



RESEARCH ARTICLE

Enhancing resilience in IoT cybersecurity: the roles of obfuscation and diversification techniques for improving the multilayered cybersecurity of IoT systems

Sampsa Rauti¹  and Samuli Laato^{1,2} 

¹Department of Computing, University of Turku, Turku, Finland

²Faculty of Information Technology and Communication Science, Tampere University, Tampere, Finland

Corresponding author: Sampsa Rauti; Email: sjprau@utu.fi

Received: 04 July 2023; **Revised:** 02 August 2024; **Accepted:** 10 October 2024

Keywords: obfuscation; diversification; IoT; software security; privacy

Abbreviations: IoT, Internet of things; EU, European Union; GDPR, General Data Protection Regulation

Abstract

In our digitalized modern society where cyber-physical systems and internet-of-things (IoT) devices are increasingly commonplace, it is paramount that we are able to assure the cybersecurity of the systems that we rely on. As a fundamental policy, we join the advocates of multilayered cybersecurity measures, where resilience is built into IoT systems by relying on multiple defensive techniques. While existing legislation such as the General Data Protection Regulation (GDPR) also takes this stance, the technical implementation of these measures is left open. This invites research into the landscape of multilayered defensive measures, and within this problem space, we focus on two defensive measures: obfuscation and diversification. In this study, through a literature review, we situate these measures within the broader IoT cybersecurity landscape and show how they operate with other security measures built on the network and within IoT devices themselves. Our findings highlight that obfuscation and diversification show promise in contributing to a cost-effective robust cybersecurity ecosystem in today's diverse cyber threat landscape.

Policy Significance Statement

Our work offers an overview of the scientific literature on the IoT device cybersecurity landscape, and the role of obfuscation and diversification techniques. The findings highlight obfuscation and diversification as promising approaches for providing a cost-effective layer in the multilayered security of IoT systems. We encourage building a stronger link between legislation such as the General Data Protection Regulation (GDPR) and policy documents and advocate that multi-layered cybersecurity measures should be mandatory for high-risk IoT systems. We discuss the difficulties deriving concrete design and implementation guidelines from existing IoT policies and security legislation. We propose amending existing IoT policies by providing stronger connections to legislation, and simultaneously, to provide more concrete implementation examples for IoT developers.

1. Introduction

The world is becoming increasingly interconnected in both the physical and digital space. One manifestation of this trend is the growing use of commercial cyber-physical systems and smart devices in

households as well as industrial production (Statista, 2023). When such systems are connected to one another over a network, the resulting network is called the Internet of Things (IoT). Since there is some dispute over the exact definition of the term (Li et al., 2015), in this study, we define IoT as a broad umbrella term that generally refers to connecting smart house appliances (e.g., lamps, vacuum cleaners, or refrigerators), industrial devices, urban infrastructure (e.g., lamp posts, security cameras, sprinkler systems) and transportation (cars, airplanes, drones) to the internet. IoT devices can be remotely controlled, they can automatically utilize online data to optimize their performance, and they overall hold the potential to automate mundane tasks, improve energy efficiency, and even improve safety and security (Kumar et al., 2019; Li et al., 2015; Nord et al., 2019).

Despite these many promises, the concept of IoT has been plagued by security concerns pertaining primarily to privacy and cybersecurity (Li et al., 2016; Lu and Da Xu, 2018). Regarding privacy, IoT devices often accumulate sensitive sensor data from users, and if leaked, this data may be used for nefarious purposes (Weber, 2015). To counter this, edge and fog computing approaches have been proposed where the users' data never leaves their houses (Li et al., 2018). However, privacy issues may also arise through hacked IoT devices where an adversary gains access to the devices through e.g., weak passwords or the IoT devices running outdated systems with security vulnerabilities (Kolias et al., 2017). For example, a few of the largest botnet cases reported during the past decade (Mirai, Meris) have been running on IoT devices (e.g., cameras and internet routers)¹. In addition to being used as part of a botnet for distributed denial-of-service (DDoS) attacks, compromised IoT devices may be used for a wide variety of nefarious or otherwise unwanted purposes ranging from spying on users to mining cryptocurrencies for the benefit of the perpetrator (Vignau et al., 2019).

The cybersecurity concerns and issues associated with IoT devices have been cited as a key barrier to adopting and using these systems (AlHogail and AlShahrani, 2019). One way to mitigate customers' hesitancy, is to adopt cybersecurity policies, such as those offered by ENISA (The European Union Agency for Cybersecurity) (ENISA, 2019), NIST (National Institute of Standards and Technology) (Ross et al., 2021) and Microsoft (Abendroth et al., 2017), which encourages IoT device manufacturers and providers to ensure a certain level of safety and protection for their systems. Taking a step back and looking at what legislation we have, GDPR (General Data Protection Regulation) already obligates companies to adopt "*appropriate technical and organizational measures*"² for assuring the cybersecurity of IT systems but provides only little guidance into what these technical measures are. This shifts the responsibility back to the developers, who are required to first define adequate cybersecurity measures for their specific use case, and then oversee their implementation. Here the role of cybersecurity policies is critical, as they offer comprehensive hands-on guidelines, frameworks, and best practices for developing secure systems (ENISA, 2019; Ross et al., 2021; Abendroth et al., 2017). Such guidelines can also build robustness in the overall IoT ecosystem, for example, in the format of guiding developers to use secure communication protocols and network segmentation (Mhaskar et al., 2021) as well as securing application programming interfaces (APIs) so that in the case of a security breach the damage done is mitigated (Lu and Da Xu, 2018).

This does not mean there would be a lack of resources spent on exploring cybersecurity options for IoT devices. For example, in the summer of 2024 Elsevier's Scopus listed over 4000 peer-reviewed studies with the keywords "IoT" and "cybersecurity" appearing in the title, abstract, or keywords. Within this body of research, academics have explored multiple proactive (Hetzler et al., 2023; Lei et al., 2018; Rauti and Leppänen, 2017) and reactive (Khraisat et al., 2019; Dissanayake et al., 2022; Aslan and Samet, 2020) measures. Among the proactive measures, some that have seen relatively little attention are obfuscation and diversification measures, but the few works that exist, suggest them as potentially beneficial measures worthy of further investigation (Collberg, 2018; Rauti et al., 2021). Therefore, in order to understand obfuscation and diversification as cybersecurity approaches for IoT devices, we observe the overall IoT

¹ Cybersecurity journalist Brian Krebs discusses IoT botnets and why they are popular in the following post: <https://krebsonsecurity.com/2021/09/krebsonsecurity-hit-by-huge-new-iot-botnet-meris/>, visited on the 13th of May, 2022

² Recital 78 of the GDPR, <https://gdpr-info.eu/recitals/no-78/>

cybersecurity landscape and locate how obfuscation and diversification fit in. Accordingly, we formulate the following research question (RQ) to guide this study:

RQ: How do obfuscation and diversification techniques compare and relate to the overall cybersecurity landscape of IoT devices?

To answer this question, we first systematically reviewed the academic literature on diversification and obfuscation techniques for IoT security ($n = 81$), and extracted the approaches for enhancing the multilayered security of IoT systems. In order to then understand these solutions as part of the overall IoT cybersecurity solutions landscape, we performed a bibliometric co-word analysis of the overall IoT cybersecurity research field ($n = 3682$) and evaluated obfuscation and diversification techniques in relation to this research profile. With this approach we contribute to the research field of IoT security (Abdullahi et al., 2022; Lu and Da Xu, 2018) by synthesizing the academic knowledge on obfuscation and diversification techniques (Hosseinzadeh et al., 2018) for improving the multilayered security of IoT devices. In addition, based on our findings, we derive policy implications for three prominent IoT cybersecurity policies. Finally, we extract future work avenues which can guide the next steps of academic research on obfuscation and diversification techniques within the domain of IoT cybersecurity.

The rest of this study is structured as follows. In [Section 2](#), we give an introduction to the cybersecurity of IoT devices, as well as diversification and obfuscation as security measures. In [Section 3](#), we describe our methods for the two literature search processes and subsequent data analyses. The section presents the results of our literature review, explores the found categories of diversification and obfuscation approaches, discusses an example architecture for multilayered security, and refines existing policies to account for multilayered security. [Section 5](#) summarizes our key findings, outlines implications for policy and practice, and presents an agenda for future research in this field. [Section 6](#) concludes our work.

2. Background

2.1. Cybersecurity of IoT devices

There are many characteristics in the proposed and existing use cases of IoT devices that make it critical to ensure their cybersecurity. These characteristics include IoT devices being part of people's homes, meaning compromised systems can be used to collect private or sensitive information, the IoT devices being critical cyber-physical systems that may cause harm in the real world through remote controlling (e.g. Rauti et al. (2020)) and the increased power consumption of a compromised system, them being used in botnets (Vignau et al., 2019). In order to improve the cybersecurity of IoT devices, it is paramount to understand their key characteristics and how they differ from other software systems and technologies. Drawing from previous academic literature on the topic, we list the key cybersecurity characteristics of IoT devices in [Table 1](#).

Implementing multilayered security measures is crucial to achieve effective protection of sensitive data and critical systems from advanced threats in all systems, not only IoT devices (Upadhyay et al., 2021; Rauti et al., 2021; Bhatia et al., 2008). We understand multilayered security as using several software security techniques to make up multiple layers of security to form a robust and comprehensive defense strategy. A multilayered approach provides increased defense by having multiple barriers in place and addressing various attack vectors. The ability to detect and respond to security incidents is enhanced as a result. For IoT devices in particular, past research lists several software security measures that can be employed in a multilayered security scheme:

- **Data encryption:** end-to-end encryption should be applied for all sensitive data that is stored or transmitted by IoT devices (Rajesh et al., 2019). This way, the data is protected against interception and unauthorized access, both in transit and at rest. It is worth noting that in some low-resource IoT devices, encryption can be too performance-intensive to be a viable alternative as a security measure (Panahi et al., 2021).

