

# Towards a framework for Assessing cybersecurity risks in Internet of Things (IoT) devices

<sup>1</sup>Zhilei Qiao<sup>1</sup> Julio C. Rivera<sup>2</sup> Mi Zhou<sup>3</sup>

<sup>1,2</sup>*Department of Management, Information Systems, and Quantitative Methods, Collat School of Business, University of Alabama at Birmingham*

<sup>3</sup>*Department of Accounting, School of Business, Virginia Commonwealth University*

<sup>1</sup>*qiaozl@uab.edu*, <sup>2</sup>*jrivera@uab.edu*, <sup>3</sup>*mizhou@vcu.edu*

## ***Abstract***<sup>2</sup>

*The term Internet of Things (IoT) refers to a broad class of devices used by business entities as well as consumers to provide or consume a broad array of services. All these devices share their need to connect to the internet to deliver their native functionality. This connection requirement exposes the devices to the cybersecurity threats found on the internet. Existing literature on IoT cybersecurity solution models has shown that different technologies, such as communication technologies, mobile-app based authorization framework, graph-theoretic approach or blockchain technologies, have been majorly proposed to solve IoT security issues. However, these studies only focus on some specific IoT security issues like data theft or security issues on some specific layer across the whole IoT architecture. Therefore, there is a lack of systematic framework to solve IoT cybersecurity issues. This paper presents a framework for assessing such risks. In the qualitative analysis results, the device threats seem more severe than data confidentiality and privacy issues. This surprising finding highlights the significances of security taxonomy because both issues are based on different technical requirements. Our study has important managerial and practical implications for users, managers, and policymakers.*

**Keywords:** *Internet of Things, risk, adoption, cybersecurity*

## **1. Introduction**

The Internet of Things (IoT) is a term covering a broad array of devices “that connect, communicate or transmit information with or between each other through the Internet.” (Commission, 2015; Feng, Yao, & Sadeh,

---

<sup>1</sup> Zhilei Qiao is the contact author.

<sup>2</sup> We are grateful to Dr. Tawei (David) Wang, USA, DePaul University, for his support as peer editor of this article.

2021). Such flexibility in its ability to share information is one of the primary drivers of IoT adopted by both business entities and consumers. Unfortunately, this connection to the Internet also exposes these devices to connections from other, unexpected and unauthorized, devices on the Internet (Chanal & Kakkasageri, 2020). In 2017, security experts have identified the potential threats targeting home devices through internet-facing webcams and other devices into massive botnets (Brenner, 2017). Furthermore, IoT devices may depend on a remote service infrastructure to deliver their functionality, potentially exposing users to threats compromising their privacy and data confidentiality. For example, a CNN Business reports the privacy and data confidentiality issues of Amazon's Alex in 2019: a "Not only is Alexa listening when you speak to an Echo smart speaker, an Amazon employee is potentially listening, too." (Valinsky, 2019) In the current cybersecurity environment, the adoption of IoT devices brings exposure to an array of cybersecurity threats.

Therefore, IoT cybersecurity market has increased steadily. MarketsandMarkets Company, as the largest revenue impact company in the world, predicts that the market size is expected to grow from USD 12.5 billion in 2020 to USD 36.6 billion by 2025, at a Compound Annual Growth Rate (CAGR) of 23.9% during the forecast period<sup>3</sup>.

However, the development of IoT is still at its infancy stage and all of the related issues need to be solved (Qi et al., 2019). Since IoT security is the foundation for the development of IoT, IoT cybersecurity has been a challenging task. The two core considerations of IoT security are access control and data confidentiality (Bertino, 2016). IoT devices are inherently tiny and specific functions-oriented with limited protection embedded in the devices because strong protection systems are costly and cannot be installed in a small device. In addition, a Gartner analyst reports that IoT connects 20 billion devices by 2020 (Markose, Sharief, Ramprasath, & Krishnaraj, 2021). These devices are heterogeneous and imply potential security challenges. IoT communication technologies also collect a massive amount of data and information from users. Once these data or information are disclosed, they will have a significant impact on users' lives and work because they can be used for understanding and predicting their behaviors.

