk-based adaptive security framework for IoT in eHealth to estimate and predict risk damages and future benefits, and to learn identified new or unknown threats to IoT eHealth systems. The framework is based on a continuous cycle of adaptive risk management, adaptive security monitoring, predictive analytics, automated adaptive decision-making, and evaluation and validation metrics.

The study in [16] present a contribution to the development of the risk assessment approaches that enables to evaluate project reliability and facilitates the analysis of a systems vulnerability. Results of this research can also be applied as a preventive approach that helps decision makers to improve their business model reliability.

In [17] a risk management methodology is proposed, this methodology aims to design such an autonomous system that can deal with respective risks at multiple levels of the mobile cloud and IoT infrastructure, while taking into consideration the current context situations for more proactive risk mitigation.

The study of [18] presents a methodology to model threats and risk analysis of IoT systems with an automated process. Starting from the system model, built in compliance with the ISO/IEC 30141 standard directives, and thanks to the information collected in a threat catalogue, the proposed process enables to identify applicable threats, evaluate the risk associated with such threats, and determine the countermeasures to enforce in terms of security controls.

In [19] , the focus of the research was the conduction of a comprehensive security risk assessment for IoT – based Smart Homes, this contribution give an overview of the security threats, impacts, risks, and approaches to ensure the security of the smart home environment.

The authors in [20] gives a board overview of IoT by describing the working of layers and then discusses different security loopholes on different layers of IoT (Physical layer, Network Layer, Processing Layer and Application Layer). Furthermore, it presents the countermeasures against security threats from the prevention of any damage to IoT network.

In [21], the contribution of this work presents new challenges on security risks at the level of IoT technology. This contribution is based mainly on the analysis of other research works and allows giving visibility on the mitigation of vulnerabilities at the level of the layers of the IOT.

3.2 Motivation for choosing Octave Methodology

When we want to apply security risk assessment to any system, we must to know what to protect and why. It is obvious that protecting information assets is a necessary component of protecting fire detection system security as it determines feasibility and success of this system. So, we have concentrated in this article mainly on the security of the information assets of the fire detection system given the criticality of the information in the proper functioning of this system. However, when we focus on the information assets in the assessment, all other important assets can be easily assessed and processed as locations of the information assets where they live. For this purpose, we are adopted OCTAVE Allegro methodology as it is best suited to answering the risk assessment questions:

1. What are the emerging security threats from fire detection system?
2. What are the consequences of these threats (Impacts)?
3. Are there suitable countermeasures to propose?
4. What to recommend the users?

The OCTAVE methodology was used to have a complete and comprehensive vision of the risks, vulnerabilities and impacts on information assets. So, it is best suited to answering the research problems compared with other security risk assessment methodologies that were considered. It consists of eight steps that are organized into four phases. As shown in “Fig. 3”.The Octave method is based on four major phases eights steps. With the help of worksheets provided by the methodology we can capture the outputs from each step in the risk assessment and use them to input into the next step which follows. In this way it enables us to keep continuous focus on the asset step by step during the process of risk assessment and explore problematic situations more easily.

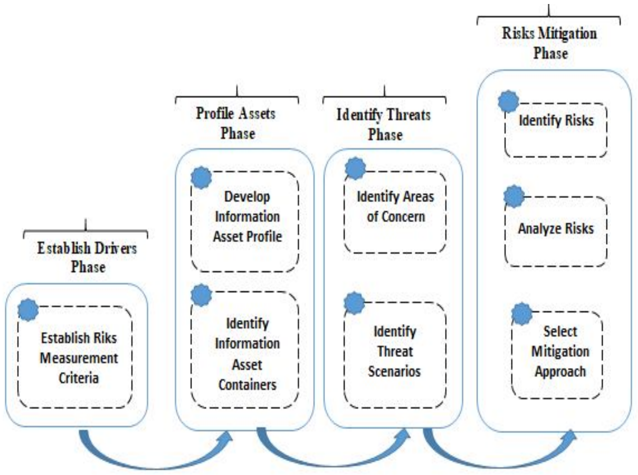
Establish Drivers Phase
Establish Riks Measurement Criteria
Profile Assets Phase
Develop Information Asset Profile
Identify Information Asset Containers
Identify Threats Phase
Identify Areas of Concern
Identify Threat Scenarios
Risks Mitigation Phase
Identify Risks
Analyze Risks
Select Mitigation Approach

Figure 3: OCTAVE methodology steps.

