International Journal of Engineering Applied Sciences and Technology, 2024
Vol. 9, Issue 03, ISSN No. 2455-2143, Pages 105-114
Published Online July 2024 in IJEAST (http://www.ijeast.com)

CYBERSECURITY ON IOT SYSTEMS BASED MULTI-LAYERED SECURITY RISK ASSESSMENT

Abdoul Aziz Issaka Hassane, Ali Hamadou
Department of Mathematics,
Dan Dicko Dankoulodo University of Maradi, Niger

Kadri Chaibou
Department of Mathematics and Computer Science,
Abdou Moumouni University, Niamey, Niger

Lanciné Camara
Social Science and Management University of Bamako,
Bamako, Mali

Abstract— **IoT systems contribute to digital transformation through the development of smart concepts. However, the IoT has also generated new security challenges that require security tools to be adapted, such as risk analysis methodologies.**

Many organizations use a variety of methods and frameworks to assess cybersecurity risks. However, most current risk assessment methods are for generic software systems, so there is no holistic approach to risk assessment for IoT technologies, especially due to the diversity of IoT systems

The purpose of our study is based on the following question: What IoT device factors should be considered in cybersecurity risk assessment methods?

In this study we first propose a cybersecurity risk assessment model based on vectors such as vulnerabilities and attacks, which evaluates the security risk from different dimensions of physical layer, network layer and application layer. Secondly, we design the mathematical assessment model for computing risk value of IoT system and then establish the mapping relationship table that the risk value is transformed into risk level.

Keywords— **Cybersecurity, iot, Risk assessment,**

I. INTRODUCTION

The term Internet-of-Things (IoT) refers to network connected cyber-physical devices that can communicate and share data in different constrained environments [1] In a broader definition, IoT devices are defined as any device with an IP address connected to a network [2]. It can transfer information via Wi-Fi, Bluetooth, or wired technologies. The IoT devices are present in almost each sector of life, from performing ordinary daily activities to industrial sensors and measurement devices.

Implementing the smart concept from a technological perspective is based on the use of emerging technologies such as artificial intelligence (AI), big data, machine learning (ML), Internet of Things

(IoT) and the cloud [3]. However, these technologies has introduced additional aspects related to cybersecurity. The IoT has certain particularities in relation to security in contrast with AI, big data, ML and cloud; this is because of factors such as location in less protected environments such as streets, traffic lights and agricultural fields, among others [4]

Security attacks have seen significant growth in recent years, generating considerable economic impacts for a variety of organizations. For example, in December 2021, Bitmart, a cryptocurrency trading platform, suffered a security breach, losing nearly USD 150 million in stolen tokens (BBC 2022). In a similar case, carried out in June 2021, gas pipelines in the United States suffered a ransomware attack, forcing the Colonial Pipeline to pay USD 5 million to retrieve its operations (New York Times 2022).

In august 2022 a hospital southeast of Paris has been crippled by an cyberattack, drastically reducing the number of patients who can be admitted and forcing a return to pre-digital workflows. (France24 2022)

IoT devices have inherent characteristics, such as heterogeneity of technologies and protocols, reduced computational capacity and limited security mechanisms [5].

In relation to this aspect, security risk analysis method in an IoT context has been discussed by some researchers in recent years.

However, each proposed method exploits different factors or characteristics of IoT systems compared to other methods, and sometimes there is no rational reason to choose the specific factors used. Analyzing the factors used by different methods can help provide a more in-depth calculation of IoT security risks. Therefore, there is a gap in formal methods for analyzing IoT security risks and factors that contribute to more accurate and effective development of IoT security risk analysis methods.

Based on the literature review and analysis, this study develops a scientific approach to calculate the cyber risk of IoT systems while taking into account IoT-specific influencing factors. These factors are used to calculate the risk impact of IoT devices.

Based on this, we propose the following objectives for this study:

1.Identify key factors that influence the security risk level of IoT systems.

