**ARTÍCULO ORIGINAL**
**INFORMÁTICA EMPRESARIAL**

# Literature review of small office-home office (SOHO) networks security from 2017-2022

## Revisión de literatura de seguridad de redes en oficinas pequeñas-oficinas caseras entre 2017-2022

Sajay Souchay Alzugaray[1,*] https://orcid.org/0000-0001-8744-4787
Yadary Ortega González[1] https://orcid.org/0000-0001-7706-4924
Jan Reyniers[2] https://orcid.org/0000-0002-7384-5237

[1]Technological University of Havana "José Antonio Echeverria" (CUJAE), Cuba
[2]Translator and editor-in-chief of the EPO publishing house

[*]Autor para la correspondencia: ssouchaya@ind.cujae.edu.cu

**ABSTRACT**
Infrastructure is the basic layer in Enterprise Architecture (EA) methodologies. The network components, their configuration and security are elements that require special attention from enterprise architects. According to actual conditions, most of networks can be identified as small or home/office networks. The increase in wireless devices has brought an increase in the amount of SOHO networks as well. The providers of infrastructure for this type of network don't pay attention to making their components safer while users face problems making their networks more secure. SOHO network security is a major concern to consider. This study applied a systematic mapping of the literature resulting in the discovery of a decrease in the publication productivity in this research field despite the high productivity of researchers in China, India and South Korea.
**Keywords:** enterprise architecture; small office home office network; literature review; security; vulnerabilities.

**RESUMEN**
La infraestructura es la capa básica de las metodologías de Arquitectura Empresarial (AE). Los componentes de red, su configuración y seguridad son elementos que requieren especial atención por parte de los arquitectos

empresariales. En la actualidad, la mayoría de las redes se identifican como pequeñas o domésticas. El aumento de dispositivos inalámbricos también ha impulsado el crecimiento de las redes SOHO. Los proveedores de infraestructura para este tipo de red no se preocupan por mejorar la seguridad de sus componentes, mientras que los usuarios enfrentan dificultades para aumentarla. La seguridad de las redes SOHO es una preocupación fundamental. Este estudio aplicó un mapeo sistemático de la literatura, lo que resultó en el descubrimiento de una disminución en la productividad de las publicaciones en este campo de investigación, a pesar de la alta productividad de los investigadores en China, India y Corea del Sur.

**Palabras clave:** arquitectura empresarial; red de oficina pequeña - oficina casera; revisión de literatura; seguridad; vulnerabilidades.

Recibido:18/03/25

Aprobado:08/05/25

# Introduction

Many tendencies in the world are currently stimulating the creation of home offices and small offices [1], especially the evolution and connection of devices. Entrepreneurship and the new businesses constitution are some of the most common. Another factor pushing this tendency was the COVID-19 pandemic [2]. During this pandemic, the entire world population was forced to stay home and change into a new remote work method based on the establishment of home offices or small offices at their homes. From the perspective of Enterprise Architecture (EA), this phenomenon demands attention since the analysis of the infrastructure layer with this methodology relays on its specific characteristics [3].

Small Office/Home Office Networks, known as SOHO, are the initials used to describe small local networks [4]. This term is strictly related to the information technology (IT) field. A traditional SOHO network is composed by "(…) computers, printers, networking devices as switches and routers as well as Network Attached Storages or other storage devices" [5]. More complex SOHO networks can include "(…) TVs on the Smart TV platform, digital video cameras, players and other microprocessor devices" [4].

SOHO networks, like many other networks, can be structured in two types of local area networks (LAN): wired (just known as LAN) or wireless (known as WLAN). In the specific case of WLAN connections, the amount of SOHO networks is a variable correlated to the amount of existing WLAN connections and the existing number of wireless technologies [6]. Therefore, due to the exponential increase of the number of wireless technologies humanity is experiencing as civilization, the percentage of SOHO networks is increasing as well [7].

Due to the number and variety of connected devices on the network [8], and their user-friendly focused design rather than security-based design these devices have become the source of serious security gaps for SOHO networks [5]. In addition, the type of equipment used for this kind of networks is very poorly protected [4] and "major manufacturers of network equipment for use in small corporate networks do not pay sufficient attention, as they are aiming at simplicity and cheapness of components to be able to target a larger audience [4]. Unfortunately, the security considerations in the current state for SOHO WLANs counterbalance the connectivity advantages, as default settings for wireless access points often provide no encryption or network protection [7]. Studies prove that the most serious security gaps on this type of network are related to wireless networks due to their nature
[5].