The OCTAVE methodology mainly focuses on information and its vulnerable locations; thus it allows assessing other critical assets in relation to the information identified before. However, the OCTAVE method is well suited to the risk assessment of the fire detection system since it allows both to have visibility on the assets and their security.

4. CASE STUDY RESULTS AND DISCUSSION

4.1 Case study results

In this section, we are applying OCTAVE methodology to Fire Detection System. Firstly, we began by collecting all security threats using the OCTAVE methodology. We are used and based on several standards, norms of security, several and similar works to this study cited in related work for applying this methodology in Fire detection system.

To simplify the presentation of the OCTAVE methodology re (risks identification and mitigation), the results is presented in form of three tables:

Table 1: shows the identification of information assets used in the risk assessment process, the possible security threats according to different assets containers, as the result of studying the entire fire detection system.

Table 2: gives an overview of the potential risks in an IoT-Fire detection System. The identified risks contain: the user authentication, fire detection system devices, user behavior, and data exchanged via the Internet. In Table 2, the possible impacts or potential risks are determined and connected to the assets and threats mentioned in Table 1.

Table 3: reports possible countermeasures with the goal of protecting information assets, and hence making a fire detection system more secure.

Table 1: Security threats found by performing an information risk assessment in terms of the possible threats associated with information assets.

Asset ID	Information Asset	Possible Security Threats
1	- Data collected by Sensors / data Forest Fire detection status information	- Data alteration - Denial-of-service (DoS) attacks - Device (Sensor) compromising - Information Disclosure - Function Interruption
2	- Information Resources (sensors, gateways, internet server…)	- Stealing private information - Make data inaccessible due to hardware failure
3	- User Credentials (Username and Password)	- User Impersonation Identity - Credential Theft
4	- Fire detection structure/inventory information	- The attacker can gain access to this information asset and search for specific device with known vulnerabilities to attack the system.
5	- Logs information	- The attacker can gain access to the logs data and obtain useful information.
6	- Information (data) transmitted through the system Gateway	- An attacker can steal information and data packet Transmitted via the system gateway.
7	- Location Tracking Information	- An attacker can observe the location data traffic
8	- Dashboard platform	- An attacker can get access to the platform and injected malicious code into apps
9	- Fire detection system setup information	- Information modification

(

Table 2: Security risks identified by performing the information risk assessment in terms of the possible impacts and the risk score.

Threat ID	**Possible Impacts (Risks)**
1	- Sensors will not detect risks like fire. - Manipulate the sensor measurements to infiltrate the system with wrong data, e.g. to cause certain actuations. - Financial loss - Reputation damages loss of information - The attacker can add a command and control interface to allow him to control the system remotely.
2	- User Privacy Violation - Financial loss - damage to reputation - loss of information
3	- Unauthorized access to the system. - Unauthorized Execution of Operations. - Loss of control over the system - Financial loss
4	- The attacker finds the weakest device with known vulnerabilities and attack it. - The attacker takes control over fire detection system. - Financial loss
5	- The attacker finds a way to access the main system and control it. - Financial loss
6	- The attacker can add virus to the data packet, then releases in the system, takes up system resources through constant self- replication, so that the system can't complete the relevant work, and it brings the system down making it unusable lastly. - Possibility of injecting new security vulnerabilities into the system
7	- Sensors will not detect risks like fire. - Manipulate the sensor measurements to infiltrate the system with wrong data, e.g. to cause certain actuations. - Financial loss - Reputation damages loss of information - The attacker can add a command and control interface to allow him to control the system remotely.
8	- An attacker can control database and information
9	- Difficulty in setting up the fire detection system correctly - Misuse of the system with the possibility of malfunction - Financial losses

Table 3: Possible Mitigation countermeasures to be applied in Fire Detection System