2. Establish a method to calculate an approximate value of the security risk of an IoT system.

3. Determine a risk level (very high, high, medium, low, very low) relevant to the risk value

The rest of the paper is structured as follows. Section 2 presents a literature review of risk assessment in IoT ecosystems. Section 3 provides a works related to risk identification methods in IoT environments. We focus on the methodologies supporting our proposal. In Section 4 our design research methodology to identify the factors of IoT devices that contribute to risk security and experimental results are presented. Finally, Section 5 concludes this study.

II. LITERATURE REVIEW

2.1 RISK ASSESSMENT KEY CONCEPTS

Niesen et al. [6] define risks as harmful events, uncertain and inherent to any organizational activity. Some risks can be predicted and solved instantly. Other risks are unexpectedly unpredictable due to the low occurrence likelihood.

Risk identification is the process of cataloging vulnerabilities regarding causes and scenarios of occurrence, which means to find, recognize and describe the risks [7].

Assets encompass devices, equipment, and systems subject to vulnerabilities and often targeted by cyberattacks. These attacks can affect business models and operational aspects. Therefore, identification should provide resources capable of identifying the system's critical functions [8].

In risk assessment, identification is the first stage that supports the following steps of assessment, planning, and monitoring. In industry, risk identification contributes to managing cybersecurity of diverse assets [9].

2.2 CHALLENGE ON IDENTIFYING RISKS IN IOT SYSTEM

According to Radanliev et al. [10], there are several challenges on identifying risk emerging from connected devices and services, especially on IoT components.

One of the changes in the IoT is the change in the dynamic and size of the network [11]. Moreover, due to the connections between IoT devices, the security of one device is also dependent on the security of other devices to which it connects and as these devices increase, the risk added to the system increases [12].

Some specific challenges are: absence of hazard identification and disaster prevention; absence of economic impact assessments of cyber-IoT risks; and interaction between the volume of data generated by IoT devices and different activities (machine learning, ethics, business models).

It is estimated by experts that by 2030 IoT technology will affect the world economy by 11% of GDP, which will reduce energy consumption by up to 20% [13].

Smart devices are currently utilized in personal, industrial, medical devices, smart cars, smart homes, aircraft, finances, shopping behavior, inventory control, energy and water control. IoT is Currently, implemented in electrical power management such as energy-saving, power monitoring, digital metering. In the future, the number of Things acting in the system will grow exponentially [14].

The application of smart devices would create large savings for manufacturers, the savings are estimated to be $57.4 billion annually in the US and it is expected to increase the economic impact to at least $4 trillion per year by 2025[15].

Therefore, the data used in IoT systems becomes a problem for manufacturers and consumers. IoT cybersecurity risks are increasing at an alarming rate, requiring data to be protected from theft, manipulation and deception. In general, data availability, integrity, and confidentiality are becoming increasingly relevant to IoT. Security concerns are legitimate concerns for leveraging the economic value of digital and smart infrastructure [16]

III. RELATED WORKS

This subsection provides a brief overview of risk identification methods in IoT environments. We focus on the methodologies supporting our proposal

3.1 IOT LAYERS AND VULNERABILITIES / ATTACKS

According to different studies [17][18][19], there are different opinions on IoT security architecture.

Some studies identify three layers, others four or five, and still others consider six layers of security. This article analyzes the three-layer architecture, including the physical layer, network layer and application layer Figure1