---

<sup>3</sup> <https://www.marketsandmarkets.com/PressReleases/iot-security.asp>

Malicious data (e.g., personal identity information, financial data, and medical information) should be dealt with in the IoT network.

Hence, as IoT is revolutionizing the global communication network comprising of people, devices, intelligent objects, data, and information, it is critical to design a systematic framework or model to manage IoT cybersecurity issues (Liang & Ji, 2021). Existing literature on IoT cybersecurity solution models has shown that different technologies, such as communication technologies, mobile-app based authorization framework, graph-theoretic approach or block-chain technologies (Al-Sibai, Alrubaie, & Elmedany, 2021; Burhan, Rehman, Khan, & Kim, 2018; Latif, Idrees, Ahmad, Zheng, & Zou, 2021; Šikanjić, Avramović, & Marinković, 2021), have been majorly proposed to solve IoT security issues. However, these studies only focus on some specific IoT security issues like data theft or security issues on some specific layer across the whole IoT architecture. Therefore, there is a lack of systematic framework to solve IoT cybersecurity issues.

This paper seeks to conduct qualitative analytics and develop a systematic framework that can analyze the nature of cybersecurity threats and the resulting risks faced by entities adopting IoT devices. The paper attempts to identify the categories of functional capabilities that IoT devices may deliver, and the cybersecurity threats these capabilities may bring with them. Understanding the nature of these capabilities can lead to identifying the cybersecurity risks to a given IoT device. In the next section, we first formulate a definition for IoT and then discuss the nature of risks inherent in such devices. We then develop a risk assessment framework for IoT devices and present a summary of this framework and its structure.

## **2. Literature Review**



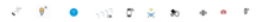
### **2.1. Defining Internet of Things and its Structure**

The term “Internet of Things” was first introduced in the late 1990s (Hadzovic, 2021), and although there is no one definition for the term; the Federal Trade Commission (FTC) report on Privacy & Security in a

Connected World has defined it as “*devices or sensors – other than computers, smartphones, or tablets – that connect, communicate or transmit information with or between each other through the Internet* (p. 6)”(Commission, 2015). This definition covers a wide range of devices and supporting technologies used in commercial and consumer environments. IoT devices have a combination of features, including electronic components, software, sensors, and network connectivity, which may exchange data with servers, centralized systems, or other connected devices (Bertino, 2016).

A useful way of understanding IoT devices is via its architectural model describing device capabilities. To date, scholars have identified a three-layer model (Table 1) that provides a useful abstraction in analyzing IoT device capabilities and features (Burhan et al., 2018; Nord, Koohang, & Paliszkiwicz, 2019). Specifically, Nord et al. (2019) postulate an architectural model consisting of a sensing layer, a network layer, and an application layer. In this model, the sensing layer consists of an IoT device’s environmental sensing and data collection capabilities; the network layer addresses an IoT device’s network communication capabilities; and the application layer covers an IoT device’s software delivered functionality, either on the device or through supporting software services.

**Table 1. Three Layers of IoT Architecture**

Layers	Description	Applications	Security	
			Data Risks	Device Threat
<b>Application</b>	IoT device’s software functions		E.g., Audio Input, E-ticket	E.g., Audio Play function, Flight Apps
<b>Networking</b>	Networking and data transmission		E.g., MAC address, WIFI guest account information	E.g., Bluetooth connection; WIFI connection; Hotspot
<b>Sensing</b>	Sensing objects and data, data collection and extraction		E.g., Image, Video, Audio,	E.g. Web camera, apple watch

Regarding sensing capabilities, IoT devices employ a wide range of sensors collecting such things as video, audio, positional, device status, and other environmental data (Burhan et al., 2018). From a network communication perspective, IoT devices use a broad array of technologies ranging from wired communication to wireless communication using anything from Wi-Fi to Bluetooth to cellular

communication, and other wireless technologies (Burhan et al., 2018). Finally, at the application layer, the software processes and interprets sensor data, as well as commands the use of IoT device capabilities (Gubbi, Buyya, Marusic, & Palaniswami, 2013). With software-driven command of device capabilities, this may include device capabilities from as simple as turning on a switch, to a complex set of commands directing all aspects of the device (Adat & Gupta, 2018). Many devices offer combinations of these capabilities, resulting in a rich and complex mix of device capabilities.