Threat ID	**Possible Mitigation Approaches**
1	- Limit network traffic to be accessed only by authorized users. - Use communication protection protocols - Hardware maintenance Backups - Use secure communication channel by using VPN based on IPsec or SSL/TLS. - Use dedicated high availability, redundant systems with uninterruptible power supplies (UPS). - Have multilayer security countermeasures. - Use Firewall and IDS (Intrusion Detection System) / IPS (Intrusion Prevention System)
2	- Restrict access to fire detection system resources. - Use communication protection protocols - Use encrypted communication channel. Secure all systems by applying multi security layers such as encryption, installing antivirus (antimalware) program on the system, intrusion prevention / detection systems. - Use Uninterruptable Power Supply (UPS)
3	- Block access to the systems through biometrics (Fingerprint Scanners). - Implement multi□factor authentication. Enforce a strong passphrase policy - Secure all systems by applying multi security layers such as encryption, installing antivirus (antimalware) program on the system, intrusion, prevention / detection systems. - Avoid writing complicated user ID and Passwords on paper and hide it near the workstation or the system. - User awareness program to make them aware about social engineering. - Avoid using compromised devices to get access to the system.
4	- Limit network traffic to be accessed only by authorized users. - Use communication protection protocols - Use encryption mechanisms Backups - Apply multilayer security countermeasures to secure all systems. - Use IDS (intrusion detection system) / IPS (intrusion prevention system) - Use secure communication channel by using VPN based on IPsec or SSL/TLS. - Awareness training program for the inhabitants to make them aware about security risks and social engineering.
5	- Limit network traffic to be accessed only by authorized users. - Use communication protection protocols. - Avoid logging information that would give useful information to an attacker. - Limit the access to the logs by applying access control mechanisms. - When sent to a remote system, logs should be protected by cryptographic mechanisms. - Apply multilayer security countermeasures to secure all systems.
6	- Secure the network layer through the network security services and access control, such as limiting the IP address, encrypting network layer and using firewalls. - Use communication protection protocols such as SSL/TLS over TCP/IP or DTLS over UDP. - For safe transmission of data use secure protocol such as SSL. - Perform router configuration management. - Implement gateway blacklisting to avoid connecting to known malicious domains and IP addresses.
7	- Limit network traffic to be accessed only by authorized users. - Use communication protection protocols - Locations information should be protected from unauthorized access Such information should not be sent in clear text, and thus a secure communication (encrypted) protocol is needed in this system for encrypting the traffic between the tracking system and the listener device. - Have multilayer security countermeasures.

8	- Using secure wireless communication technology to avoid accessing hackers to personal data.
9	- Use a robust authentication mechanism - Secure system configurations. - Make awareness and training programs regarding system security

4.2 Discussion

As we can see, The Octave methodology was applied to the Fire detection System and permitted as shown in the Tables to identify 9 critical information assets.

In Fire Detection System environment, an attacker cans cause several damages. For example: taking the Id 1 (data collected by sensors) in table 1: firstly, the possible security threats are: data alteration, denial-of-service (dos) attack, device (sensor) compromising, information disclosure and function interruption. Secondly, the possible risks are: sensors will not detect risks like fire, manipulate the sensor measurements to infiltrate the system with wrong data, financial loss, reputation damages loss of information, the attacker can add a command and control interface to allow him to control the system remotely.

However, the possible measures can be: limit network traffic to be accessed only by authorized users, use communication protection protocols, hardware maintenance backups, use secure communication channel by using vpn based on ipsec or ssl/tls, use dedicated high availability, redundant systems with uninterruptible power supplies (ups), have multilayer security countermeasures and use firewall and ids (intrusion detection system) / ips (intrusion prevention system).

The Octave method makes it possible to identify the most serious risks. Indeed, the main existing source at the Fire detection System is related to the sensors and transmission sources. Thus, the most critical risk is the information asset, since the information at the level of this studied system is sensitive to its functioning. Other risks are sensitive in relation to this system such as: communication between devices which must be ensured by the various security mechanisms.
The various approaches proposed should be taken into account in order to mitigate the various risks identified. If the system maintains a good level of security, facilitates its proper functioning and ensures its feasibility.

5. CONCLUSION AND PERSPECTIVES

This paper presents the risk assessment of Fire detection System. So, this system is vulnerable to different security attacks and threats. This paper gives an overview of risk assessment using the OCTAVE methodology, which presents an overview about security risks vulnerabilities, impacts and mitigation mechanisms. However this contribution can be useful used in the future to implement security policy and security requirements for Fire Detection System and others each system.

ACKNOWLEDGMENT

This work was supported by Mohamed First University. The authors would like to thank the president of Mohamed First University for financially supporting this work, as part of the PARA project.