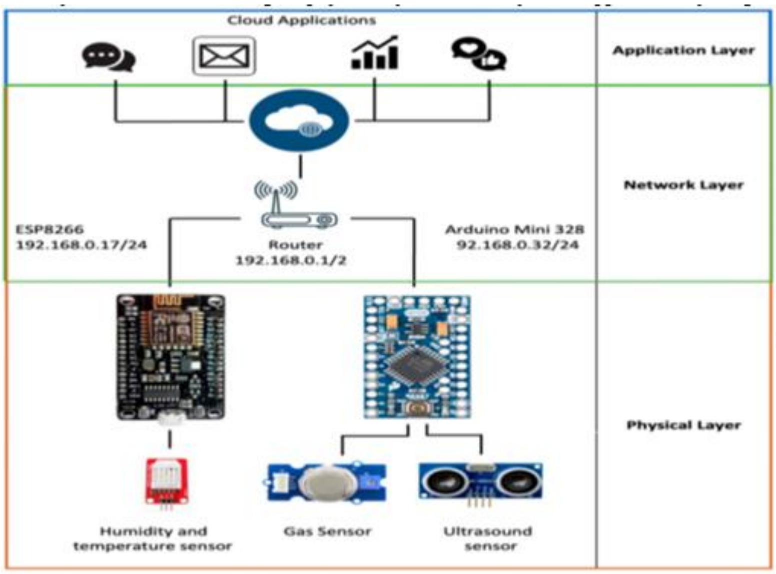

Fig. 1. Iot device architecture

Since each layer of the IoT architecture has unique security issues and interacts with other layers, security measures should be considered for the entire architecture [20].

A literature review of cybersecurity technologies through the lens of the IoT architecture helps us have a systematic and integrative view of the IoT cybersecurity. The following is based on Ali's three-layer architecture of IoT [21]

IoT attacks are classified based on IoT architecture and application scenarios [22]. All three IoT layers, namely application, network, and hardware layers, have security issues.

Physique layer

The IoT Physique layer consists of smart devices with sensors, actuators, and microcontrollers that have high processing power and the ability to connect to the network and connect to applications over the network. This device will allow us to collect data from areas with all these capabilities. Since all the data we need to process is collected at this level, we need to pay attention to data protection and make sure it is correct information from the sensors.

This layer contains different kinds of sensors that can be physically attacked at one spot for a long time, such as Bluetooth, GPRS, Wi-Fi, Zigbee and WSN [23].

The most frequent attacks are hardware attacks on the Physique layer. Different IoT devices, such as smart technology, video games, collect information about us and some hackers can exchange or access this information for illegal reasons. Tampering Node and Hardware Jamming are general attacks on the Physique layer, replacing or destroying the node in the first attacker to gain access to the node by collecting the cryptographic keys while the attacker can substitute a section of the hardware node in the latter and can gain routing table by catching the gateway node (24)[25] [26].

Other types of attack are injecting a noise in data and denial attack where the data containing incorrect or inaccurate information that happens during transmission or attacking a programmed file is used to fail the control of the node and decrease the battery life.

Network layer

Data from the Physique layer is transferred across the network layer. This layer receives data from multiple heterogeneous devices, which increase the thread for this layer.

An intrusion detection system (IDS) is used to detect attacks, take corrective measures, and monitor packets. The IDS deploys various intrusion detection techniques: statistical analysis for anomaly detection [27]; evolutionary algorithm for classifying intrusions based on error conditions, behavior, and attempted intrusions [28]; protocol verification for classifying suspicious behaviors; data mining techniques such as random forest method and deep learning for classifying network breach patterns [29].

- Man-in-Middle: In this threat, the attacker is not there to appear directly on a network device, they use the IoT authentication mechanism to communicate with the two sensor nodes to get all the sensitive data [30]
- Router Gateway: The connection between the sensors and the internet gateway is disconnected or fake information can be injected between node sensors and routers using DoS or routing table attacks.
- Sniffing: All information from the network and sensors can be obtained during communication between the nodes using a simple sniffer request (Arshad).

Application layer

The malicious attack could be caused by a virus in the application software code that causes the application to malfunction. If an attacker is aware of the application's flaws, the security risk of data latency increases at the application layer. The program is easily hackable and can be shut off due to vulnerability issues.

malicious code attacks and weakened software that allows a worm to be found and installed on internet-connected devices. Phishing is another type of attack where the attackers impersonate the user and use a reverse engineering model to identify a weak point in the end nodes. [31- 32]

Luckily in the past few decades, risk assessment is becoming an integral part of the software development; however, many of the vulnerabilities discovered in IoT are from this layer.

3.2 Cybersecurity risk assessment

Industries that are more exposed to technology security issues, like banking, healthcare, and the military, have more serious security-related issues.

Nowadays, security aspects represent one of the most significant barriers for the adoption of large-scale IoT deployments, based on the risk assessment theory, Xiong et al. [33] proposed a risk analytic method based on fuzzy analytic hierarchy process that consider five aspects of the security assessment items equipment layer, data layer, network layer, application layer and management layer.