Users within SOHO environments may face legitimate difficulties that constrain their ability to deploy their technology appropriately [7]. SOHO networks are more vulnerable to network attacks and intrusions, because in most cases, effective intrusion detecting systems are too expensive for such kind of networks [9]. The impact of the deficiencies described can result, in the worst case, in the complete collapse of the network [5]. In the worst cases, it can result in violation of user's privacy and confidentiality [10, 11, 12].

In that sense, the aim of this study is to determine the contributions of the research results in the past years to the SOHO network security study field. To achieve this objective, the analysis has been carried out using the systematic mapping technique applied by Melendez et al. [13]. The next section of this article approaches the systematic mapping process application. Subsequently, the article describes the results obtained to give an answer to the research questions at issue.

# Methods

The study was carried out using the methodology of literature systematic mapping used by Melendez et al. [13] and proposed by [14]. In this section the authors will present elements like the research questions and the gathering of papers procedure, as well as the selection of paper criteria, the data extraction and classification parameters.

## Definition of the research question

To achieve the objective of the study, three research questions (RQ) were defined:

RQ 1: How did publications about SOHO networks evolve during the last years? This question is focused on determining how the behavior of publications related to SOHO networks security has varied over the last past years and what's the existing relationship among them. Furthermore, this question aims to analyze the bibliometric existing relationships between them and to look deeper into their nature to better understand the evolution on the knowledge associated with this research field.

RQ 2: Which are the main problems considered in literature affecting SOHO networks security? With this question the authors pretend to find out if there are some determined vulnerabilities for SOHO networks security mentioned in the selected scientific literature, and which is their nature.

RQ 3: What are the contributions of this publications to the SOHO network security as a knowledge field? The aim of this question is to identify existing solutions focused on solving SOHO networks security problems and vulnerabilities.

## Collection of studies

For the elaboration of the search strings used to recover the papers, the authors followed the PICO strategy (Population, Intervention, Comparison, Results) presented by Santos [15]. Only two elements of this strategy were considered to obtain a wider range of search results. The Population is related to the group of elements that will be subject to revision. The authors considered as population all elements that include the keywords "small office home office network" or simply "SOHO network".

By using the expected information, you want to retrieve during the search, as part of the search string, you get the Results component of the PICO strategy. In our

case it will be the elements related to network security. In this scenario the considered keywords were: ("security" AND "vulnerabilities" AND "intrusion").

The obtained search strings were: 1) ("small office home office network") AND ("security" OR "vulnerabilities" OR "intrusion" OR "cybersecurity") and 2) ("SOHO network") AND ("security" OR "vulnerabilities" OR "intrusion" OR "cybersecurity"). This search strings were executed in scientific online databases as: Scholar Google, IEEExplore and ScienceDirect.

## Selection of studies

The selection of the primary studies to take into consideration was executed during three different phases. The application of exclusion criteria (EC), through which the authors will be able to determine which studies will not be considered admissible for this research, constitutes the first phase. The second phase is to apply inclusion criteria (IC) that allow us to select the studies that can be relevant to consider, according to some of their characteristics or variables. Finally, the validation phase aims to corroborate the pertinence of the selected studies to answer the research questions previously stated through quality criteria (QC).

For the first phase, the applied EC are mentioned below:

- EC1: studies not published as scientific paper or conference paper.
- EC2: studies published before 2017.
- EC3: studies written in languages different than English or Spanish.
- EC4: duplicate studies.
- EC5: studies from which it is not possible to retrieve the article in digital format.
- EC6: studies of which the year of publication cannot be determined.

The IC applied to the retrieved set of studies was:

- IC1: studies of which titles and keywords are related to research questions are accepted.
- IC2: studies whose summaries, introduction or conclusions are related to the objective of the present study.

The third stage consisted of the validation of the primary studies to answer the research questions. The QC determined for applying during this research were:

- QC1: is the study related to the research questions?
- QC2: do the findings of the study contribute or help to answer the research questions?
- QC3: does the study contain a clear statement of the objectives of the research?
- QC4: are the objectives appropriately related to the title and keywords of the study?
- QC5: do the conclusions address the objectives of the research?