REFERENCES

1. M. A. Khan, **Efficacy of OCTAVE Risk Assessment Methodology in Information Systems Organizations**, Int. J. Comput. Appl. Technol. Res., vol. 6, no. 6, pp. 242–244, 2017.
2. W. Benzekri, A. El Moussati, O. Moussaoui, and M. Berrajaa, **Early forest fire detection system using wireless sensor network and deep learning**, Int. J. Adv. Comput. Sci. Appl., vol. 11, no. 5, pp. 496–503, 2020.
3. D. Zorbas and B. O’Flynn, **Autonomous collision-free scheduling for lora-based industrial internet of things**, 20th IEEE Int. Symp. A World Wireless, Mob. Multimed. Networks, WoWMoM 2019, 2019.
4. W. Abbass, Z. Bakraouy, A. Baina, and M. Bellafkih, **Intelligent risk management framework**, IAES Int. J. Artif. Intell., vol. 8, no. 3, pp. 278–285, 2019.
5. P. Radanliev, D. De Roure, C. Maple, J. R. Nurse, R. Nicolescu, and U. Ani, **Cyber Risk in IoT Systems**, Univ. Oxford Comb. Work. Pap. Proj. reports Prep. PETRAS Natl. Cent. Excell. Cisco Res. Cent., vol. 169701, no. 2017, pp. 1–27, 2019.
6. S. Almuhammadi and M. Alsaleh, **INformation S Ecurity MAturity MOdel For Nist CYber SEcurity**, pp. 51–62, 2017.
7. P. Radanliev et al., **Cyber Risk impact Assessment - Assessing the Risk from the IoT to the Digital Economy**, Univ. Oxford Comb. Work. Pap. Proj. reports Prep. PETRAS Natl. Cent. Excell. Cisco Res. Cent., no. March, pp. 1–11, 2019.
8. M. Issam Khalil Abu-Baker, M. Khair Saleem Abu-Zaid, H. Alsawalqah, Y. Al-Shamayleh, and B. Al-Shboul, **The Impact of the Implementation of Capability Maturity Model Integration on User Satisfaction: Case Study on Software Companies in Jordan**, J. Softw., vol. 14, no. 7, pp. 293–311, 2019.
9. A. Feutrill, D. Ranathunga, Y. Yarom, and M. Roughan, “**The Effect of Common Vulnerability Scoring System Metrics on Vulnerability Exploit Delay**,” Proc. - 2018 6th Int. Symp. Comput. Networking, CANDAR 2018, pp. 1–10, 2018,
10. B. Ali, **Internet of Things based Smart Homes: Security Risk Assessment and Recommendations**, 2016.
11. P. Radanliev et al., **Integration of cyber security frameworks, models and approaches for building**

design principles for the internet-of-Things in industry 4.0, IET Conf. Publ., vol. 2018, no.CP740, pp. 1–6, 2018.

12. J. Wynn, **Threat Assessment and Remediation Analysis (TARA),**MITRE Corp., no. 14, pp. 14–2359, 2014, [Online].Available: http://www.dtic.mil/dtic/tr/fulltext/u2/1016629.pdf.
13. P. Radanliev et al., **Future developments in cyber risk assessment for the internet of things**, Comput. Ind., vol. 102, pp. 14–22, 2018.
14. B. Yan, X. Wang, and P. Shi, "**Risk assessment and control of agricultural supply chains under Internet of Things**," Agrekon, vol. 56, no. 1, pp. 1–12, 2017.
15. H. Abie and I. Balasingham, **Risk-Based Adaptive Security for Smart IoT in eHealth**, no. SeTTIT, pp. 269–275, 2013.
16. K. Mahmood, E. Shevtshenko, T. Karaulova, and T. Otto, "**Riskihindamise metoodika väikeste ja keskmise suurusega ettevõtete virtuaalettevõttele,**" Proc. Est. Acad. Sci., vol. 67, no. 1, pp. 17–27, 2018.
17. J. Samad, K. Reed, and S. W. Loke, A **risk aware development and deployment methodology for cloud enabled Internet-of-Things**, IEEE World Forum Internet Things, WF-IoT 2018 - Proc., vol. 2018-Janua, pp. 433–438, 2018.
18. V. Casola, A. De Benedictis, M. Rak, and U. Villano, **Toward the automation of threat modeling and risk assessment in IoT systems**, Internet of Things, vol. 7, p. 100056, 2019.
19. B. Ali and A. I. Awad, **Cyber and physical security vulnerability assessment for IoT-based smart homes**, Sensors (Switzerland), vol. 18, no. 3, pp. 1–17, 2018.
20. I. Cvitić, M. Vujić, and S. Husnjak, **Classification of security risks in the IoT environment**, Ann. DAAAM Proc. Int. DAAAM Symp., vol. 2015-Janua, no. 2016, pp. 731–740, 2015.
21. M. M. Ahemd, M. A. Shah, and A. Wahid, **IoT security: A layered approach for attacks & defenses**, Int. Conf. Commun. Technol. ComTech 2017, pp. 104–110, 2017.