In order to eliminate the fuzziness of qualitative assessment and the uncertainty caused by lack of information, multiperson multi-attribute network security risk assessment method based on Grey linguistic variables was established in [34]. To evaluate of security risk components, Landucci et al. [35]

expand and adapt the principles and concepts of physical security to the security risk analysis of chemical and process facilities. For accurately assessing the network security risk in real time, a new network security risk assessment method based on hidden Markov model was proposed in [36] and a network security risk assessment system based on chaotic particle swarm optimization (BP) neural network was designed in [37].

In order to measure the risk and avoid the influence of subjective factors, Yang et al. [38] proposed a measurement and assessment model of cloud computing risk to use Markov chain and information entropy for describing random risk environment and measuring risk.

Thibaud et al. [39] take into consideration that, to undertake a risk evaluation, vulnerability and IoT threat mappings are factors to be considered. Lee proposes two dimensions to evaluate the risk; the first one is related to the frequency of attacks of each IoT asset–vulnerability–threat, and the other dimension is the expected financial loss per attack.

Park et al. [40] propose a risk evaluation based on threat analysis as a cause of vulnerability and impact, for which they also define threats such as Threat Event Frequency (TEF) for IoT devices in relation to the device’s contact valorization and the action performed against it. In relation to the vulnerabilities (VUL) of IoT devices, VUL is measured as a combination of threat capability (TCap) and control strength (CS), and indicates the difficulty of successful attacks based on the common vulnerability scoring system (CVSS).

Lee In [41] mention that not only are security risks important, but privacy risks are as well, followed by the proposition of the use of the LINDDUN method. According to Shivraj, this method reduces the limitation of existing risk assessments based on STRIDE/DREAD to address privacy risks.

Kieras et al. [42] focused on the major details of IoT devices, and for the risk evaluation he defines four related components that are: security attributes, dependencies, security logical functions, and security risks. Their analysis is based on the graph’s concepts.

IV. CYBERSECURITY RISK ASSESSMENT BASED IOT LAYERS

Our cyber risk assessment based Iot layers consists of three major activities:

1. Identify the most relevant risk factors in IoT layers.
2. Establish a method to calculate an approximate value of the security risk of an IoT system.
3. Determine a risk level (very high, high, medium, low, very low) relevant to the risk value

4.1 Risk factors identification

The IoT risk identification involves understanding how intruders launch cyberattacks. Intruders have two different mindsets: explorative and exploitative.

Intruders usually use intentional, intuitive thinking and extensive experimentation during the exploratory stages. Once they have gained access to a system, they will turn to an exploitative mindset in order to succeed. The risk identification stage identifies IoT vulnerabilities and cyber threats, threat types and vulnerabilities are then identified for each IoT asset.

The goal of this paper is to provide a wider range of security flaws and exploits that affect Internet of Things platforms. Because it categorizes the various attacks into three distinct classes physical, network, and application vulnerabilities—our classification differs from previous classifications. An Internet of Things system is susceptible to physical attacks, network attacks, and application attacks from the system. It should be noted that environmental attacks such as earthquakes are not included in this work since our research focuses on planned attacks from an enemy.

A summary of the classification of the attacks is shown in **Table 1** below.

Table -1 attacks to layers of Iot systems

LAYERS	VILNERABILITY / ATTACKS
Application	
	Virus
	Spyware
	Phishing Attacks
	Trojan
	Malicious Scripts
	Denial of Service
	Social Engineering
	Malware
	Injection
Network	
	Main-in-the-middle
	RFID Spoofing
	RFID Cloning
	RFID unauthorised access
	Denial of Service
	Sinkhole attack
	Sybil attack
	Flooding
physical	
	Node Tampering
	Node Jamming
	Node Injection
	Code injection on the node
	RF Interference
	Sleep Deprivation Attack
	Eavestdropping
	Physical Damage

Based on the challenge classification presented in this Section, we will outline future directions for risk assessment

An IoT system consists of three different layers each with vulnerabilities and security attacks. To address these attacks and to successfully protect the IoT system, this section presents a multi-layered security risk assessment approach.

The attribute of vulnerability is the vulnerability degree of each IoT device layer when the IoT system is attacked.