As presented in the applied method proposed by Melendez et al. [13] and following recommendations of other authors [16, 17] the authors assigned scores to every study during the quality evaluation phase. In case the study meets the evaluated criteria, its assigned value will be 1, 0.5 in cases where the study partially fulfills the criteria and 0 for studies that do not meet the criteria. For the selection of the studies, a lower limit score was settled in 4. The studies with a total score greater than 4 were, consequently, considered as primary studies for this research.

# Results

The execution of the search string returned 429 studies. In the execution of the first stage 44 studies were obtained, and in the second stage, 13 primary studies were achieved. During the third phase application, these studies were reaffirmed since they obtained scores greater than 4.

## Extraction, classification and initial results

For the extraction of information from the selected primary studies were analyzed using a systematic literature review matrix. The matrix summarizes relevant data from each study regarding the elements that it approaches. The field defined for the structuration of this matrix were: the authors names and year of publication, the type of study, type of publication and country of origin. This type of structured analysis facilitated the initial understanding of the primary selected studies.

The fields determination to constitute the systematic literature review matrix were strongly related to the needed analysis to answer the research questions. The authors names and year of publication allow to make an analysis related to the Annual productivity and Author productivity. Considering the type of study as a field gives you a preview about the type of community that is giving more interest to this subject. This type of publication allows to introduce cluster when analyzing

the evolution of this research area based on its publications. Finally, considering the origin country helps to locate the evolution within determined geographical areas.

# Discussion

This section presents the answer to the formulated RQ based on an analysis from the data extracted from the primary studies.

RQ 1: How have publications about SOHO networks security evolved during the last years?

During the realization of this investigation, a lot of information about SOHO networks was found. Despite that, when the subject specifically is its security, productivity is lower and especially during the last 5 years. This behavior is easily perceived when consulting Fig. ***1***. The unstable behavior of annual productivity in this research field is a concerning element to take into consideration. Furthermore, no co-citation or co-authorship networks were found between the primary studies.

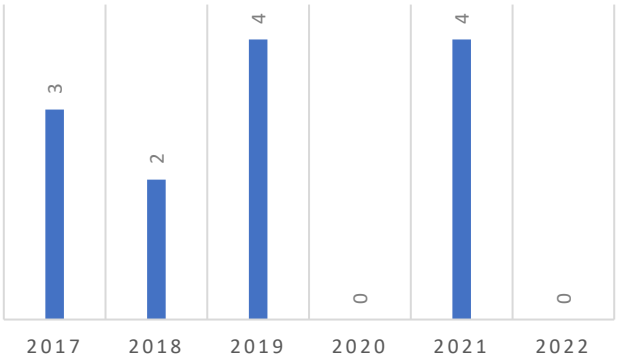


**Fig. 1 -** Annual productivity among primary studies.

Countries like India, China and South Korea had a significant role in the publications' evolution during the last years. These three countries have produced, only by themselves, almost half (46.15%) of the publications that can be found about this subject. Another observable behavior is that theoretical studies are in the period after 2019. As observable in Table 1***Fig. 1*** most of the studies are in the Eurasian region. In this region there is a considerable dissemination of studies. In the case of the publications type, the behavior is quite homogeneous, since 77% of them are journal articles focused on practice studies. As well can be perceived, in Table 1, most of the studies are oriented toward practical applications and to problem-solving in this research field. Regarding the authors, it is possible to

identify some of them with an important productivity in this field of knowledge, in short periods of time.

RQ 2: Which are the main problems considered in literature that affect SOHO networks security?

"Network security can be considered as the act of safeguarding multiple networks containing both open and remote communications, public services among trades, government institutions and other entities. Network security has expanded into a major element in any administrative structure" [18]. Also, Kandan et al. [18] identifies 10 types of attacks among which are:

1) malware attacks
2) identity spoofin
3) sniff attack
4) man in the middle attacks (MITM
5) ARP attacks
6) browser attacks
7) worm attacks
8) botnet
9) DNS spoofing attacks
10) back door attacks

On the other hand, Burlachenko et al. [19], contribute with:

11) MAC spoofing attacks
12) SSL strip

Perera et al. [20] shows some other types of attacks such as:

13) impersonation attacks
14) eavesdropping
15) system intrusions

Sahoo et al. [21] informs about another types of attack:

16) Distributed denial of service (DDoS) attack.