In addition to an IoT device's native hardware capabilities, there is the added dimension of how the device uses its capabilities and what it communicates to the outside world. Given that IoT devices connect to the Internet, they send and receive data as part of their operation. Many IoT devices rely on the data they send and receive to augment their native capabilities. Typically they use services provided by the device vendors or other third-party service providers, who in turn, use the data to deliver additional functionalities or services (Cvitić & Vujić, 2015). How to handle this data and who is the recipient and owner of such data adds to the complex nature of IoT devices and their adoption. Thus, IoT represents a complex technical architecture with implications for how information is received, transmitted, and processed. Such a device carries with it the potential to compromise the confidentiality, integrity, and availability of an organization or home user's security and privacy.

## **2.2. Internet of Things Risk Assessment**

IoT devices operate in environments that combine sensing, communications, and processing capabilities. Each of those areas exposes users to risk (Ashibani & Mahmoud, 2017). Those risks range from the theft of data to the takeover and malicious control and actuation of IoT devices (Fagan, Megas, Scarfone, & Smith, 2019). Even though this broad range of risks exists, it is useful to think of risks as falling into two broad categories: risks to data security and risks to the control of the IoT device itself (Fagan et al., 2019)

Data security risks range from the theft of data from an IoT device or its sensors to the theft of data collected by a third-party service augmenting

IoT device functionality. In addition to the direct threat to data security, there is also the indirect threat of inferring valuable information from any data collected. Direct threats to data security are relatively easy to understand since the data will be of value to the party acquiring it. For example, gaining access to Personally Identifiable Information (PII) is recognized as something valuable to those engaging in identity theft (Commission, 2015).

Indirect threats to data security, however, are a more subtle but no less threatening breach of data security. These threats arise from the collection of enough data to infer information that may be of value to a malicious third-party. For example, collecting data on something as innocuous as turning lights on or off may lead to the creation of a profile showing a dwelling's occupancy patterns. In such a case, the individual data points themselves are not of value, but when aggregated, they can be used to infer behavior patterns (Hou, Qu, & Shi, 2019). Thus the risk assessment process should not neglect this aspect.

Risks to the control of IoT devices are no less threatening than data security risks. IoT devices are a combination of computing hardware, sensing capabilities, and controlling software. Each of those areas poses an attack vector for a malicious third-party seeking to control the device. Generally, vulnerabilities in these areas are the results of flaws in the device's operating software or the firmware embedded in the device hardware. The exploitation of these attack avenues can allow malicious third-party to control an IoT device and, depending on the device's capabilities, to engage in a wide variety of malicious behaviors. Apart from using a device to surveil or generate attacks on other Internet attached devices, there is the real possibility of actuating an IoT device's embedded capabilities to manipulate it or attached devices (Arora, Kaur, Bhushan, & Saini, 2019; Commission, 2015).

### **3. A Proposed Risk Assessment Framework for Internet Of Things Devices**

The purpose of proposing a risk assessment framework is to give IoT technology adopters a frame of reference when gauging their cybersecurity risk exposure. For security professionals, this is the first step in deciding how to mitigate risk, and ultimately deciding what level of risk to accept. As such, a framework should be a guide on what items should be assessed, and allow the technology adopting entity to make decisions on how to handle their risk exposure. The nature of IoT devices with their wide range of capabilities and applications requires that we develop a framework with a sufficient level of abstraction applicable to all IoT devices.