Table 1. *Key cybersecurity characteristics of IoT devices*

Concept	Description
Rarely updated	Very few IoT devices require updating beyond cybersecurity updates. (Remesh et al., 2020)
Minimal install	IoT devices typically run on low-power components and require small tailored operation systems e.g., a minimal install Linux distribution. (Hahm et al., 2015; Zikria et al., 2018)
Focus on data	A lot of IoT devices have sensors that collect data – this allows them to optimize energy consumption and so forth However, this data can also be highly sensitive. (Xu et al., 2019)
Communication with other devices	Extra care is needed to ensure that only trusted and desired parties are able to communicate with the IoT device. (Kolias et al., 2017)

- **Access control:** access control measures such as authentication and authorization restrict access to data and other resources based on user roles and privileges (Ravidas et al., 2019). Attention should be paid to appropriately setting default access permissions, as well as regularly reviewing and updating these permissions. Appropriate and strong authentication and authorization mechanisms need to be implemented to ensure that only trusted and authenticated devices or users can get access to an IoT device and critical resources (El-Hajj et al., 2019). Authentication entails providing credentials like usernames and passwords to prove one's identity. Authorization involves giving or denying access rights and permissions to users.
- **Software updates:** IoT devices' software should be kept up to date by applying the latest security patches and updates released by the vendors (Turner, 2019). This is an important way to strengthen software security and address known vulnerabilities. It is worth noting, however, that in many IoT devices, updates are not applied regularly or the device is not meant to receive updates at all (Kaur et al., 2023).
- **Secure configuration:** attention should be paid to the secure configuration of IoT devices (Bellman and van Oorschot, 2019). Unnecessary services should be disabled or turned off to minimize the attack surface. Securing configuration can also involve changing default credentials, securing remote access, and implementing multi-factor authentication, for example.
- **Virus, intrusion, and vulnerability monitoring:** the IoT system can be regularly scanned for vulnerabilities, and possible malicious activity and intrusions can be monitored. However, these kinds of monitoring tools are usually overly resource-intensive to be used with IoT devices (Alrubayyi et al., 2021). Because of constraints in processing power, memory, and energy, robust malware monitoring and detection mechanisms are challenging to implement.

In addition to these, there are obfuscation and diversification approaches (Collberg, 2018; Rauti et al., 2021), which are the main focus of this study, and which we discuss in further detail next.

2.2. *Obfuscation and diversification to enhance the multilayered security of software systems*

One of the important principles when developing software for IoT devices is to keep memory usage and computational requirements low so that IoT devices, with their limited memory and computation power, are able to operate smoothly (Hahm et al., 2015). This principle also holds for security solutions on IoT devices – performance, effectiveness, and power consumption should not be sacrificed for security when it can be avoided. This means many traditional solutions such as large anti-virus programs are not a reasonable security solution for most IoT devices and systems. Instead, computationally inexpensive and memory-efficient solutions are needed.

One such solution is interface diversification, which is an approach based on creating unique instances of software interfaces (Rauti et al., 2021). The program code is diversified so that different instances are syntactically different but functionality is not affected. Interface diversification can be achieved by employing various different source code obfuscation techniques (Collberg et al., 1997). Cohen presented one obfuscation approach in 1993 and proposed creating diversified versions of operating systems (Cohen, 1993). After this, there has been a large body of research concerning interface diversification (Hosseinzadeh et al., 2018), and in recent years, the idea has also been increasingly been applied to software running on IoT devices (Hosseinzadeh et al., 2016; Koivunen et al., 2016; Mäki et al., 2016).

Although there are billions of IoT devices connected to the internet, only a relatively small set of different operating systems and programs are being used on these devices. This monoculture is not unique only to IoT devices but is a key reason why obfuscation and diversification approaches hold so much potential in improving system security (Collberg, 2018). In other words, due to the identical design and well-known interfaces, large groups of IoT devices are susceptible to the same vulnerabilities and security attacks. Therefore, a malicious adversary can compromise a huge number of systems with a single attack, as evidenced by e.g., the Mirai botnet attacks (Kolias et al., 2017). Interface diversification is a way to add multiculturalism to the software design, which mitigates opportunities for non-targeted large-scale attacks (Rauti et al., 2021). Assuming a malicious attacker discovers how one unique IoT device is diversified, the other devices are still safe due to their unique and secret diversification. It would take more time and resources for the attacker to reverse engineer the diversification procedure, significantly slowing down the attacker. In the best scenario, the attacker is forced to build system-specific attack models, which renders various currently existing botnet approaches obsolete.

One of the main advantages of diversification is that the technique can improve system security without a significant increase in resource consumption (Rauti et al., 2021). For instance, using simple obfuscation techniques such as changing the names and parameter order of functions does not lead to increased computational power or memory usage. This makes the techniques particularly suitable for IoT devices that run preferably on low power and computational resources (Hosseinzadeh et al., 2016; Koivunen et al., 2016; Mäki et al., 2016). With the continuously increasing number of IoT devices, the incentives to attack the devices with bulk attacks also increase. For this reason, proactive protection techniques, in particular those addressing the monoculture issue of IoT (Collberg, 2018), should be given careful consideration. Here, obfuscation and diversification appear as the most promising solutions.

2.3. *Benefits and shortcomings of enhancing IoT security through diversification*

Recent studies have emphasized that since IoT devices are relatively seldom updated and run a very limited and rather static set of software, which can further fuel the monoculture problem (Collberg, 2018). To address this, internal interface diversification solutions may be particularly relevant and effective (Rauti et al., 2021), as well as other approaches discussed under the term “moving target defense” (Ge et al., 2021; Navas et al., 2020) e.g., in the popular IoT cybersecurity policy of NIST (Ross et al., 2021). Interface diversification has the following favorable properties:

Proactiveness. Interface diversification can be considered a proactive security measure: unlike many traditional security solutions, diversification does not assume that the exploit works in a certain way or that the malicious binary follows a specific pattern. Previously unknown zero-day exploits will be rendered useless if they try to use well-known interfaces (Cohen, 1993; Koivunen et al., 2016).

Passiveness. Interface diversification passively waits for the malware to make its move. The solution does not waste resources in trying to prevent malware from infiltrating the system or executing. However, the harmful software is prevented from working in an intended manner.

Low-performance requirements. When the diversification solution is kept relatively simple, for example by only diversifying system call numbers or names of library functions, the effects on the system performance are negligible or modest (Collberg et al., 1997). Obviously, this property is especially important in low-resource IoT devices.

Orthogonality. Interface diversification can be seen as a part of a multilayered security scheme. Diversification is orthogonal: it can be used together with many other security approaches. Traditional solutions such as intrusion detection systems and cryptography can be combined with interface diversification to enhance overall security (de Haro-Olmo et al., 2020). This is an important property because interface diversification is not a silver bullet that works against all attack scenarios.

Counterbalancing poor security. Interface diversification counterbalances the poor security of IoT devices by providing an additional layer of security. Even if a malicious program finds a vulnerability and invades the device, it cannot use the essential interfaces of the target system. This is especially important because software on IoT devices is often not updated regularly.

Invisibility. When diversification is applied to internal interfaces of the system, a normal end user does not notice anything out of the ordinary (Collberg et al., 1997). External interfaces that the user directly interacts (such as graphical user interfaces) with are left intact and not affected by diversification. Diversification also does not affect the software development process and programmers' work, because it can be applied automatically after the source code has been compiled.

The list of shortcomings of the approach is shorter, with perhaps the most important one being the monetary costs of implementing such solutions and challenges in deploying updates to the obfuscated devices (Koivunen et al., 2016). Even in cybersecurity, some cost/gain balancing needs to be done, and some obfuscation approaches may be needlessly costly while offering security that could also be achieved through other means. Another shortcoming may be on usability. It is not always entirely clear who would be in charge of obfuscating the system and deploying the solution. There is also the additional work of ensuring that the system would operate as intended for the user even after such measures have been put in place.

3. Materials and methods

The research process in this study is depicted in Figure 1. We conducted two literature searches, one for obfuscation and diversification for IoT cybersecurity, and another to understand the overall IoT cybersecurity research landscape. We then combined our findings from these approaches to understand obfuscation and diversification as part of the multilayered security solutions for IoT devices. With this approach, we can conceptually root the research on obfuscation and diversification firmly within the

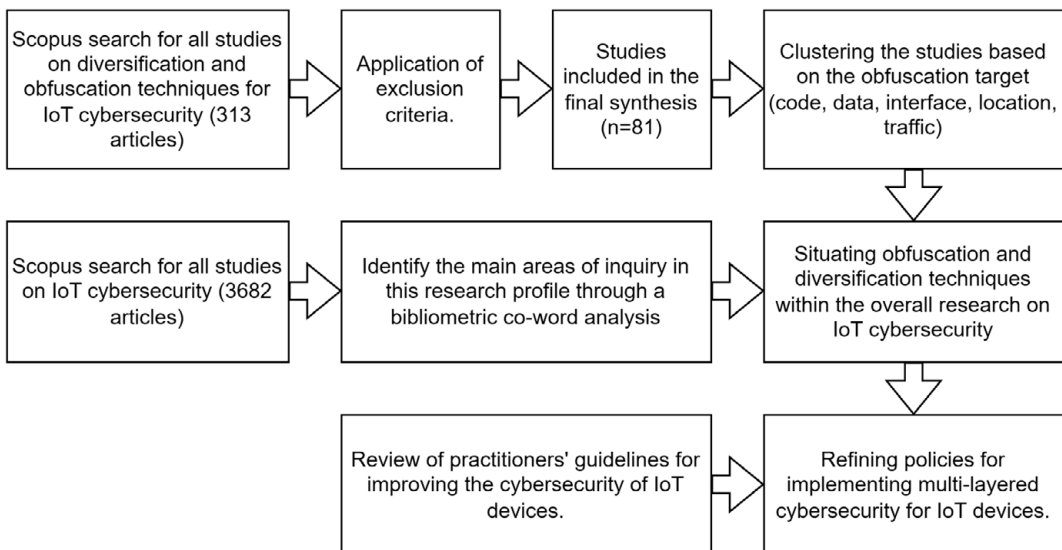


Figure 1. An overview of the research process in this study.