The problems with SOHO networks' security are the result of two combined factors: the existence of vulnerabilities and the attack target (2,9). Publications

focus on either element. In this sense, Kandan et al. [18] established network's security vulnerabilities can either be of hardware or software type. Vulnerabilities are mostly associated with the components of the network. Hardware vulnerabilities refer to smartphones, firewall, routers, switchers, IoT devices, among others. On the other hand, software vulnerabilities can be related to TCP/IP protocol flaws [20], firewall rules, routers vulnerable code [22] and code-execution vulnerability [23].

**Table 1 -** Main information on primary studies

| Authors (year) | Type of Study | Type of publication | Origin Country |
|---|---|---|---|
| A. Mani Kandan; G. Jaspher Willsie Kathrine & Alfred Raja Melvin (2019) | Theoretical | Journal article | India |
| Ivan Burlachenko; Iryna Zhuravska; Yevhen Davydenko; Volodymyr Savinov (2018) | Practical | Conference paper | Ukraine |
| M.A.D.S.R.Perera; C.U.Hemapala; D.M.R.Udugahapattuwa; A.N.Senarathne & A.A.S.R.Amarathunga (2019) | Practical | Conference paper | Sri Lanka |
| Hyung-Jong Kim & Soyeon Park (2017) | Practical | Conference paper | South Korea |
| Kshira Sagar Sahoo; Sanjaya Kumar Panda; Sampa Sahoo; Bibhudatta Sahoo & Ratnakar Dash (2019) | Practical | Journal article | Not specified |
| Imran; Faisal Jamil & Dohyeun Kim (2021) | Practical | Journal article | South Korea |
| Heba A. Hassan; Ezz E. Hemdan; Walid El-Shafai; Mona Shokair & Fathi E. Abd El-Samie (2021) | Theoretical | Journal article | Not specified |
| Ibbad Hafeez; Aaron Yi Ding; Markku Antikainen & Sasu Tarkoma (2018) | Practical | Journal article | Finland, Germany & Netherlands |
| Saurabh Malgaonkar; Rohan Patil; Aishwarya Rai & Aastha Singh (2017) | Practical | Journal article | India |
| Yu Zhang; Wei Huo; Kunpeng Jian; Ji Shi; Haoliang Lu; Longquan Liu; Chen Wang; Chao Zhang; Baoxu Liu & Dandan Sun (2019) | Practical | Journal article | China |
| Yu Zhang; Wei Huo; Kunpeng Jian; Ji Shi; LongquanLiu; YanyanZou; Chao Zhang & Baoxu Liu (2021) | Practical | Journal article | China |
| Nadav Rotenberg; Haya Shulman; Michael Waidner & Benjamin Zeltser (2017) | Practical | Journal article | Israel |
| Tohid Jafarian; Mohammad Masdar; Ali Ghaffari & Kambiz Majidzadeh (2021) | Theoretical | Journal article | Iran |

Source: Self-made

RQ 3: What are the contributions of this publications to the SOHO network security as a knowledge field?

Kandan et al. [18] proposes a list of measures for preventing attacks depending on the type of attack. For instance, "using strong encrypted communication, Virtual Private Network (VPN) and hypertext transfer protocol secure (HTTPS)" for MITM type of attacks. For the case of backdoor attacks, it is suggested to maintain the operating system and Antivirus software up to date because it can help to clear the payloads created during the attack. The main protection against these attacks is to have a strong firewall working on the network. On the other hand, updating the applications can help to protect you from the botnet attacks. Any unknown link in mail should be checked thoroughly before downloading it. As smartphones are easy objects for botnet attacks due to command and control, it is advised to check any package before application installation.

Burlachenko et al. [19] proposes a solution based on the application of the methodology of multi-agent system (MAS) network protection. With its application the time metrics of the software protection functions productivity against heterogeneously distributed deterministic attacks have increased the efficiency by 21%. This is due to the reduction of the time of recognition and localization of the incident. "Using the methodology of MAS network protection increases a network load by 11% on and does not exceed 63% at peaks". Perera et al. [20] propose a product called Dynamic Defender. This solution provides the user with a single device that provides a secure internet connection and secure web navigation experience. Comprised by four machine learning modules it brings a solution over the issue where SOHO type and small-scale businesses did not have internet security and internet quota management for their users. One of its more important modules is the intrusion detection based on anomalies.

