TRILHA PRINCIPAL

Trends, Opportunities, and Challenges in Using Restricted Device Authentication in Fog Computing

Wesley dos Reis Bezerra, *PhD Candidate, PPGCC/UFSC*,
Carlos Becker Westphall, *Prof. Dr. PPGCC/UFSC*,

Abstract—The few resources available on constrained devices in Internet of Things are an important issue when we think about security. In this perspective, our work proposes an agile systematic review literature on works involving the Internet of Things, authentication, and Fog Computing. As a result, related works, opportunities, and challenges found at the intersection of those areas were brought, supporting other researchers and developers who work in those areas.

Index Terms—internet of things, authentication, constrained devices, fog computing

I. Introduction

Security is a challenge in several areas of computing, especially for the Internet of Things (IoT)[1]. Specifically, when it has few resources[2]–[4], such as the battery, processing, storage, and throughput, security concerns may be relegated to the role of a minor and unimportant nuisance.. Thus, devices that have fewer resources tend to implement weaker security.

However, even with few resources, it is important to properly implement security in IoT[5] systems − in our case the implementation of device authentication. For that, it is necessary to know this specific area's trends, challenges, and opportunities. There was a lack of a preliminary study with the desired focus.

As a solution, this work aims to bring documentary resources that represent possible future developments in the area but also exposes problems that researchers/developers must avoid. This material was obtained from an agile systematic literature review (SLR) to answer the following questions.

- what are the opportunities for IoT authentication in Fog Computing?
- what are the challenges for IoT authentication in Fog Computing?
- what are the main works related to the topic of IoT authentication at Fog Computing?

The work is organized as follows: in the second section, the materials and methods used were presented; then, in the third section, a agile systematic literature review was presented; in the next section, there is the quantitative analysis of the data obtained from the researched works; finally, the conclusion and future works were brought in the sixth section.

II. Materials and methods

This study utilized the customization of the ProKnow-C [6] and EBSE [7] systematic review method focusing on the state of the art opportunities in the researched area, Figure 1. The systematic review is a structural investigation which uses systematic procedures for searching, synthesis, and analysis [8] of the collected evidence. This methodology enabled the reduction of bias in surveying the bibliographic portfolio [9], obtaining quantitative data and a more focused, higher quality portfolio.

Significant tools contributed to greater quality and replication of the process. Mendeley[1], was used for managing the bibliographic portfolio, which allowed for the creation of folders to organize articles and store them while synchronized with the cloud. With respect to creating datasets, LibreOffice Calc [2] - was used to create the spreadsheets that documented the project and the datasets' generation in the CSV format to read later and create charts. Lastly, concerning the generation of charts, GNUPlot[3] - enabled the automation of charts in this work.

III. Systematic Review of Literature

The ACM Digital Library, IEEE Xplorer, Scopus, ScienceDirect, and Scielo portals were selected due to its expressiveness in the area of computing. All chosen portals allow access to many publications in journals and conferences. Moreover, such portals permit free access to many publications through partnerships between universities and CAPES[4].

Concerning the engineering process of query-string, four main areas were chosen. The selected areas were IoT, authentication, fog computing, and message protocols. The results can be seen in Table I, which offers an overview of the last three years of publications in each area. A three-year time window (2018-2020) was chosen due to the present study because we are only seeking new works and trends in the mentioned areas. For the initial exploration of the number of
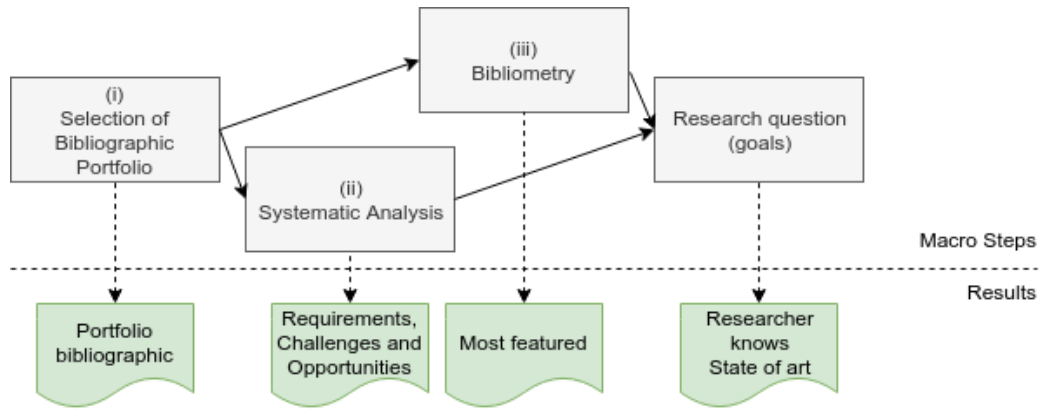
Fig. 1. ProKnow-C Macro Steps (adapted from [6]) - In gray are the macro-steps, and in green are the results of each process. It is important to note that the systematic analysis (ii) and bibliometric (iii) processes must occur in parallel.