As the first step towards risk treatment, risk assessment is the most important part of the risk management process. Among the elements taken into account in the risk assessment process are the attack's likelihood and impact of the attack.

Our risk assessment process is divided into the following steps in Fig.2

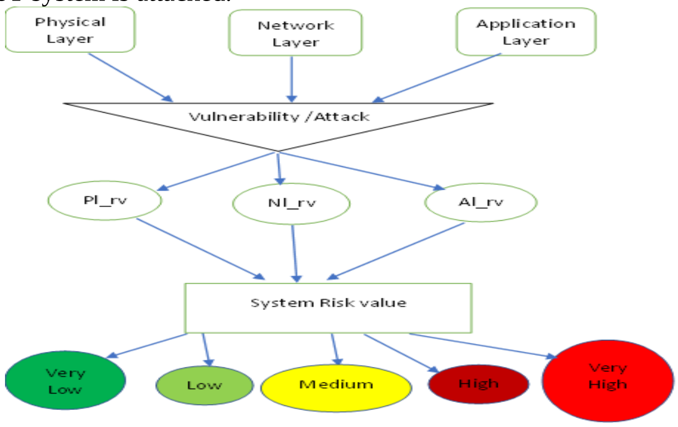

Fig. 2. Risk evaluation process on Iot systems

_ Step 1. Analyze and classify the data of physical layer, network layer, application layer of the physical network system,
_ Step 2. Investigate and identify vulnerabilities / attacks
_ Step 3. Calculation of layer risk value
_ step 4. Calculation of system risk value
_ Step 5. Risk level estimation, as follows:
1 indicates that it is not important and there is almost no loss of the system after damage; 2 indicates that it is not very important and the system loss is very low after being damaged; 3 indicates that it is generally important, and the system will cause medium loss after being damaged; 4 indicates that it is more important, and the system will cause more serious losses after being damaged; 5 indicates that it is particularly important, and the damaged system causes particularly serious losses.

Two factors related from a security perspective are:

a. Vulnerability: The weakness in each layer of an IoT architecture, which is the possibility of suffering attacks;
b. Attack: IoT systems are made up of a set of protocols, technologies, and devices, so depending on this set, it is possible that one device is more susceptible to an attack than another.

4.2 RISK VALUE CALCULATION

Our investigation approach is based on the following research question: What is the mathematical model required to determine a quantitative value of the security risk of an Iot sytem based on layers frames?
The vulnerability identification is used to evaluate the risk value on each layer. Therefore, in order to assess the risk value of the Internet of things, we need to first identify vulnerabilities and attacks on the three layers of IoT devices.
Sample IoT risk weigh is furnished in Table 2.

Table -2 attacks risk weight

LAYERS	VILNERABILITY / ATTACKS	Risk weigh
Application		
	Virus	5
	Spyware	3
	Trojan	3
	Denial of Service	5
	Social Engineering	3
	Malware	4
	Injection	3
Network		
	Main-in-the-middle	5
	RFID Spoofing	2
	RFID Cloning	3
	RFID unauthorised access	4
	Denial of Service	4
	Sinkhole attack	4
	Sybil attack	2
Physical		
	Node Tampering	2
	Node Jamming	1
	Node Injection	3
	Code injection on the node	3
	RF Interference	2
	Sleep Deprivation Attack	1
	Eavestdropping	3

To assess the degree of impact on IoT attacks relative to the likelihood of a systematic risk event, we determine a risk scale.

According to the principle of risk calculation, the formula of risk value is done based on quantitative weightage.
the formula of risk value of device d is as follows:

Risk value of device d is Rvd = (Rwp + Rwn + Rwa) /3 (1)

where Rwp represents the risk weight on physical layer, Rwn represents the risk weight on network layer and Rwa represents the risk weight on application layer

Rwp = $\sum_{i=1}^{n} RWi/N$ (2)

Rwn = $\sum_{i=1}^{n} RWi/N$ (3)

Rwa = $\sum_{i=1}^{n} RWi/N$ (4)

the formula of risk value of the dimension i is as follows:

RVi = $\sum_{i=1}^{n} Ri/N$ (5)

4.3 Risks level evaluation

According to mapping relationship of risk value and risk level in Table 3, the risk level can be got to analyze the current risk profile of IoT system.