As mentioned in the previous discussion, a useful abstraction when examining IoT device capabilities is the three-layer architectural model postulated by (Nord et al., 2019). This model identifies three categories of IoT device capabilities: 1) a sensing layer, 2) a network layer, and 3) an application layer. The previous discussion also identifies two areas of risk inherent in all IoT devices; risks to data security, and risks to control of IoT devices (Commission, 2015). Therefore, it is useful to examine each architectural layer from the perspective of both risks to data security and risks to IoT device control.

In the following tables, we capture the types of risks associated with the sensing, network, and application layers in IoT devices in two categories – data risks and device threats. Within the data risks, we have direct and indirect risks to both privacy and confidentiality. Direct data risks are those that occur from loss of privacy or confidentiality from the compromise of specific data elements; for example, data considered to be PII. Indirect data risks would be those resulting from the collection of data that infers compromising information about the targeted entity, such as collecting data about behaviors or events that can lead to inferring a pattern of behavior.

In the realm of device threats, we have the risk of loss of device control, as well as the risk of device function blocking. Loss of device control

can lead to data theft, where data collected by the device or its services may be collected for use by a malicious third-party. Related to this risk is the compromise of device control, allowing a third-party to surveil an entity through the use of device sensors and capabilities. A third-party gaining device control might also use the device's capabilities to actuate a device's sensing or manipulation capabilities, including device capabilities that might command other devices. Repurposing a device might lead to using that device for purposes other than those for which it was intended, such as generating attacks on other devices or computing platforms. Finally, the risk of device function blocking exists when a device is prevented from fulfilling its intended function(s) via malicious attacks, such as might result from a denial of service attack.

The risks enumerated above illustrate broad categories of risks and ensure that the risk assessment process evaluates risk exposure in each category. IoT devices are subject to multiple cybersecurity risks, and in fact, there is overlap in the risk categories identified. However, when these risks are evaluated using the sensing, network, and application architectural layers, the nature of the risks at each layer may take on a different character.

In Table 2, we see how the risk categories are applied at the sensing layer. This layer comprises the sensing capabilities that an IoT device may have, illustrating the types of data that such a device may collect. Some of these capabilities are bidirectional, such as devices that combine both input and output capabilities, as might be seen in two-way video devices or voice-controlled personal assistants. Beyond that, there is a wide range of devices that are capable of sensing such things as temperature and other environmental data or delivering data on a device's current status. Furthermore, some of these also allow for the manipulation of the device's state or of other devices that it controls. A simple example of such a device might be an Amazon Echo Dot, a popular consumer device that serves as an intelligent digital assistant, is used as an example for illustrative purposes. This device allows a user to communicate via voice and has an internal speaker that provides audio responses. The device connects to a network through its Wi-Fi



connection (as well as through Bluetooth, if enabled). Functionality for the device is managed via its onboard software and its communication with a third-party service provider (i.e., Amazon). The Echo device software also has an extensible framework for adding additional features, as well as allowing it to interface and possibly control other devices. Control of other devices depends on a software interface providing access to the other device's third party services.

**Table 2. Sensing Layer (Amazon Echo Dot Example)**

	Data				Risk				Function Blocking
	Privacy		Confidentiality		Device Loss of Control				
	Direct	Indirect	Direct	Indirect	Data Theft	Surveillance	Malicious Actuation	Repurposing	
<b>Sensor Capabilities</b>									
<b>Video (Still or Motion)</b>									
Input									
Output									
<b>Audio</b>									
Input	X	X	X	X	X	X	X	X	X
Output	X						X	X	X
<b>Environmental State</b>									
Position									
Temperature									
Other	X	X	X	X	X	X			
<b>Device Status</b>									
Device Sensing Parameters					X	X			

At the sensing layer, we can identify risks to data due to the Echo's combination of input and output audio capabilities. In this regard, those capabilities can be used to collect data directly or generate audio output, as well as indirectly to sense patterns of behavior related to audio input. Data on the device's state or the state of other devices it controls may be obtained from the Echo device. Both situations can lead to data theft or use of the device for surveillance. Finally, there is the possibility of a denial of service attack on such a device, both by flooding its network interface, as well as preventing the device from responding to voice commands by generating enough audio interference to prevent it from detecting voice commands.