Kim & Park [24] proposes a password management scheme named the SPT (Secure Password Translator) specially developed for SOHO environments. It focuses on lowering the vulnerabilities of the network by the protection of its documentation. This solution helps the companies to manage the strength of documents in a well-organized manner and in the case of incidents, it can separate the responsibilities. Moreover, it is a solution that can be applied to SOHO environments to manage documentation and passwords in a proper manner. Sahoo et al. [21] widely discusses DDos attacks and the various aspects of this kind of threat for SOHO networks. Their work represents an important theoretical contribution to this subject. They propose the emergent field of software-defined networking as solution to DDos attacks due to its efficiency to detect this specific type of threat. For this reason, they have proposed a detection scheme for

discovering DDoS attacks. Furthermore, they clarify a set of future research tasks that have a high research value.

Jamil et al. [25] express an intrusion detection system based on the ensemble of prediction and learning mechanisms to improve anomaly detection accuracy in a network intrusion environment. This article is a good expression of a visible tendency on integrating artificial intelligence and machine learning to seek more effective solutions on detecting and mitigate network attacks. During its application, the solution showed an intrusion detection accuracy over 98%. A favorable element of this research is its contribution to the structuration of training and testing models to enable machine learning.

The research of Sultana et al. [26] produces an extensive analysis of techniques and means employed up to date for intrusion detection. Their analysis goes from the traditional intrusion detection systems (based on anomaly detection and misuse detection) to the explanation on the use of machine learning for intrusion detection. Other techniques such as deep learning for network intrusion detection systems and software-defined networking (SDN)-based intrusion detection systems are approached. Moreover, they offer a look into the advantages of the use of Blockchain for the same purpose. Combinations like blockchain-based Internet of Things (IoT) or blockchain-based SDN and IoT architecture are described. As other articles mentioned before, this one provides a list of prominent open problems and future work directions for the research community.

Hafeez et al. [27] proposes a self-adaptive and semi-supervised learning-based classification scheme named IoTguard, which predicts traffic class (malicious or benign) based on the network activity of the device generating that traffic. It demonstrates that a simple, yet effective, clustering technique combined with in-depth feature analysis enables real-time traffic classification, without requiring dedicated hardware, in just 250 MS. “This paper introduces a threat model based on the most common attacks in IoT landscape and a real-world testbed setup for collecting network data and device level logs.”

By Malgaonkar et al. [28] the need for a new Wi-Fi security protocol arises. The security feature followed is encryption/decryption of the data that are being exchanged. To achieve that goal, the authors start making an interesting review of currently existing security methods like: WEP protocol, WPA, TKIP and 802.1x. Their objective was to understand the aspects within their algorithms to evaluate the protocols and help to make them more efficient. After they apply experimental design, they arrive at the conclusion that their solution can be used to assess a

register network configuration and the impact of variation of different parameters in it.

Zhang et al. [29] proposes a solution SRFuzzer to improve the effectiveness of SOHO routers by minimizing issues like the lack of input specification, lack of routers' internal running states, and lack of testing environment recovery mechanisms. The framework is fully automatic, and it is centered in multi-type vulnerabilities of SOHO routers. In comparison with similar products on the market, SRFuzzer outperformed those three comparative fuzzers in all types of vulnerabilities. Specifically, it found more memory corruption issues and more command injection issues than the rest.

Zhang et al. [22] shown a continuation of the priorly shown study. The authors implemented ESRFuzzer as a prototype tool by integrating the above improvements into SRFuzzer and deployed it in a realworld environment. Their objective is to build an automatic fuzzing framework for FWSR and to find as many vulnerabilities as possible. Improvement in this version of the solution is that it is based on the detection of the READ-op issue by improving the SRFuzzer with D-CONF mode fuzzing mechanism. Its performance was outstandingly good compared with the previous version of the same solution.

The purpose of Rotenberg et al. [23] was to bridge the existing gap between reality and the known defense strategies to prevent bypassing vulnerabilities over SOHO routers. They performed an evaluation of authentication bypass vulnerabilities. The results of this study show a large fraction of misconfigurations and insecurity issues in configuration of SOHO routers, which stand in sharp contrast to the awareness of the security and research communities to the vulnerabilities as well as a large body of work studying related topics.