Table -3 Risks level evaluation

Risk level		Risk value range
Very high	5	R ≥ 4,5
high	4	3,5 ≤ R < 4,5
medium	3	2,5 ≤ R < 3,5
Low	2	1,5 ≤ R < 2,5
Very low	1	R < 1,5

By calculating the data of Internet of things system, we can get risk value as shown in table 4 below. The risk weight of each dimension can be calculated according to Formula 1 and the corresponding risk level can be got by Table 3.

Table -4 : corresponding risk weight of each device according to risk factors

	Vulnerability/ Attacks			Risk weight
Devices	Physique	Network	Application	
Device 1	Node injection	Main-in-the-middle	Virus	4,333
Device 2	Node Jamming	RFID Spoofing	Spyware	2
Device 3	Node tampering	RFID Cloning	Trojan	2,666
Device 4	Code injection on the node	RFID unauthorised access	Denial of Service	4
Device 5	RF Interference	Denial of Service	Social Engineering	3
Device 6	Sleep Deprivation Attack	Sinkhole attack	Malware	3
Device 7	Eavestdropping	Sybil attack	Injection	2,666

According to the vulnerability and threats analysis of three key elements: physic, network and application layers, the possibility of security incidents and the degree of loss after damage are determined.

The risk weight is divided as follows: 1 means that there is almost no harm to the device. 2 indicates that the damage caused is very small. 3 indicates that the damage caused is general. 4 indicates that the damage is greater. 5 indicates that the damage caused is particularly serious.

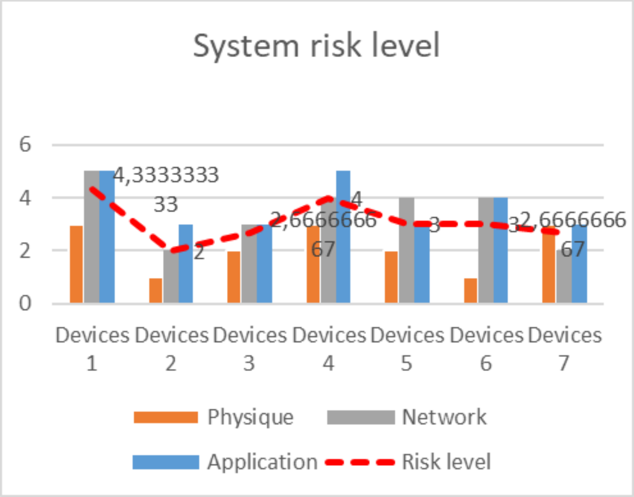

Fig. 3. Iot systems Risk evaluation

V. CONCLUSION

In this study, we propose a multi-dimensional security risk assessment model based on three layers for the IoT system. Assets that create vulnerability are described by classifying the types of attacks that threaten the physical layer, network layer, and application layer of IoT. The contribution of this study is to explain the layers of cyber-physical systems that make up the IoT which were evaluated separately and their vulnerabilities and threats were examined. The proposed IoT security risk assessment model is a holistic security model that evaluates each layer of cyber-physical systems separately against vulnerabilities and threats, based on the risk value calculation and determine the risk-level of the system. Therefore, the research on the level protection mechanism of the IoT system as a future research direction is of great theoretical significance.

VI. REFERENCE

[1] Samin Rahman, Humahun Kabir, (2018) "A Survey Analysis and Model Development for Internet of Things (IoT) System for City Buildings: Dhaka City, Bangladesh Perspective," TENCON 2018 - IEEE Region 10 Conference, Jeju, Korea (South), 2018, pp. 1229-1234.

[2] X. Lu, Q. Li, Z. Qu and P. Hui, (2014), "Privacy Information Security Classification Study in Internet of Things," International Conference on Identification, Information and Know Physique in the Internet of Things, Beijing, 2014, pp. 162-165.

[3] Andrade, R.O.; Yoo, S.G. A Comprehensive Study of the Use of LoRa in the Development of Smart Cities. Appl. Sci. 2019, 9, 4753.