Table 2. *The search terms*

Main word	Synonyms or closely related terms
IoT	Internet of things, internet-of-things, smart home, smart devices, home automation
Cybersecurity	Data security, cyber security, information security, software security, security, privacy, trust
Diversification	Diversification, obfuscation, randomization, randomization

broader IoT cybersecurity field. Furthermore, as we observe obfuscation and diversification from this broader vantage point, we can derive points of departure for future work related to aspects such as the practicality, applicability, and feasibility of obfuscation and diversification for improving the multilayered cybersecurity solutions of IoT devices.

3.1. Literature research

3.1.1. *The first search: obfuscation and diversification for improving IoT cybersecurity*

In March–April 2022, we gathered keywords related to IoT, cybersecurity, and diversification. These keywords were gathered from reading existing literature reviews on IoT cybersecurity (Corallo et al., 2022; Lee, 2020; Lu and Da Xu, 2018; Kuzlu et al., 2021) and obfuscation and diversification (Hosseinzadeh et al., 2018). In addition, we read white papers and selected practitioner blog posts (e.g.³) on obfuscation and diversification for IoT. The final set of search terms resulting from this preliminary scoping are displayed in Table 2.

We chose to search for studies from the Elsevier Scopus research database due to its coverage of relevant research and its high standards in indexing studies. Scopus contains research from several relevant information systems and computer science research databases such as IEEE Xplore, DBLP Computer Science Bibliography, and ACM Digital Library. Furthermore, Scopus offers researchers a high level of control over the search terms and results curation as well as easy-to-use export tools. For these reasons, Scopus was estimated to be a good fit for this research.

Using the keywords specified in Table 2, we conducted a search on Scopus in April 2022. We limited the search to peer-reviewed studies only, which left us with 313 articles. We then proceeded to read the abstracts of the studies, excluding (1) articles that were not in English; (2) articles that were not peer-reviewed; and (3) articles that were not related to obfuscation and diversification techniques for IoT cybersecurity. During this process, we noticed that in particular the search term *diversification* was used to refer to various things other than the software/network cybersecurity techniques. Examples included (1) mentions where diversification was used to describe the proliferation, distribution, or adoption of IoT devices in real-world context; and (2) studies where “diversification” was used to describe the growing variance in the types of available IoT devices. We followed the abstract screening with a full-text assessment of the remaining studies and used the same criteria as in the previous step. These processes were carried out by the first author and resulted in the final number of 81 articles to be included in the final synthesis.

3.1.2. *The second search: the overall literature on IoT cybersecurity*

A preliminary search showed us that the amount of literature on IoT cybersecurity is enormous. For this reason, we chose the bibliometric co-word approach for understanding this research field, which is a particularly suitable method for bringing clarity to complex and large research fields (Laato et al., 2022; Malanski et al., 2021; Van Eck and Waltman, 2010). Similarly to the previous step we used Scopus. Since false positives are a critical concern in bibliometric reviews, we paid extra care in selecting the keywords.

³ <https://encyclopedia.thefreedictionary.com/internet+of+things>, accessed April 5, 2022

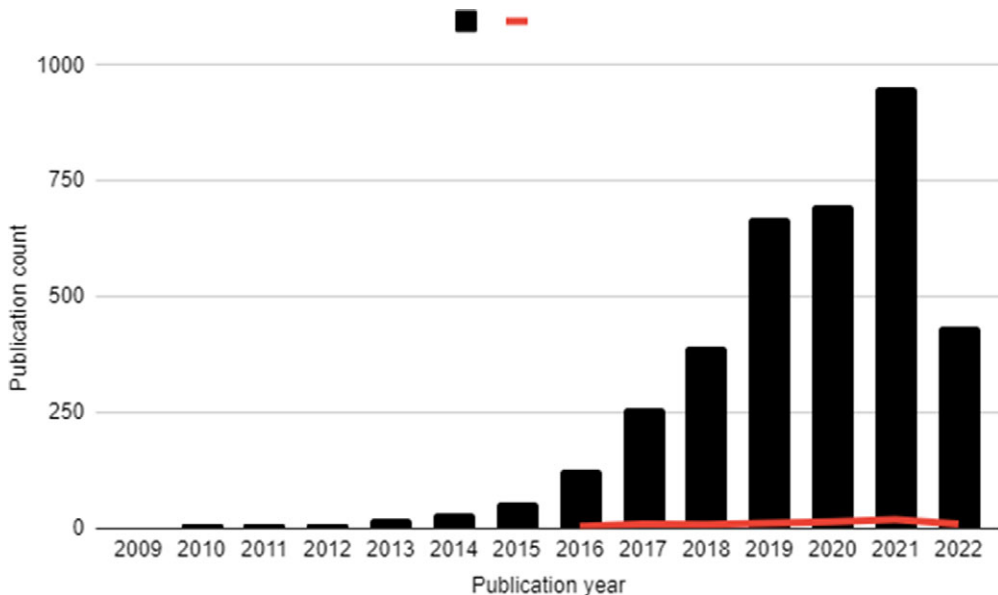


Figure 2. The publication years of the studies on IoT cybersecurity (black columns) compared to the publication years of diversification and obfuscation for IoT cybersecurity (red line). Both trends are similar in trajectory with no notable observable differences.

For example, we omitted general one word keywords such as *security*, *privacy* and *trust* which were part of the search string in the first search. Instead, we chose more descriptive terms such as *software security* and *information security*. Based on these keywords we formulated a search string combining the IoT and cybersecurity keywords. The final search was performed on the 11th of June 2022. This search resulted into 4218 articles. The articles were limited to peer-reviewed studies only (journal articles, conference proceedings and book chapters), which resulted in the final number of 3682 articles to be included in the bibliometric review.

3.2. Data analysis

We began our analysis by reading through the 81 studies to familiarize ourselves with their contents, and for supporting our understanding of the feasibility of the measures. We then specifically extracted from the initial set of papers ($n = 81$) the target of the technical obfuscation (which was specified either explicitly or implicitly), the publication years of the studies to see if obfuscation techniques were a growing, diminishing or stable trend within the broader IoT cybersecurity literature and an overview of the outcomes, whether the authors expressed obfuscation and diversification as promising solutions for IoT cybersecurity or not.

Second, we moved to the larger sample of studies ($n = 3682$), and extracted bibliometric information from the studies including (1) publication year; (2) document type; (3) subject area; (4) publication venue; (5) most popular keywords; and (6) country of the first author. From this information, we are able to obtain an understanding of where the research has been conducted and published and when. This data could also reveal biases in the research field and offer opportunities for future research.

Third, we conducted a co-word analysis to understand the research profile in more detail. Co-word analysis is a data mining technique that connects keywords that appear in the same paper together, forming a network of concepts that highlights their relationships (Van Eck and Waltman, 2010). In this study, we specified that only keywords that appeared in four or more studies are included in the final concept network. By setting this limit, the analysis result excludes weak relationships (that may be accidental) and