Table 3 applies the risk categories to an IoT device’s network layer. Regardless of the nature of an IoT device, in order to function, it must communicate with a network. Communication may be through wired or wireless means. While there are risks such as man-in-the-middle attacks that are shared by both wired and wireless communication, the realm of wireless communication has many more opportunities for malicious exploitation. Due to the many potential wireless communication protocols, an IoT device may communicate through, each with its peculiar vulnerabilities, it is essential to evaluate the risks a device is subject to in each risk category.

**Table 3. Network Layer (Amazon Echo Dot Example)**

	Data				Risk				Function Blocking
	Privacy		Confidentiality		Device Loss of Control				
	Direct	Indirect	Direct	Indirect	Data Theft	Surveillance	Malicious Actuation	Reputational	
<b>Communications Capabilities</b>									
Wired									
<b>Wireless</b>									
Wi-Fi	X		X		X	X			X
Bluetooth	X		X		X	X			X
Near Field Communication									
Cellular									
Sound									
Light									
Other									

Examining an Echo Dot at the network layer perspective reveals that the Echo uses two wireless interfaces. Both of these interfaces are subject to the known cybersecurity threats associated with those communications methods. Since communication utilizes radio transmission, radio signals can be intercepted and captured, leading to risks regarding any data transmitted. Finally, a denial of service attack can be deployed against such a device’s network layer, by flooding the network with radio frequency interference.

Lastly, the application layer ties together the sensing and network capabilities to give an IoT device its functional capabilities. This layer

may include application software on the device, as well as services provided by a third-party. This combination presents a challenge when evaluating risks, as particularly when evaluating the risks from third-party services, there may be little transparency. IoT devices contain a software layer that acts as an operating system and supports hardware and networking functionality, as well as the software that provides device functionality. Each of these areas of potential vulnerability must be evaluated based on their associated risks.

Table 4 summarizes the application layer risks. This layer addresses device functionality in terms of both data collection and device control. From a data perspective, how data are collected, used, and stored are areas that need to be assessed for risk. As mentioned earlier, the data an

**Table 4. Application Layer (Amazon Echo Dot Example)**

	Data				Risk				Function Blocking
	Privacy		Confidentiality		Device Threats				
	Direct	Indirect	Direct	Indirect	Data Theft	Surveillance	Malicious Actuation	Repurposing	
<b>Capability</b>									
<b>Data Collection</b>									
Sensor Input	X	X	X	X	X	X			
<b>Data Persistence</b>									
Long Term	X	X	X	X	X	X			
Short Term	X	X	X	X	X	X			
<b>Data Use</b>									
Immediate Function	X		X		X	X			
Cummulative Capture & Processing	X		X		X	X			
<b>Data Storage</b>									
Local Device	X		X		X				
Remote Storage	X		X		X				
<b>Device Control</b>									
<b>Control Actuation</b>									
Device Only					X	X	X	X	X
Other Devices					X	X	X	X	X

IoT device collects or works with, may not be just stored on the device, but may also be handled and stored by third-party services. Complicating this picture further is how an IoT device is controlled, or in turn, controls other devices. Each of these areas needs to be

evaluated for cybersecurity risks to get an accurate picture of the risk exposure in adopting a given IoT device.

The application layer reveals a wealth of cybersecurity risks. The software that controls the device may be susceptible to exploitation, opening to a range of risks spanning data theft to malicious control and repurposing of such a device. Complicating the picture further is the susceptibility of third-party services to malicious exploitation that can result in data theft or compromise, as well as the possibility of malicious device actuation or repurposing. Adding to this is the potential for the functionality of the device to be blocked either through local control or through the third party services a device may use.

In the Amazon Echo Dot example, a device user would be able to use the proposed framework to evaluate their risk exposure from adopting the device. The risks identified show a certain degree of overlap based on the architectural layer analyzed. That overlap is a result of the different facets of a device's capabilities highlighted by each architectural layer. So while one layer may emphasize the sensing aspect of a device, another layer emphasizes the software control of those sensing mechanisms. Ultimately, looking at the aggregate results provides a comprehensive view of the cybersecurity risks associated with the adoption of an IoT device.