[4] Lopez-Vargas, A.; Fuentes, M.; Vivar, M. (2020) Challenges and Opportunities of the Internet of Things for Global Development to Achieve the United Nations Sustainable Development Goals. IEEE Access 2020, 8, 37202–37213.

[5] Andrade, R.O.; Yoo, S.G.; Tello-Oquendo, L.; Ortiz-Garces, I. A Comprehensive Study of the IoT Cybersecurity in Smart Cities. IEEE Access 2020, 8, 228922–228941.

[6] T. Niesen, C. Houy, P. Fettke, and P. Loos, "Towards an integrative big data analysis framework for data-driven risk management in industry 4.0," Proceedings of the Annual Hawaii International Conference on System Sciences, vol. 2016-March, pp. 5065–5074, 2016.

[7] ISO Central Secretary, "Risk management — Guidelines," International Organization for Standardization, Geneva, CH, Standard, 2018.

[8] M. Lezzi, M. Lazoi, and A. Corallo, (2018) "Cybersecurity for Industry 4.0 in the current literature: A reference framework," Computers in Industry, vol. 103, pp97–110, https://doi.org/10.1016/j.compind.2018.09.004

[9] M. P. Barrett et al., "Framework for improving critical infrastructure cybersecurity," National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep, 2018.

[10] P. Radanliev, D. De Roure, J. R. Nurse, R. Nicolescu, M. Huth, S. Cannady, and R. M. Montalvo, (2018) "Integration of cyber security frameworks, models and approaches for building design principles for the internet of Things in industry 4.0," IET Conference Publications, vol. 2018, no. CP740, pp. 1–6,

[11] J. R. C. Nurse, P. Radanliev, S. Creese and D. De Roure, "If you can't understand it, you can't properly assess it! The reality of assessing security risks in Internet of Things systems," Living in the Internet of Things: Cybersecurity of the IoT - 2018, London, 2018, pp. 1-9.

[12] J. Chen and Q. Zhu, (2019) "Interdependent Strategic Security Risk Management With Bounded Rationality in the Internet of Things," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 11, pp. 2958-2971.

[13] V. G. Semin, E. R. Khakimullin, A. S. Kabanov and A. B. Los, "Problems of information security technology the “Internet of Things”," 2017 International Conference "Quality Management,Transport and Information Security, Information Technologies" (IT&QM&IS), St. Petersburg, 2017, pp. 110-113.

[14] B. F. Zahra and B. Abdelhamid, "Risk analysis in Internet of Things using EBIOS," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, 2017, pp. 1-7.

[15]] J. R. C. Nurse, P. Radanliev, S. Creese and D. De Roure, "If you can't understand it, you can't properly assess it! The reality of assessing security risks in Internet of Things systems," Living in the Internet of Things: Cybersecurity of the IoT - 2018, London, 2018, pp. 1-9.

[16] P. Radanliev, D. De Roure, S. Cannady, R. M. Montalvo, R. Nicolescu and M. Huth, "Economic impact of IoT cyber risk - Analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance," Living in the Internet of Things: Cybersecurity of the IoT - 2018, London, 2018, pp. 1-9.

[17] J. DAZINE, A. MAIZATE and L. HASSOUNI, "Internet of things security," 2018 IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD), Marrakech, Morocco, 2018, pp. 137-141.

[18] T. Ara, P. G. Shah, M. Prabhakar, "Internet of Things Architecture and Applications: A Survey", Indian Journal of Science and Technology, vol. 9, no. 45, 2016.

[19] S. Li, T. Tryfonas, H. Li, "The internet of things- a security point of view", Internet Research, 2016.

[20] Bendavid, Y.; Bagheri, N.; Safkhani, M.; Rostampour, S. IoT Device Security: Challenging “A Lightweight RFID Mutual Authentication Protocol Based on Physical Unclonable Function”. Sensors 2018, 18, 4444.

[21] Kurdistan Ali & Shavan Askar (2021). Security Issues and Vulnerabilities of IoT Devices. International Journal of Science and Business, 5(3), 101-115. doi: https://doi.org/ 10.5281/zenodo.4497707

[22] K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray, Y. Jin, Internet-of-Things security and vulnerabilities: taxonomy, challenges, and practice. Journal of Hardware and Systems Security 2, 97–110 (2018)

[23] (Arshad et al., 2020). Arshad, M. J. Evaluating Security Threats for each Layers of IoT System.