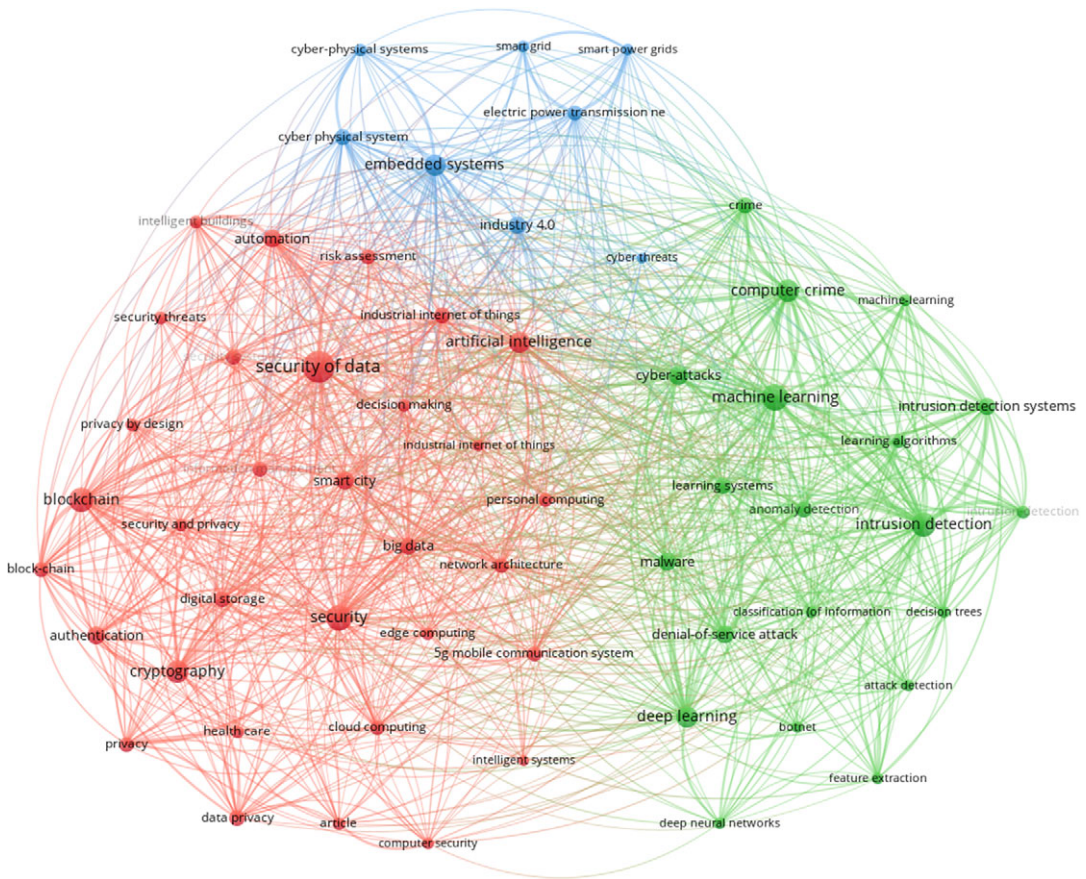


Figure 3. Visualizing the bibliometric co-word analysis.

thus increases the reliability of the result. We performed the analysis using the VOSviewer tool (Van Eck and Waltman, 2010), and looked at the author-given keywords. We iterated the analysis a couple of times and combined similar keywords together, and testing the outcome by tweaking how many times the keywords had to appear together in the sample of studies to be included in Figure 3. The iterations and decisions in this process were influenced by the authors' evolving understanding of the research profile as they got more acquainted with the studies in the final sample.

Fourth, we compared the target areas of obfuscation from the initial set of papers ($n = 81$) as well as the publication years of these studies to those within the broad IoT cybersecurity research ($n = 3682$). This approach allowed us to obtain an understanding of the trends and trajectories of obfuscation and diversification research within the overall IoT cybersecurity research domain.

Fifth and finally, we reviewed practitioners' guidelines for improving the cybersecurity of IoT devices. Our main aim was to understand what the existing policies are for improving and implementing cybersecurity for IoT devices, and whether our work would offer any implications to them. We chose to review three prominent policy guidelines which were selected as follows. First, we looked for IoT cybersecurity policy documentation from technology industry leaders and chose a document provided by Microsoft. Second, we looked at major policy providers in the European and North American regions and settled upon the policies offered by ENISA and NIST. More precisely, we refer to the ENISA guidelines for IoT cybersecurity (ENISA, 2019) (particularly Section 4.2 of this document, which includes the recommended technical measures), Microsoft's cybersecurity policy for the internet of things Abendroth et al. (2017), and NIST's general guidelines for developing cyber-resilient systems (Ross et al., 2021).

4. Findings

We present our findings by first focusing on the overall bibliometric profile of the IoT cybersecurity field and then connecting the findings from the obfuscation and diversification literature to this research field. Finally, we present our examination of the guidelines for IoT cybersecurity and what implications our findings have for those existing policies and beyond.

4.1. *The bibliometric profile of the research field of IoT cybersecurity*

As demonstrated in [Figure 2](#), the research field of IoT cybersecurity is growing strongly with more publications out each year than the year before. The field began growing rapidly in 2013, and the number of publications more than doubled each year until 2017. Afterwards the growth of the research field has continued steadily at a roughly linear rate, but as of 2019 has also shown some signs of plateauing soon. Perhaps unsurprisingly, the number of IoT cybersecurity publications is positively correlated with the number of publications within the entire field of IoT. According to Scopus, the number studies mentioning IoT in the title, abstract, or keywords has been in the tens of thousands each year after the year 2017, peaking at 62,549 studies published in 2021. From here we can make the crude estimation that IoT cybersecurity research is roughly one-seventh of the total number of IoT publications. Looking at obfuscation and diversification within the IoT cybersecurity field, we see that it represents roughly 1/45 of the overall IoT cybersecurity research. As a trend, obfuscation for IoT research has been growing roughly at the same rate as the overall IoT cybersecurity research.

The majority of the studies within the field of IoT cybersecurity are published in conference proceedings ($n = 2037$) followed by journals ($n = 1439$). The remainder ($n = 206$) are book chapters and other peer-reviewed publications. According to Scopus, these studies are overwhelmingly carried out in the field of computer science ($n = 2972$) or engineering ($n = 1928$), but a significant number of studies are also conducted within the field of mathematics ($n = 575$) and decision sciences ($n = 564$). There is also overlap in the field classifications, meaning some studies are interdisciplinary and related to both mathematics and computer science. The majority of the research is produced by scholars from the USA ($n = 641$) followed by China ($n = 567$), India ($n = 452$), the United Kingdom ($n = 303$), and Australia ($n = 164$). Altogether, the research has been carried out in 101 different countries. While there certainly is an emphasis on the USA, China, and India, these numbers roughly correlate to the overall research output of these countries. Hence, we estimate that no significant country-related publication bias exists in this domain.

The results of the co-word analysis are displayed in [Figure 3](#). The concept map in [Figure 3](#) illustrates that while academics have studied many security technologies closely related to obfuscation and diversification, these techniques, and proactive cybersecurity measures in general, seem to be missing from the big picture. Next, we discuss these two in further detail with references to the studies.

4.2. *Categories of diversification and obfuscation approaches within the landscape of IoT cybersecurity research*

[Table 3](#) shows different categories of obfuscation related to IoT cybersecurity. Most of the obfuscation schemes introduced in analyzed papers concentrated on obfuscating data ($n = 22$). The data processed by IoT devices can be obfuscated to protect users' privacy or intellectual property. While encryption is usually the primary method for protecting data from adversaries, using obfuscating techniques instead of encryption is often necessary when it comes to IoT devices with limited resources and low computational power (Khan et al., 2017). A special category of data obfuscation in mobile IoT devices is location obfuscation ($n = 11$), which aims to preserve the user's location privacy while preserving service utility (Butun et al., 2019).

Many obfuscation approaches concentrate on traditional code obfuscation ($n = 10$), in other words, obfuscating the internal structure of programs in order to make it more difficult for the adversaries to understand reverse engineer, and modify programs. For example, Nausheen and Begum propose

Table 3. *The obfuscation targets*

Obfuscation target	Number of publications
Data obfuscation	22
Code obfuscation by malware	17
Location obfuscation	11
Code obfuscation	10
Traffic obfuscation	8
Route obfuscation	7
Interface obfuscation	4
IP address obfuscation	2

protecting mobile eHealth applications using code obfuscation techniques (Nausheen and Begum, 2018), while Pastrana et al. present an obfuscation mechanism against code reuse attacks for embedded devices (Pastrana et al., 2016).

Several internal interfaces of IoT devices can also be obfuscated ($n = 4$) to prevent malware authors from abusing the device's resources. Koivunen et al., for example, propose obfuscating several internal interfaces of IoT devices, such as system call interfaces and operating system libraries (Koivunen et al., 2016). Interface diversification is a lightweight protection mechanism that does not require lots of computational resources, unlike many traditional software security mechanisms.

In the studied papers, software obfuscation is also regularly used by malware authors to hide the malicious nature of their code and executables ($n = 17$). As malware authors produce several diversified functionally equivalent versions of their harmful programs, approaches for measuring the similarity of these diversified pieces of malware have to be developed (e.g., Venkatraman and Alazab, 2017).

When it comes to obfuscation on network level, obfuscating the contents and patterns of network packets is a popular approach ($n = 8$). Datta et al. introduce a library that replaces standard networking functions and obfuscates traffic patterns of an IoT device by using payload padding, fragmentation mechanisms, and randomly generated fake traffic (Datta et al., 2018). The way packets are routed in a network ($n = 7$) can also be obfuscated (Bin-Yahya and Shen, 2022). For example, Bin-Yahya and Shen (Bin-Yahya and Shen, 2021) present a proactive route mutation scheme that alters the routes in wireless sensor networks to prevent reconnaissance and sniffer attacks. Research has also looked at IP address obfuscation ($n = 2$) and reassigning IP addresses as a moving target defense approach in order to prevent attackers from targeting IoT devices (He et al., 2021).

Turning to the larger IoT security picture of Figure 3, we can see that obfuscation and proactive security methods in general are absent in the picture. However, software and network-level obfuscation contribute to many general principles in the red area, such as security, data security, and cryptography. Software security is enhanced by protecting the internal structure of programs and diversifying interfaces, making it difficult for malware to attach itself to programs or interfaces and abuse them to achieve its goals (Cohen, 1993). On the other hand, data privacy in IoT systems can also be protected by using obfuscation like lightweight encryption when computation-intensive encryption methods cannot be used to ensure confidentiality of data (Yavari et al., 2017).

In the green area, central themes are malware, machine learning, and intrusion detection. Obfuscation is connected to machine learning and artificial intelligence mainly through efforts by researchers to use these approaches to classify and understand obfuscated malicious code (Dib et al., 2021). Obfuscated malicious programs and network traffic can also be detected by intrusion and anomaly detection tools.

Finally, the blue area highlights the industrial internet and applications of IoT such as smart power grids and power transmission networks. Such parts of critical infrastructure that may never receive security updates can greatly benefit from supplementary security measures such as diversification (Koivunen et al., 2016).