#### **4. Conclusion**

This paper presents a framework for evaluating cybersecurity risk exposure when adopting IoT devices. It is by no means an exhaustive treatment of the risks associated with device adoption, but it does provide a systematic approach to evaluating risk. The three-layer architectural model provides a useful abstraction of an IoT device's capabilities, facilitating the evaluation of risks in the data and device threat categories. Proceeding through a risk analysis at each architectural layer yields a comprehensive view of IoT cybersecurity risks.

The decision to adopt an IoT device is a balance between a device's perceived benefits to users and the inherent cybersecurity risks in adopting such a device. In making such a decision, users need to weigh potential risks, the likelihood of realizing those risks, and the perceived benefits of the device. The proposed framework addresses the potential risk question. The framework does not address the issue of the likelihood that a particular risk is realized; that exercise is something users will have to engage in based on the proposed device's use and environment. Furthermore, if the decision is made to adopt an IoT device, users will also have to decide what steps to take to mitigate or accept any risks that are identified as likely to be realized. Those decisions, though, rely on developing a comprehensive picture of the cybersecurity risk exposure inherent in adopting a given IoT device.

The study yields several interesting managerial implications. The study proposed a qualitative framework to assess the cybersecurity of IoT. Firms could have a macro perspective to understand the threats of IoT cybersecurity issues from their products or services. It can establish a foundation of deep insights that enable organizations to map out how these security issues relate to certain layers of IoT structure, scenarios, or products. Tapping into what motivates a particular security issue through this qualitative framework could help firms understand the issue more deeply and more comprehensively. We suggest that the framework would consider emphasizing the types and chances of securities differently across the whole architecture. For example, in the Amazon Echo Dot case, we clearly present the potential security issues across the sensor layer, network layer, and application layer. Specifically, the most vulnerable layer in the IoT structure may be the application layer, compared to sensor and connection layers. The insight highlights the necessity and significance for firms to take security solutions on the application layer. The study also contributes to risk management literature. Risk classification is a strategic approach to risk management. Firms segment their resources into certain risk categories so that they focus on similar or related issues to improve efficiency. In the qualitative analysis results, the device threats seem more severe than data confidentiality and privacy issues. This surprising finding highlights the significances of security taxonomy because both

two issues are based on different technical requirements. Accordingly, the distinction between the two IoT security issues can help improve risk assessment efficiency and performance. Additionally, although the paper uses a three-layer architecture, the proposed framework can also be applied to IoT architectures with four layers and five layers.

The insights of the study also have important implications for practitioners. This study offers firms in the IoT industry a systematic framework to engage in cybersecurity risk discovery. The framework provides firms with general guidance on how to relate various security risks to different layers and functions of IoT devices. Since the framework requires professionals with expertise in data and device administration, firms need to employ people who possess the technical skills in performing large scale data analysis and device management. Cybersecurity issues of IoT are commonly discussed among professionals in industries, but only interspersed in some specific layer or communication technology. Although there are some cybersecurity frameworks such as NIST Cybersecurity Framework, there lacks a framework specially designed for IoT. This implies that risk management of IoT industry would greatly benefit in terms of reliability by employing our proposed risk assessment framework to highlight the potential risks in data and device access control from a holistic perspective. A traditional risk analysis cannot be relied upon to identify risks as, counter to the conventional wisdom, device threats may have a higher incidence in the IoT industry than data risks. This implies that, while practitioners can continue to focus on data breach or data confidentiality issues, device threat analysis may also be a primary mechanism used to locate the cybersecurity issues in the IoT industry.

## **Acknowledgement**

The authors are grateful to the editors, especially Professor Nagib Callaos, for their guidance. We also send our thanks to Dr. Tawei (David) Wang, USA, DePaul University for his support as peer editor of this article, and Dr. Fengchun Tang USA, Virginia Commonwealth University, School of Business, for his support as a non-anonymous peer reviewer of this article.