Jafarian et al. [30] explain, categorize, and compare the state-of-the-art schemes applied in detecting and mitigating anomalies in SDNs. This paper categorizes the SDN anomaly detection mechanisms into five categories: (1) flow counting scheme, (2) information-based scheme, (3) entropy-based scheme, (4) deep learning, and (5) hybrid scheme. The research gaps and major existing research issues regarding SDN anomaly detection are highlighted. The review of the studies revealed that DoS attacks are considered as the most significant external threats in SDNs. The review of the related studies indicates that different techniques and methods were used for collecting statistical data, which is a need for the anomaly detection algorithm.

# Conclusions

The main objective of this study was to determine the contributions that researchers have made on the SOHO network security field. In RQ1, it has been possible to identify behavioral patterns in the productivity of the publication. The productivity around this subject tends to increase but with an unstable behavior, especially in the last 5 years. Also, publications are in the Eurasian region of the world with China, India, and South Korea as the most productive countries on the subject. From RQ2 it was possible to determine the classification for SOHO network security problems into attacks and vulnerabilities. The authors also discover sources of software and hardware clusters vulnerabilities. Furthermore, a list of sixteen types of attacks that affect SOHO networks was synthetized. By answering RQ3 it was easy to grasp the conclusion that 77% of the studies are more focused on practical implementation than on theoretical study.

# References

1. Zhang Y, Huo W, Jian K, Shi J, Liu L, Zou Y, et al. ESRFuzzer: an enhanced fuzzing framework for physical SOHO router devices to discover multi-Type vulnerabilities. Cybersecurity. 2021 Dec 1;4(1).

2. Siem E. Intrustion Detection in Soho Networks Using Elasticsearch Siem. 2021 [cited 2022 Oct 13]; Available from: https://search.proquest.com/openview/1418d1c0b1a6c27a5f429739a0771312/1?pqorigsite=gscholar&cbl=18750&diss=y

3. Höpfner R, … BRBP& DUP, 2022 undefined. Demonstration of the Impact of Enterprise Architecture Management in a Company by Using Frameworks. opus4.kobv.de [Internet]. 2022 [cited 2022 Oct 26]; Available from: https://opus4.kobv.de/opus4-fhws/files/2009/SMEs_and_International_Business.pdf#page=113

4. Basinya E, Rudkovskiy A. Automatic traffic control system for soho computer networks. Studies in Systems, Decision and Control. 2019;199:743–54.

5. Kavalaris S, … ESJ of CS and D, 2015 undefined. Multimedia implementations for soho networks and their security issues: Opening pandora's box with sonos and sonosnet. researchgate.net [Internet]. 2015 [cited 2022 Oct 13]; Available from: https://www.researchgate.net/profile/Stylianos-Kavalaris/publication/282391898_Multimedia_Implementations_for_SOHO_Networks_and_Their_Security_Issues_Opening_Pandora's_Box_with_Sonos_and_SonosNet/links/562

38fc108aed8dd1948ba16/ Multimedia-Implementations-for-SOHO-Networks-and-Their-Security-Issues-Opening-Pandoras-Boxwith-Sonos-and-SonosNet.pdf

6. Panigrahi GR, Barpanda DNK, Panda M. A Virtual & Pragmatic Analysis on Networked Security Incident, its Handling & Reporting Measures. In: 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA) [Internet]. IEEE; 2020 [cited 2022 Oct 15]. Available from: https://ieeexplore.ieee.org/document/9132951/

7. Ghita B V, Furnell SM. Assessing the usability of WLAN security for SOHO users. 2006 [cited 2022 Oct 13]; Available from: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.717.4637&rep=rep1&type=pdf

8. Lara A, Mayor V, Estepa R, Estepa A, Díaz-Verdejo JE. Smart home anomaly-based IDS: Architecture proposal and case study. Internet of Things. 2023 Jul 1;22:100773.

9. Burmaka I, Dorosh M, Skiter I, Lytvyn S. Architecture of Distributed Blockchain Based Intrusion Detecting System for SOHO Networks. Lecture Notes in Networks and Systems. 2022;344:313–26.