4.3. An example framework applying obfuscation and interface diversification as a part of a multilayered software security scheme

As noted previously, one of the key advantages of interface diversification and obfuscation techniques is the fact that they are orthogonal. Diversification can be combined with many other security measures. Several traditional security techniques and approaches, such as intrusion detection systems and access control mechanisms can be used together with obfuscation and diversification to enhance overall security (Rauti et al., 2021; de Haro-Olmo et al., 2020). In what follows, we describe a conceptual software security framework consisting of several, mostly proactive, security measures. The framework demonstrates how interface diversification can be used along with other security mechanisms to improve the security of IoT systems. We will also discuss the relationship other techniques have with interface diversification. The framework includes the following security measures:

- **Interface diversification:** Essential interfaces of the system, including e.g. operating system library interfaces and the system call interfaces are diversified to prevent malicious actors from abusing them. Consequently, it becomes more challenging for the adversary to gain access to valuable resources such as data.
- **Data obfuscation:** Data stored on the IoT device can be obfuscated for better data security and privacy. While encryption should usually be the primary way to protect data from unauthorized access, it is sometimes too performance-intensive for IoT devices. In these cases, obfuscation is employed as a lightweight mechanism to protect data.
- **Access control:** It is important to ensure the IoT device is protected by strong authentication and authorization mechanisms. Special care should be taken to change the default credentials. Interface diversification and obfuscation can protect the device even in cases in which the authentication mechanism fails, for instance, because of a weak password.
- **Software updates:** If possible, the system should receive software updates regularly. However, as this is often not the case with many IoT devices, diversification and obfuscation as security measures can complement missing software updates, providing an additional level of security. Moreover, zero-day threats aiming to exploit unknown vulnerabilities in the target device's software frequently appear. These threats cannot be thwarted with software updates when they first appear. Interface diversification is an important security measure that introduces unpredictability for the attacker and prevents many zero-day attacks ((Rauti et al., 2021).
- **Moving target defense (MTD):** MTD ((Lei et al., 2018) can be used to change the diversification regularly and increase uncertainty for the attacker. This is an effective, proactive, and adaptive defense mechanism ((Cho et al., 2020), which still has only modest costs in terms of resource consumption. A newly diversified set of interfaces can be installed into the system as a part of a software update, for instance.
- **Secure configuration:** The system has to be protected by using a secure configuration and minimizing attack surface by only including the necessary services in the system. The secure configuration also supports diversification solutions: implementing, deploying, and changing interface diversification is easier with a limited set of interfaces and services.
- **Intrusion detection:** Oftentimes, continuously monitoring an IoT system with solutions such as intrusions detection systems and antivirus software, which are potentially quite intensive resource, may not be a viable option. Employing interface diversification and obfuscation techniques is one way to fill this gap. However, some lightweight intrusions detection schemes may still be feasible on IoT devices. One way to implement a lightweight intrusion detection scheme in the host system is to uniquely diversify the interfaces in a system but also leave the original interfaces as traps for attackers. As the trusted programs in the system only use the new secret interfaces, the use of the "fake original interfaces" is always suspicious and a sign that something abnormal is happening in the system.

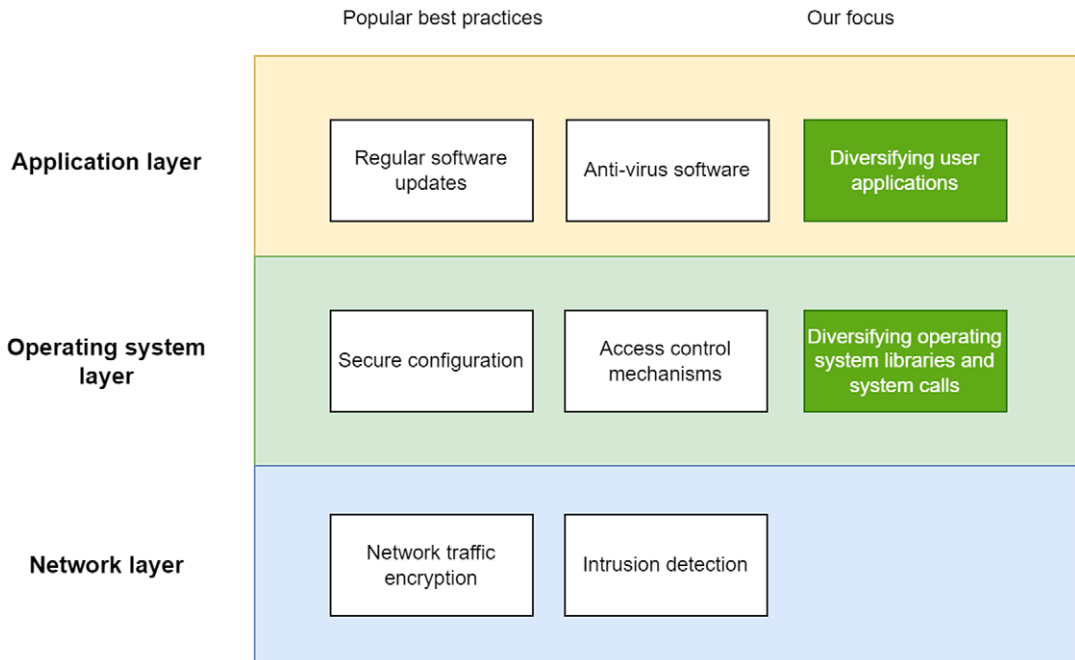


Figure 4. An example of the practical architecture of the multilayered software security scheme. *NOTE:* This is not an exhaustive summary of all possible cybersecurity measures, but rather, it is an exemplar of cybersecurity architecture.

This proactive security framework lays a basis for a collection of security measures that are a good fit for IoT systems with restricted resources, focus on data, rare updates, and minimal installs – key characteristics we described previously. As a multilayered security framework, it sets several barriers for the attacker and makes use of several proactive measures, adding uncertainty to the system from an adversary’s viewpoint. At the same time, it only requires a modest amount of resources such as computational power.

The conceptual framework we presented is an example of seamlessly combining interface diversification and obfuscation with other security measures. At the same time, it can also be understood as an example case of a possible recommendation or guideline of how to implement data security in IoT systems, bridging the obvious gap between practical software development and security policies. For instance, it is one possible way to implement the appropriate technical measures described only vaguely in the GDPR.

Figure 4 shows an abstract example of a multilayered software security scheme for IoT sorted into three layers: (1) application; (2) operating system; and (3) network layers. We situate existing cybersecurity measures within these three layers and display on the right in green boxes how obfuscation and diversification can be applied as proactive measures to boost the cybersecurity within this type of architecture for IoT cybersecurity. Note that based on this study we are not proposing at this stage to add obfuscation and diversification to the network layer due to problems in interoperability. While this has been investigated in a few works (Mäki et al., 2016), we encourage future research on this topic. Overall, the visualization in Figure 4 highlights the orthogonality of interface diversification as a software security measure: it can be used along with other measures in a multilayered scheme. Moreover, diversification itself is a multilayered security measure in the architecture, as it covers both the operating system level and applications (e.g., when diversifying the system call interface, we are making changes on the operating system layer, but these changes need to be propagated to trusted applications in the application layer in order for these applications to keep working (Rauti et al., 2021).

Table 4. Existing popular privacy policies discussed in this study

Publisher	Pub. year	Description	Link
ENISA	2019	IoT-specific cybersecurity policy /guidelines with a focus on software development. Covers the entire lifecycle of IoT products.	ENISA (2019)
Microsoft	2017	High abstraction level guidelines for IoT cybersecurity. Provides general guidance for developers and organizations but offers only minimal technical guidance.	Abendroth et al. (2017)
NIST	2021	A general cybersecurity policy for developers. Covers cybersecurity guidelines in IoT but also beyond.	Ross et al. (2021)

4.4. Refining existing policies to account for multilayered cybersecurity

In this section, we discuss refining existing IoT security policies and guidelines to account for implementing multilayered cybersecurity with obfuscation and diversification. As mentioned in [Section 3.3](#), we refer to three prominent cybersecurity policies: (1) ENISA (ENISA, 2019), (2) NIST (Ross et al., 2021), and (3) Microsoft (Abendroth et al., 2017). We summarize the characteristics of these policies in [Table 4](#). The guidelines from ENISA and Microsoft are IoT-specific, but the NIST policy is broader, yet it also covers IoT cybersecurity.

While prominent in the guidance offered by NIST (Ross et al., 2021), an element that receives minimal attention in ENISA's (ENISA, 2019) and Microsoft's (Abendroth et al., 2017) documents when contrasted against the academic corpus on IoT cybersecurity, is multilayered security and resilience. For example, ENISA's guideline recommends strict access control and choosing third-party libraries that are updated regularly (ENISA, 2019, p. 54). These are indeed important practices, but the principles of resilience can be better followed by building failsafe approaches in case these mechanisms fall short due to e.g., the following reasons: users may choose weak passwords or third parties may fail to update their software components (assuming the software of the specific IoT device can be updated at all) and even in the worst cases, accidentally introduce new vulnerabilities through updates. In these cases, diversification appears as a component of multilayered cybersecurity, a backup mechanism, and the next layer of defense protecting critical resources of the system. Microsoft's IoT security policy document Abendroth et al. (2017) does not go into details about technical software security measures. It mentions some security solutions as examples, mostly traditional software security measures as opposed to proactive security measures such as diversification. Although the importance of resilience is mentioned and emphasized (Abendroth et al., 2017, p. 9), proactive solutions and multilayered schemes are missing. In general, while proactive security measures improving resilience appear in the general cybersecurity policy document of NIST (Ross et al., 2021), they could be better integrated and included in the IoT-specific policy documents offered by Microsoft (Abendroth et al., 2017) and ENISA (ENISA, 2019).