## References

- Adat, V., & Gupta, B. B. (2018). Security in Internet of Things: issues, challenges, taxonomy, and architecture. *Telecommunication Systems*, 67(3), 423–441.
- Al-Sibai, H. S., Alrubaie, T., & Elmedany, W. M. (2021). IoT cybersecurity threats mitigation via integrated technical and non-technical solutions. *International Journal of Electronic Security and Digital Forensics*, 13(3), 298–333.
- Arora, A., Kaur, A., Bhushan, B., & Saini, H. (2019). Security concerns and future trends of Internet of Things. In *2019 2nd international conference on intelligent computing, instrumentation and control technologies (ICICICT)* (Vol. 1, pp. 891–896). IEEE.
- Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*, 68, 81–97.
- Bertino, E. (2016). Data Security and Privacy in the IoT. In *EDBT* (Vol. 2016, pp. 1–3).
- Brenner, B. (2017). Know the risks of Amazon Alexa and Google Home. Retrieved from <https://nakedsecurity.sophos.com/2017/01/27/data-privacy-day-know-the-risks-of-amazon-alexa-and-google-home/>
- Burhan, M., Rehman, R. A., Khan, B., & Kim, B.-S. (2018). IoT elements, layered architectures and security issues: A comprehensive survey. *Sensors*, 18(9), 2796.
- Chanal, P. M., & Kakkasageri, M. S. (2020). Security and privacy in IOT: a survey. *Wireless Personal Communications*, 115(2), 1667–1693.
- Commission, F. T. (2015). *Internet of things: Privacy & security in a connected world*. Washington, DC: Federal Trade Commission.
- Cvitić, I., & Vujić, M. (2015). CLASSIFICATION OF SECURITY RISKS IN THE IOT ENVIRONMENT. *Annals of DAAAM & Proceedings*, 26(1).
- Fagan, M., Megas, K., Scarfone, K., & Smith, M. (2019). Core cybersecurity feature baseline for securable IoT devices: A starting point for IoT device manufacturers. National Institute of Standards and Technology.
- Feng, Y., Yao, Y., & Sadeh, N. (2021). A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1–16).
- Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660.
- Hadzovic, S. (2021). Internet of Things from a regulatory point of view. In *2021 20th International Symposium INFOTEH-JAHORINA (INFOTEH)* (pp. 1–4). IEEE.
- Hou, J., Qu, L., & Shi, W. (2019). A survey on internet of things security from data perspectives. *Computer Networks*, 148, 295–306.
- Latif, S., Idrees, Z., Ahmad, J., Zheng, L., & Zou, Z. (2021). A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things. *Journal of Industrial Information Integration*, 21, 100190.
- Liang, W., & Ji, N. (2021). Privacy challenges of IoT-based blockchain: a systematic review. *Cluster Computing*, 1–19.
- Markose, A., Sharief, S., Ramprasath, J., & Krishnaraj, N. (2021). Survey on Application of IoT and its Automation. *International Journal of Advanced Engineering Research and Science*, 8, 6.
- Nord, J. H., Koohang, A., & Paliszkievicz, J. (2019). The Internet of Things: Review and theoretical framework. *Expert Systems with Applications*, 133, 97–108.
- Qi, X., Su, Y., Yu, K., Li, J., Hua, Q., Wen, Z., ... Sato, T. (2019). Design and performance evaluation of content-oriented communication system for IoT network: A case study of named node networking for real-time video streaming system. *IEEE Access*, 7, 88138–88149.
- Šikanjić, N., Avramović, Z. Ž., & Marinković, D. (2021). Cybersecurity IoT Architecture: One Proposed Solution for the Security Risks and Threats. In *The 1st International Conference on Maritime Education and Development: Icmmed* (p. 325). Springer Nature.

Valinsky, J. (2019). Amazon reportedly employs thousands of people to listen to your Alexa conversations. CNN Business. Retrieved from <https://www.cnn.com/2019/04/11/tech/amazon-alexa-listening/index.html>