10. Zheng T, Liu M, Puthal D, Yi P, Wu Y, arXiv XH arXiv preprint, et al. Smart Grid: Cyber Attacks, Critical Defense Approaches, and Digital Twin. arxiv.org [Internet]. 2022 [cited 2022 Oct 15]; Available from: https://arxiv.org/abs/2205.11783

11. Marcos da Silva L, Bonini de Britto Menezes H, dos Santos Luccas M, Mailer C, Sandro Roschildt Pinto A, Boava A, et al. Development of an Efficiency Platform Based on MQTT for UAV Controlling and DoS Attack Detection. mdpi.com [Internet]. 2022 [cited 2022 Oct 15]; Available from: https://www.mdpi.com/1424-8220/22/17/6567

12. Smiliotopoulos C, Barmpatsalou K, Sciences GKA, 2022 undefined. Revisiting the Detection of Lateral Movement through Sysmon. mdpi.com [Internet]. 2022 [cited 2022 Oct 15]; Available from: https://www.mdpi.com/2076-3417/12/15/7746

13. Melendez K, Dávila A, Melgar A, Melendez K, Dávila A, Melgar A. Literature Review of the
Measurement in the Innovation Management. Journal of technology management & innovation [Internet]. 2019 [cited 2025 Apr

4];14(2):81–7. Available from: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-27242019000200081&lng=es&nrm=iso&tlng=en

14. Petersen K, Feldt R, Mujtaba S, Mattsson M. Systematic mapping studies in software engineering. 12th International Conference on Evaluation and Assessment in Software Engineering, EASE 2008. 2008;

15. Santos C, CAM Pimenta - Revista latino-americana. The PICO strategy for the research question construction and evidence search. SciELO Brasil [Internet]. 2007 [cited 2022 Oct 14]; Available from: https://www.scielo.br/j/rlae/a/CfKNnz8mvSqVjZ37Z77pFsy

16. Sulayman M, … EM on ASE and I, 2009 undefined. A systematic literature review of software process improvement in small and medium web companies. Springer [Internet]. 2009 [cited 2022 Oct 15];59 CCIS:1–8. Available from: https://link.springer.com/chapter/10.1007/978-3-642-10619-4_1

17. Kitchenham B, … EMIT on, 2007 undefined. Cross versus within-company cost estimation studies: A systematic review. ieeexplore.ieee.org [Internet]. 2007 [cited 2022 Oct 15]; Available from: https://ieeexplore.ieee.org/abstract/document/4160970/

18. Kandan AM, Kathrine GJ, Melvin AR. Network Attacks and Prevention techniques - A Study. In: 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT) [Internet]. IEEE; 2019 [cited 2022 Oct 15]. Available from: https://ieeexplore.ieee.org/document/8869077/

19. Burlachenko I, Zhuravska I, Davydenko Y, Savinov V. Vulnerabilities Analysis and Defense Based on MAS Method in Fast Dynamic Wireless Networks. In: 2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS) [Internet]. IEEE; 2018 [cited 2022 Oct 15]. Available from: https://ieeexplore.ieee.org/document/8525692/

20. Perera MADSR, Hemapala CU, Udugahapattuwa DMR, Senarathne AN, Amarathunga AASR. Secure
Web Navigation with Intrusion Detection And Quota Management for SOHO and Small Scale
Businesses. In: 2019 International Conference on Advancements in Computing (ICAC) [Internet]. IEEE;

2019 [cited 2022 Oct 15]. Available from: https://ieeexplore.ieee.org/document/9103418/

21. Sahoo KS, Panda SK, Sahoo S, Sahoo B, Dash R. Toward secure software-defined networks against distributed denial of service attack. Journal of Supercomputing. 2019 Aug 1;75(8):4829–74.

22. Zhang Y, Huo W, Jian K, Shi J, Liu L, Zou Y, et al. ESRFuzzer: an enhanced fuzzing framework for physical SOHO router devices to discover multi-Type vulnerabilities. Cybersecurity. 2021 Dec 1;4(1).

23. Rotenberg N, Shulman H, … MWP of the, 2017 undefined. Authentication-bypass vulnerabilities in SOHO routers. dl.acm.org [Internet]. 2017 Aug 22 [cited 2022 Oct 13];3:68–70. Available from: https://dl.acm.org/doi/abs/10.1145/3123878.3131989

24. Kim HJ, Park S. Secure Password Translation for Document Protection of SOHO Companies. In: 2017 International Conference on Software Security and Assurance (ICSSA) [Internet]. IEEE; 2017 [cited 2022 Oct 15]. Available from: https://ieeexplore.ieee.org/document/8392620/

25. Jamil F, Sustainability DK, 2021 undefined. An ensemble of prediction and learning mechanism for improving accuracy of anomaly detection in network intrusion environments. mdpi.com [Internet].
2021 [cited 2022 Oct 15]; Available from: https://www.mdpi.com/1262832

26. Sultana N, Chilamkurti N, Peng W, Alhadad R. Survey on SDN based network intrusion detection system using machine learning approaches. Peer Peer Netw Appl. 2019 Mar 1;12(2):493–501.