Sometimes the nature and limitations of an IoT environment itself may prevent the implementation of the technical measures the analyzed policy documents recommend. For example, all IoT devices are not well equipped to "use proven encryption techniques" (ENISA, 2019, p. 54) due to limited computational power. Therefore, in some cases, obfuscation and diversification may be a viable option to provide some lightweight data protection (Xu et al., 2020). As a generic guideline for developing cyber-resilient systems, NIST's document Ross et al. (2021) does not specifically take into account this aspect of limited resources in IoT systems. Also, some IoT devices are not built to receive regular patches and updates (ENISA, 2019, p. 55), in which case diversification and obfuscation techniques can compensate for the shortage of software patches. Some IoT devices may even intentionally be designed to never receive updates (which can be a security measure in itself), and in these cases, it is critical to assure the security of these systems. Again under these circumstances, failsafe mechanisms and multilayered security offer a solution, with obfuscation and diversification being relevant techniques to reaching these goals.

The policy documents also recommended some techniques and approaches that we can implement in practice by using obfuscation and diversification techniques. For example, when implementing anti-tampering features (ENISA, 2019, p. 55), obfuscation has been found to be a feasible solution (Collberg and Thomborson, 2002). Another example is the recommendation to use whitelists for allowed applications (ENISA, 2019, p. 56). A diversification scheme applied to a system is inherently a whitelist, where only trusted applications can successfully interact with their environment. Moreover, obfuscation can be combined with other security mechanisms, such as regular updates. Security updates are not only an important mechanism to protect from external threats (Abendroth et al., 2017, p. 12) but also a possibility to dynamically change the applied diversification, implementing moving target defense (Ross et al., 2021, p. 99), where attack surface changes, making it more difficult for the attacker to reach their goals. In this sense, obfuscation, diversification, and other proactive measures could be explicitly mentioned in the guidelines, as they align perfectly with these proposed security measures.

Yet, these techniques also carry downsides, such as there being costs involved in successfully implementing these mechanisms within IoT software, and in propagating the changes to trusted software in a way that does not cause interoperability issues with other devices in the local IoT ecosystem. Clarification of the aspects of costs and benefits could help IoT system developers choose the most appropriate measures for securing their systems, and could make the policy documents more actionable.

Lastly, with the introduction of obfuscation and diversification, the existing policies could be extended to include recommendations that may not otherwise be easy to implement. For example, ENISA's IoT cybersecurity policy document (ENISA, 2019) does not mention any kind of intrusion detection, perhaps due to the limited resources IoT devices possess. On resource-constrained devices with limited performance, memory, and energy, it is challenging to implement resource-intensive intrusion detection schemes or run complex security algorithms on these devices. Obfuscation and diversification approaches can be combined with leaving "fake original interfaces" as traps in the system (e.g., honeypots). When trusted programs only use the new diversified and secret interfaces, any abnormal activities in the system can be caught without using much memory or computing power. Also, sometimes obfuscation can be used as a lightweight alternative for resource-intensive encryption proposed in the documents (Abendroth et al., 2017, p. 10).

Of the studied guidelines, NIST's general policy document (Ross et al., 2021) is the only one mentioning diversification and proactive cyber resiliency technologies in general. NIST's document lists several proactive "strategic design principles" (Ross et al., 2021, p. 136) and advocates diversity as a method to add unpredictability. The document does not, however, go into specifics about how to implement the measures in different layers. We conceptualize a practical design by providing an example of a potential multilayered security architecture involving diversification in addition to many traditional security measures (see Figure 4). Furthermore, since the policy document of NIST is not IoT-specific, we encourage policymakers to integrate the best practices from the work of NIST and academic research to construct more up-to-date hands-on guidelines for IoT developers to ensure cybersecurity within this rapidly growing field.

To sum up, since IoT devices have characteristics that distinguish them from other software (e.g., they are rarely updated, they are minimalist, they typically gather and make use of sensor data and communicate with other devices), there is certainly a demand for IoT-specific cybersecurity policies. Within these policies, obfuscation and diversification measures, and other similar proactive measures, could be proposed and explicitly mentioned in the cybersecurity policies (ENISA, 2019; Abendroth et al., 2017; Ross et al., 2021) to apply the principle of multilayered software security in practice, and consequently, improve system resilience against cyber threats. These measures can effectively be used to compensate for several security measures that cannot be implemented, to provide practical implementation for many of the recommended practices, and even to extend the guideline with new practical security measures that might otherwise be out of reach in the IoT environment.

5. Discussion

5.1. Key findings

We summarize our key findings as follows:

First, within the broad area of IoT cybersecurity, diversification, and obfuscation are promising techniques when assessed from the perspectives of proactiveness, passiveness, performance requirements, orthogonality, and invisibility.

Second, so far these techniques have seen relatively little attention in academia, although related approaches such as moving-target defense (Ge et al., 2021; Navas et al., 2020) have been popular in systems with high-security requirements.

Third, the findings of our review encourage more research and practical work on implementing obfuscation and diversification techniques for improving the multilayered cybersecurity of IoT devices. While some popular cybersecurity guidelines for IoT developers (ENISA, 2019) do not explicitly mention obfuscation and diversification measures, these proactive approaches can be used to directly implement some other mentioned approaches such as whitelisting trusted apps and deploying anti-tampering features. However, some more general (non-IoT-specific) cybersecurity policies mention aspects related to obfuscation and diversification (see e.g., Ross et al. (2021)), which suggests that they are relevant elements requiring further elaboration in the IoT context. For this reason, to improve existing guidance for IoT developers on making their systems secure, next, we discuss the implications of our findings for policy and practice.

5.2. Implications for policy and practice

We show that while the research on obfuscation and diversification techniques (Hosseinzadeh et al., 2018; Rauti et al., 2021 for IoT cybersecurity has been steadily growing along with the overall IoT cybersecurity literature (Kuzlu et al., 2021; Lee, 2020; Li et al., 2015), these techniques are not currently mentioned in popular practitioners' guidelines for IoT cybersecurity (ENISA, 2019; Ross et al., 2021). However, our findings suggest that there might now be a reason to amend this. First, our findings demonstrate that privacy protection through e.g., data obfuscation and location obfuscation as well as security measures through code obfuscation could add significant value to IoT systems that are rarely updated and which require resource-efficient multi-layered security and privacy solutions. Second, our findings show that there is a substantial quantity of research on malicious obfuscation where malware is being obfuscated by adversaries to penetrate IoT systems, indicating a risk that requires mitigation measures. Through [Figure 3](#) we visualize the main research trends. While the research on obfuscation and diversification is academic, it is not purely theoretical. For example, some proof-of-concept solutions demonstrate empirically the effectiveness of obfuscation and diversification for improving the multilayered security of IoT devices (Rauti et al., 2021). However, without issues, such approaches increase the overall costs of producing such systems and may give rise to challenges in interoperability, as IoT systems are made unique and less predictable. Thus, cybersecurity policies for IoT devices should perhaps only encourage such solutions for more sensitive and security-critical systems.

A related stream of research, moving target defense for IoT systems (Mercado-Velázquez et al., 2021; Navas et al., 2020), was also notably absent from the guidelines for IoT cybersecurity (ENISA, 2019; Ross et al., 2021). The literature provides an indication that these two could both add value. More precisely, through obfuscation and diversification, we are able to achieve increased attack surface complexity, making it more difficult for perpetrators to enter the system. Now, by combining this with moving target approaches, we can reduce the vulnerability window of systems, as the system is regularly changed and updated. It is also possible to combine the need to whitelist trusted processes in a diversified IoT system with a honeypot, where a perpetrator will attempt to use the wrong interfaces and their activities be recorded in the honeypot. Again, this is a very concrete approach for improving the multi-layered cybersecurity for IoT devices.

Regarding policy and practitioners' guidelines, we provide the following three implications. First, obfuscation and diversification show great promise in enhancing the multilayered cybersecurity of IoT

devices. Second, these approaches improve the resilience of the system, as they introduce complexity to the interfaces and make it more difficult for malware and perpetrators to enter the system even if other cybersecurity measures fail. Third, it can be used to mitigate zero-day attacks, as after diversification an IoT system is no longer the same exact copy of all other similar systems, but to a degree more unique and hence more difficult for perpetrators to enter. Thus, in summary, and light of the reviews conducted in this work, we encourage practitioners' guides (e.g., ENISA (2019); Abendroth et al. (2017)) to consider adding guidelines for developers to improve the resilience and multilayered cybersecurity of IoT devices through obfuscation and diversification. Also, to respond to today's complex cyber threats, regulation needs to guide software developers to implement proactive and resilient multi-layered cybersecurity schemes meeting regulatory compliance.

5.3. Reflection on the current regulation

There are many privacy regulations around the world, such as the GDPR in the EU, and the California Consumer Privacy Act (CCPA) which regulates privacy and collection practices in California, USA. Here we concentrate on the GDPR. The GDPR gives broad principle-based requirements rather than describing practical implementation of security measures in a detailed manner. It is clear that such vagueness is intentional so that the regulation is flexible enough and able to cover organizations and cases of various different sizes and risk profiles. At the same time, implementation of practical security measures may become challenging without separate policies that provide more hands-on-guidance to developers. Similarly, without clear guidance on GDPR compliance, it can be difficult to evaluate whether the cybersecurity measures in an IoT system are adequate.