[24] Rao, T. A., & Haq, E. J. I. J. o. C. A. (2018). Security challenges facing IoT layers and its protective measures. 975, 8887.

[25] Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Service differentiation for video applications over OBS networks. 16th European Conference on Networks and Optical Communications, Newcastle-Upon-Tyne, pp. 200-203.

[26] Al Majeed, S., Askar, S., Fleury, M. (2014). H.265 Codec over 4G Networks for Telemedicine System Application. UKSim-AMSS 16th International Conference on Computer Modelling and Simulation (UK), Cambridge (pp. 292-297), doi: 10.1109/UKSim.2014.59.

[27] Pacheco, J.; Benitez, V.; Félix, L. Anomaly Behavior Analysis for IoT Network Nodes. In Proceedings of the 3rd International Conference on Future Networks and Distributed Systems, Paris, France, 1–2 July 2019; pp. 1–6.

[28] Li, J.; Zhao, Z.; Li, R.; Zhang, H. AI-based two-stage intrusion detection for software defined IoT networks. IEEE Internet Things J. 2019, 6, 2093–2102.

[29] Roopak, M.; Tian, G.Y.; Chambers, J. Deep Learning Models for Cyber Security in IoT Networks. In Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019; pp. 452–457.

[30] Rao, T. A., & Haq, E. J. I. J. o. C. A. (2018). Security challenges facing IoT layers and its protective measures. 975, 8887.

[31] Puthal, D.; Nepal, S.; Ranjan, R.; Chen, J. Threats to networking cloud and edge datacenters in the Internet of Things. IEEE Cloud Comput. 2016, 3, 64–71.

[32] Dharmendra Kumar and all “Cyber Risk Assessment Model for Critical Information Infrastructure” 2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC) GLA University, Mathura, UP, India. Feb 28-29, 2020

[33] Z. Xiong,G. Hao,H.E. XiaoYun, et al. Research on Security Risk Assessment Method of State Grid Physique Computing Information System[J]. Computer Science, 2019.

[34] Jialin Chen, Zheng Zhou, Yi Tang, Yi He, Shiwen Zhao, Research on Network Security Risk Assessment Model Based on Grey Language Variables. Available[C] Conf. Series: Materials Science and Engineering677 (2019) 042074.

[35] G. Landucci,N. Khakzad, G. Reniers. Principles and concepts for security risk assessment[J]. Physical Security in the Process Industry, 2020,31-70.

[36] W. Zengguang,L.U. Yu,Z. Donghao. Network Security Risk Assessment Method Based on Hidden Markov

Model[J]. Journal of Air Force Engineering University(Natural Science Edition), 2019.20(3):71-76

[37] D. Xiu-Juan. Design of Network Security Risk Assessment System Based on Chaotic Particle Swarm Optimization BP Neural Network[J]. Science Technology & Engineering, 2019.19(16):251-255.

[38] Yang M , Jiang R , Gao T , et al. Research on Cloud Computing Security Risk Assessment Based on Information Entropy and Markov Chain[J]. International Journal of Network Security, 2018, 20(4):664-673.

[39] Thibaud, Montbel, Huihui Chi, Wei Zhou, and Selwyn Piramuthu. 2018. Internet of Things (IoT) in high-risk Environment, Health and Safety (EHS) industries: A comprehensive review. Decision Support Systems 108: 79–95.

[40] Park, Mookyu, Haengrok Oh, and Kyungho Lee. 2019. Security Risk Measurement for Information Leakage in IoT-Based Smart Homes from a Situational Awareness Perspective. Sensors 19: 2148.

[41] Lee, In. 2020. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet 12: 157. doi.org/10.3390/fi12090157

[42] Kieras, Timothy, Junaid Farooq, and Quanyan Zhu. 2021. I-SCRAM: A Framework for IoT Supply Chain Risk Analysis and Mitigation Decisions. IEEE Access 9: 29827–40.