27. Hafeez I, Ding A, Antikainen M, arXiv ST arXiv preprint, 2017 undefined. Toward secure edge networks taming device to device (D2D) communication in IoT. arxiv.org [Internet]. 2018 [cited 2022 Oct 15]; Available from: https://arxiv.org/abs/1712.05958

28. Malgaonkar S, Patil R, … ARIJ of, 2017 undefined. Research on Wi-Fi Security Protocols.
researchgate.net [Internet]. 2017 [cited 2022 Oct 15];164(3):975–8887. Available from:
https://www.researchgate.net/profile/SaurabhMalgaonkar/publication/316177604_Research_on_Wi-Fi_Security_Protocols/links/5a42b86ca6fdcce19715b80b/Research-on-Wi-Fi-Security-Protocols.pdf

29. Zhang Y, Huo W, Jian K, Shi J, Lu H, Liu L, et al. SRFuzzer: an automatic fuzzing framework for physical SOHO router devices to discover multi-type vulnerabilities. dl.acm.org [Internet]. 2019 Dec 9 [cited 2022 Oct 15];544–56. Available from: https://dl.acm.org/doi/abs/10.1145/3359789.3359826?casa_token=Tg2AQuU76z0AAAAA:d5YlzCOn7K93R5SJdrH6Z4_rtj-rKEaP7Fw4-e35ytkc0isvBH0Z_ftH6CyvqJ4hWM4m0APSaH_E

30. Jafarian T, Masdari M, Ghaffari A, Majidzadeh K. A survey and classification of the security anomaly detection mechanisms in software defined networks. Cluster Comput. 2021 Jun 1;24(2):1235–53.

## Conflict of interests

The authors declare there is no conflict of interests.

## Author's contributions

**Sajay Souchay Alzugaray:** Article conception. Identification of the systematic literature review procedure to be performed. Execution of the systematic literature review procedure. Retrieval and processing of bibliographic references. Reading and analysis of the selected collection of documents based on the study's inclusion and exclusion criteria. Writing the research results. Preparation of graphs and tables. Editorial review.

**Yadary Cecilia Ortega González:** Article conception. Methodological guide for identifying the systematic literature review procedure to be conducted. Reading and analysis of the selected literature collection based on the study's inclusion and exclusion criteria. Editorial review. Review of the study's methodological rigor.

**Jan Reyniers:** Article conception. Reading of the selected collection of documents based on the study's inclusion and exclusion criteria. Editorial review. Translation of the manuscript containing research results.

## Authors' details

Sajay Souchay is a young researcher. PhD student at the Technological University of Havana "José Antonio Echeverría". She is a member of the Business Informatics scientific research group at the Industrial engineering faculty. She teaches undergraduate courses such as Organizational modeling, Informatic solutions development and Innovation with Information Technology. She is the head of the

Business Informatics department at the Industrial Engineering faculty. Her research interests include business process modelling, modelling notations, enterprise resource planning systems, enterprise architecture management and innovation management.

Yadary Ortega is a senior researcher at the Business Informatics scientific research group at the Industrial engineering faculty of the Technological University of Havana "José Antonio Echeverría". She has been the head of that scientific research group for more than 10 years. She has a PhD in technical sciences. She teaches undergraduate courses such as Organizational modeling, Innovation with Information Technology and Information Systems. She also teaches postgraduate courses such as Ontology Management, Innovation management, and Enterprise architecture management. Her research interests include semantic modeling, enterprise architecture management and Information Systems. She is a member of the Scientific Council of the Industrial engineering faculty.

Jan Reyniers is an experienced writer, editor and translator of the EPO publishing house. His experience spans over 40 years. Her translation and editing work include more than 50 texts in English, French, and Dutch. He is also a tireless researcher of cultural, political, and social issues. He is also passionate about writing plays.