When it comes to implementing privacy measures, the GDPR vaguely mentions "appropriate technical measures," but does not specifically talk about what exact measures and safeguards should be used to guarantee sufficient privacy for users. Similarly, the CCPA does talk about confidentiality and integrity of data, for example, but is not specific when it comes to technical measures. Based on our findings, one practical implementation for guaranteeing strong privacy would be multilayered cybersecurity e.g., through obfuscation, diversification, and other measures. Hence, we recommend that policymakers also more strongly reflect on what kinds of implementations and security measures would ensure that the IoT system is compliant with such regulations. This will help software architects and developers adopt the privacy-by-design approach in the software development process and give more concrete guidance on implementing the mentioned appropriate safeguards for protecting user privacy in compliance with existing regulations.

Multilayered cybersecurity is especially relevant when the privacy risk is considered high and sensitive data is being processed by IoT devices – such as in the case of medical devices. The GDPR specifically mentions some sensitive types of personal data such as data concerning health, and refers to these as "special category data". When the protection measures are chosen, the required resources and implementation costs need to be considered based on the required level of protection, which is acknowledged in Article 32 of the GDPR. However, it is important to also give recommendations for security schemes to use in situations in which sensitive information is processed and robust privacy has to be guaranteed. In these kinds of situations, the existing regulation should mention schemes like multilayered cybersecurity (Portokalidis and Keromytis (2011)) and moving target defense (Navas et al. (2020); Ross et al. (2021)).

Overall, in today's complex cybersecurity environment, just pseudonymization and encryption mentioned by Article 32 of the GDPR are not enough, especially in a limited-resource environment such as IoT devices. It is important for the legislation to also adapt and change with time, while also providing more concrete tools for developers to implement a sufficient level of privacy. Similarly, we need to update policy documents aimed at IoT developers to provide more concrete hands-on guidance on how to realistically and rigorously implement multi-layered cybersecurity that is safe and meets regulatory compliance.

Table 5. *Future research agenda on obfuscation and diversification techniques for IoT devices*

Focus area	Description of the future research topic
Case studies with commercial products	Studies on applying obfuscation/diversification in commercial products are largely missing. There is little academic knowledge on the applications of these approaches in commercial IoT products.
System comparison studies	There are various IoT devices, some with more processing power than others. Feasibility analyses are needed on what kinds of systems, and what parts of those systems, are worth protecting with diversification and obfuscation.
Approach comparison studies	It remains unclear why obfuscation and diversification have seen relatively little attention in academic IoT cybersecurity research. An important avenue for assessing the feasibility of this approach is to examine implementation costs, costs on usability, expected value, and security enhancement against various attacks.

5.4. *Limitations and future work*

This study raises questions as to why these techniques have seen so little attention in academic research despite their excellent alignment with the context of IoT cybersecurity. To investigate this issue further, we propose three key avenues for future research. First, research is needed with commercial obfuscation and diversification tools and products. This would provide insights into the size of this industry, who the main customers are, and what kind of systems are worth protecting. This leads us to our second point of departure for future research, which is to conduct experiments with diversifying various interfaces across various devices and to measure the effectiveness of these techniques against cyber-attacks. This research would allow us to gain a better understanding of what types of systems, as well as components of systems, are worth protecting via diversification. Third and finally, we propose that in the future researchers will carry out comparison analyses between obfuscation and other cybersecurity measures. Such an approach would allow the academic community as well as practitioners to understand how feasible and effective these solutions are in real world environments. These future research directions along with descriptions of them are displayed in [Table 5](#).

As with all studies our research has limitations, two of which, in particular, require further elaboration. First, we only focused on the scientific literature, but previous work has advocated for the importance of also including gray literature (Mahood et al., 2014). This limitation can be seen as intrinsic to bibliometric studies and those applying co-word analysis since gray literature sources often lack keywords and other bibliometric information that would be required to objectively compare the gray literature sources to academic studies. Second, the broader bibliometric search may have contained some false positives, which we sought to mitigate by only including domain-specific and precise keywords. Overall we estimate that the literature reviews in this study provide valuable insights into the literature profile despite these minor limitations. However, we encourage future research to look at the gray literature on the topic to compare and contrast our observations.

6. **Conclusions**

The trend of connecting various devices and sensors to the internet continues to this day, and as a consequence, we are seeing more and more cyber-physical systems and IoT devices in our daily lives. While these developments offer enormous benefits with regard to automation and optimization, there are cybersecurity concerns. The constantly shifting and changing nature of the cybercrime landscape requires multilayered proactive measures. In this study, we reviewed the literature on obfuscation and diversification techniques for IoT security. We extracted the various targets of obfuscation within the research field

of IoT cybersecurity and examined how obfuscation and diversification relate to the entire multilayered cybersecurity environment of IoT devices. In summary, by building multilayered defense mechanisms for cyber-physical systems, we ensure that even if some defenses fall, the entire system is not compromised. As a proactive invisible solution that consumes no to little energy, we encourage practitioners to look further into obfuscation and diversification approaches for improving IoT cybersecurity.

Data availability statement. All data used in the current study is made available in the study itself, with the exception of the metadata for VOSviewer. This metadata can be obtained from Scopus by using the search terms listed in Section 3. It is also available upon request.

Author contribution. S.R. and S.L. designed the study, abstracted the data, and wrote the first draft, and approved the final version of the manuscript.

Competing interest. None.

Funding statement. This research is not supported by any specific grant.

Ethical standard. The research meets all ethical guidelines, including adherence to the legal requirements of the study country.

References

- Abdullahi M, Baashar Y, Alhussian H, Alwadain A, Aziz N, Capretz LF and Abdulkadir SJ (2022) Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. *Electronics* 11(2), 198.
- Abendroth B, Kleiner A and Nicholas P (2017) Cybersecurity Policy for the Internet of Things. Available at <https://www.microsoft.com/en-us/cybersecurity/content-hub/cybersecurity-policy-for-iot> (accessed 20 December 2023).
- AlHogail A and AlShahrani M (2019) Building consumer trust to improve internet of things (IoT) technology adoption. In *Advances in Neuroergonomics and Cognitive Engineering: Proceedings of the AHFE 2018 International Conference on Neuroergonomics and Cognitive Engineering, July 21–25, 2018, Loews Sapphire Falls Resort at Universal Studios, Orlando, FL 9*. Springer, pp. 325–334.
- Alrubayyi H, Goteng G, Jaber M and Kelly J (2021) Challenges of malware detection in the iot and a review of artificial immune system approaches. *Journal of Sensor and Actuator Networks* 10(4), 61.
- Aslan ÖA and Samet R (2020) A comprehensive review on malware detection approaches. *IEEE Access* 8, 6249–6271.
- Bellman C and van Oorschot PC (2019) Analysis, implications, and challenges of an evolving consumer iot security landscape. In *2019 17th International Conference on Privacy, Security and Trust (PST)*. IEEE, pp. 1–7.
- Bhatia JS, Sehgal R, Bhushan B and Kaur H (2008) Multi layer cyber attack detection through honeynet. In *2008 New Technologies, Mobility and Security*. IEEE, pp. 1–5.
- Bin-Yahya M and Shen X (2022) Secure and energy-efficient network topology obfuscation for software-defined WSNS. *IEEE Internet of Things Journal*. 10(3), 2031–2045.
- Bin-Yahya M and Shen XS (2021) SRRM: Ranking-based route mutation scheme for software-defined wsns. In *2021 IEEE Global Communications Conference (GLOBECOM)*. IEEE, pp. 01–06.
- Butun I, Österberg P and Gidlund M (2019) Preserving location privacy in cyber-physical systems. In *2019 IEEE Conference on Communications and Network Security (CNS)*. IEEE, pp. 1–6.
- Cho J-H, Sharma DP, Alavizadeh H, Yoon S, Ben-Asher N, Moore TJ, Kim DS, Lim H and Nelson FF (2020) Toward proactive, adaptive defense: A survey on moving target defense. *IEEE Communications Surveys & Tutorials* 22(1), 709–745.
- Cohen FB (1993) Operating system protection through program evolution. *Computers & Security*, 12(6), 565–584.
- Collberg C (2018) Code obfuscation: Why is this still a thing? In *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*, pp. 173–174.
- Collberg C, Thomborson C and Low D (1997) A taxonomy of obfuscating transformations. Technical Report #148. University of Auckland, Department of Computer Science.
- Collberg CS and Thomborson C (2002) Watermarking, tamper-proofing, and obfuscation-tools for software protection. *IEEE Transactions on Software Engineering* 28(8), 735–746.
- Corallo A, Lazoi M, Lezzi M and Luperto A (2022) Cybersecurity awareness in the context of the industrial internet of things: A systematic literature review. *Computers in Industry* 137, 103614.
- Datta T, Apthorpe N and Feamster N (2018) A developer-friendly library for smart home iot privacy-preserving traffic obfuscation. In *Proceedings of the 2018 Workshop on IoT Security and Privacy*, pp. 43–48.
- de Haro-Olmo FJ, Varela-Vaca AJ and Álvarez-Bermejo JA (2020) Blockchain from the perspective of privacy and anonymisation: A systematic literature review. *Sensors* 20(24), 7171.
- Dib M, Torabi S, Bou-Harb E and Assi C (2021) A multi-dimensional deep learning framework for IoT malware classification and family attribution. *IEEE Transactions on Network and Service Management* 18(2), 1165–1177.

- Dissanayake N, Jayatilaka A, Zahedi M and Babar MA** (2022) Software security patch management—a systematic literature review of challenges, approaches, tools and practices. *Information and Software Technology* 144, 106771.
- El-Hajj M, Fadlallah A, Chamoun M and Serhrouchni A** (2019) A survey of internet of things (IoT) authentication schemes. *Sensors* 19(5), 1141.
- ENISA** (2019) Good Practices for Security of IoT. <https://www.enisa.europa.eu/publications/goodpractices-for-security-of-iot-1> (accessed 20 April 2020).
- Ge M, Cho J-H, Kim D, Dixit G and Chen I-R** (2021) Proactive defense for internet-of-things: Moving target defense with cyberdeception. *ACM Transactions on Internet Technology (TOIT)*, 22(1), 1–31.
- Hahm O, Baccelli E, Petersen H and Tsiftes N** (2015) Operating systems for low-end devices in the internet of things: A survey. *IEEE Internet of Things Journal* 3(5), 720–734.
- He G, Si Y, Xiao X, Wei Q, Zhu H and Xu B** (2021) Preventing IoT DDOS attacks using blockchain and IP address obfuscation. In *2021 13th International Conference on Wireless Communications and Signal Processing (WCSP)*. IEEE, pp. 1–5.
- Hetzler C, Chen Z and Khan TM** (2023) Analysis of SSH honeypot effectiveness. In *Advances in Information and Communication: Proceedings of the 2023 Future of Information and Communication Conference (FICC), Volume 2*. Springer, pp. 759–782.
- Hosseinzadeh S, Hyrynsalmi S and Leppänen V** (2016) Obfuscation and diversification for securing the internet of things (IoT). In *Internet of Things*. Elsevier, pp. 259–274.
- Hosseinzadeh S, Rauti S, Laurén S, Mäkelä J-M, Holvitie J, Hyrynsalmi S and Leppänen V** (2018) Diversification and obfuscation techniques for software security: A systematic literature review. *Information and Software Technology* 104, 72–93.
- Kaur B, Dadkhah S, Shoeleh F, Neto ECP, Xiong P, Iqbal S, Lamontagne P, Ray S and Ghorbani AA** (2023) Internet of things (IoT) security dataset evolution: Challenges and future directions. *Internet of Things* 100780.
- Khan KM, Shaheen M and Wang Y** (2017) Data confidentiality in cloud-based pervasive system. In *Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing*, pp. 1–6.
- Khraisat A, Gondal I, Vamplew P and Kamruzzaman J** (2019) Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity* 2(1), 1–22.
- Koivunen L, Rauti S and Leppänen V** (2016) Applying internal interface diversification to IoT operating systems. In *2016 International Conference on Software Security and Assurance (ICSSA)*. IEEE, pp. 1–5.
- Kolias C, Kambourakis G, Stavrou A and Voas J** (2017) Ddos in the IoT: Mirai and other botnets. *Computer* 50(7), 80–84.
- Kumar S, Tiwari P and Zymbler M** (2019) Internet of things is a revolutionary approach for future technology enhancement: A review. *Journal of Big Data* 6(1), 1–21.
- Kuzlu M, Fair C and Guler O** (2021) Role of artificial intelligence in the internet of things (IoT) cybersecurity. *Discover Internet of Things* 1(1), 1–14.
- Laato S, Farooq A, Vilppu H, Airola A and Murtonen M** (2022) Higher education during lockdown: Literature review and implications on technology design. *Education Research International*, 13, 7201043. <https://doi.org/10.1155/2022/7201043>
- Lee I** (2020) Internet of things (iot) cybersecurity: Literature review and iot cyber risk management. *Future Internet* 12(9), 157.
- Lei C, Zhang H-Q, Tan J-L, Zhang Y-C and Liu X-H** (2018) Moving target defense techniques: A survey. *Security and Communication Networks* 2018.
- Li S, Tryfonas T and Li H** (2016) *The Internet of Things: A Security Point of View*. Internet Research.
- Li S, Xu LD and Zhao S** (2015) The internet of things: A survey. *Information Systems Frontiers* 17(2), 243–259.
- Li X, Liu S, Wu F, Kumari S and Rodrigues JJ** (2018) Privacy preserving data aggregation scheme for mobile edge computing assisted iot applications. *IEEE Internet of Things Journal* 6(3), 4755–4763.
- Lu Y and Da Xu L** (2018) Internet of things (iot) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal* 6(2), 2103–2115.
- Mahood Q, Van Eerd D and Irvin E** (2014) Searching for grey literature for systematic reviews: Challenges and benefits. *Research Synthesis Methods* 5(3), 221–234.
- Mäki P, Rauti S, Hosseinzadeh S, Koivunen L and Leppänen V** (2016) Interface diversification in IoT operating systems. In *Proceedings of the 9th International Conference on Utility and Cloud Computing*, pp. 304–309.
- Malanski PD, Dedieu B and Schiavi S** (2021) Mapping the research domains on work in agriculture. a bibliometric review from Scopus database. *Journal of Rural Studies* 81, 305–314.
- Mercado-Velázquez AA, Escamilla-Ambrosio PJ and Ortiz-Rodríguez F** (2021) A moving target defense strategy for internet of things cybersecurity. *IEEE Access* 9, 118406–118418.
- Mhaskar N, Alabbad M and Khedri R** (2021) A formal approach to network segmentation. *Computers & Security* 103, 102162.
- Nausheen F and Begum SH** (2018) Healthcare IoT: Benefits, vulnerabilities and solutions. In *2018 2nd International Conference on Inventive Systems and Control (ICISC)*. IEEE, pp. 517–522.
- Navas RE, Cuppens F, Cuppens NB, Toutain L and Papadopoulos GZ** (2020) MTD, where art thou? a systematic review of moving target defense techniques for iot. *IEEE Internet of Things Journal* 8(10), 7818–7832.
- Nord JH, Koohang A and Paliszkiwicz J** (2019) The internet of things: Review and theoretical framework. *Expert Systems with Applications* 133, 97–108.
- Panahi P, Bayılmış Ç, Çavuşoğlu U and Kaçar S** (2021) Performance evaluation of lightweight encryption algorithms for IoT-based applications. *Arabian Journal for Science and Engineering* 46, 4015–4037.

- Pastrana S, Tapiador J, Suarez-Tangil G and Peris-López P** (2016) Avrand: A software-based defense against code reuse attacks for AVR embedded devices. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, pp. 58–77.
- Portokalidis G and Keromytis AD** (2011) Global ISR: toward a comprehensive defense against unauthorized code execution. In *Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats*. Springer, pp. 49–76.
- Rajesh S, Paul V, Menon VG and Khosravi MR** (2019) A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices. *Symmetry* 11(2), 293.
- Rauti S, Laato S and Pitkämäki T** (2020) Man-in-the-browser attacks against IoT devices: A study of smart homes. In *International Conference on Soft Computing and Pattern Recognition*. Springer, pp. 727–737.
- Rauti S, Laurén S, Mäki P, Uitto J, Laato S and Leppänen V** (2021) Internal interface diversification as a method against malware. *Journal of Cyber Security Technology* 5(1), 15–40.
- Rauti S and Leppänen V** (2017) A survey on fake entities as a method to detect and monitor malicious activity. In *2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)*. IEEE, pp. 386–390.
- Ravidas S, Lekidis A, Paci F and Zannone N** (2019) Access control in internet-of-things: A survey. *Journal of Network and Computer Applications* 144, 79–101.
- Remesh A, Muralidharan D, Raj N, Gopika J and Binu P** (2020) Intrusion detection system for IoT devices. In *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*. IEEE, pp. 826–830.
- Ross R, Pillitteri V, Graubart R, Bodeau D and McQuaid R** (2021) Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST SP 800–160 Vol. 2. Rev. 1.
- Statista** (2023) Prognosis of worldwide spending on the Internet of Things (IoT) from 2018 to 2023. Available at <https://www.statista.com/statistics/668996/worldwide-expenditures-for-the-internet-of-things/>
- Turner ME** (2019) *Internet of Things (IoT) Security in Consumer Devices*. East Carolina University.
- Upadhyay D, Zaman M, Joshi R and Sampalli S** (2021) An efficient key management and multi-layered security framework for scada systems. *IEEE Transactions on Network and Service Management* 19(1), 642–660.
- Van Eck N and Waltman L** (2010) Software survey: Vosviewer, a computer program for bibliometric mapping. *Scientometrics* 84(2), 523–538.
- Venkatraman S and Alzab M** (2017) Classification of malware using visualisation of similarity matrices. In *2017 Cybersecurity and Cyberforensics Conference (CCC)*. IEEE, pp. 3–8.
- Vignau B, Houry R and Hallé S** (2019) 10 years of IoT malware: A feature-based taxonomy. In *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*. IEEE, pp. 458–465.
- Weber RH** (2015) Internet of things: Privacy issues revisited. *Computer Law & Security Review* 31(5), 618–627.
- Xu D, Zheng M, Jiang L, Gu C, Tan R and Cheng P** (2020) Lightweight and unobtrusive data obfuscation at IoT edge for remote inference. *IEEE Internet of Things Journal* 7(10), 9540–9551.
- Xu X, He C, Xu Z, Qi L, Wan S and Bhuiyan MZA** (2019) Joint optimization of offloading utility and privacy for edge computing enabled IoT. *IEEE Internet of Things Journal* 7(4), 2622–2629.
- Yavari A, Panah AS, Georgakopoulos D, Jayaraman PP and van Schyndel R** (2017) Scalable role-based data disclosure control for the internet of things. In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, pp. 2226–2233.
- Zikria YB, Yu H, Afzal MK, Rehmani MH and Hahm O** (2018) Internet of things (IoT): Operating system, applications and protocols design, and validation techniques.