Area	2018	2019	2020
IoT	83700	59300	31800
Authentication	42700	20400	21700
Fog Computing	16100	12100	4600
Message Protocol	3330	1820	520

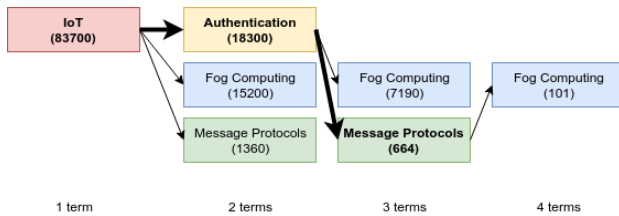publications obtained, the Google Scholar [5] tool was used, without the inclusion of patents and citations.

Fig. 2. Query Terms Tree - Results of the Analysis of the Related Publications – from the left, the search terms are combined. This combination is made with up to four terms in the rightmost column and follows the flow of each connection through the directional arrows. Also, the arrows and labels that describe the terms used together in this query are represented in bold.

During the analysis of areas, a query terms tree was created, as shown in Figure 2. In this tree, the paths taken to combine the areas forming the consultation questions can be seen. We highlighted (in boldface) the words used in the chosen query-string. It is evident that even having a consultation question with four terms, this did not present satisfactory results when submitted to the consultation portals. When submitted to such portals, it brought few or no results using all four terms. Correspondingly, we opted for the query-string of three terms: (IoT AND authentication AND "message protocols").

After submitting the query-string to the portals, it can be noticed that the portal with the highest number of results was the Digital Library ACM with eight publications, followed by Scopus with four publications. In the total sum of the results

[5]http://scholar.google.com

among all portals listed, 13 publications appeared in the last three years. This result of the portals is more restricted than the one presented in Figure 2 because the figure expresses the data searched in Google Scholar. This fact occurs because the latter, in its search, also evaluates occurrences of words in the text, while portals generally use titles, abstracts, and keywords.

Subsequently, publications that did not meet the established criteria were removed from the articles' initial list. The inclusion and exclusion criteria (Table II) are significant and directly influence the selected publications' quality [17]. It can be seen that the criteria has been divided into three inclusion factors and four exclusion factors. As the time window was used when consulting portals, it was unnecessary to include a criterion referencing maximum time for evaluated publications.

Inclusion	
I01	Complete articles from conference or periodicals;
I02	English only language articles;
I03	Full-text access available.
Exclusion	
E01	Research patents and reports;
E02	Non-scientific publication;
E03	For 2018 and 2019 publications, less than five citations;
E04	Duplicate publications.

After defining the criteria, there was the portfolio selection. The process began with 13 publications, two of which were eliminated because they were non-scientific publications, and two others were eliminated because they were duplicate publications. In the title reading phase, nine publications were analyzed, of which one publication was eliminated due to not being a title adhering to the scope of the research. In the reading phase of abstracts, two publications were eliminated, leaving only six publications in the list of articles. In the last phase, the complete reading phase, no publication was eliminated, leaving six final portfolio publications.

The final portfolio, describe in Table III, is composed of six publications. Even though this is not an expressive number,

the selected publications brought a large and diverse amount of information about the research topic. It is also observed that two of the six publications are from journals and bring a comprehensive view on the state-of-the-art and challenges related to the theme. The other publications contribute mainly to what types of solutions are being given to authentication with IoT message protocols.

A. Quantitative Data Analysis

In bibliometric analyses (BA), statistical metrics found on selected documents are expressed through a pictograph [24]. A more quantitative analysis of the research area is possible from the collected variables. Some expected results understand the main events and journals in the area, as well as the leading and most relevant authors, among other variables. It is of significant importance to know which publications are most influential by comparing the number of citations , which, even if in a limited way, describes the acceptance of the paper by the research community..

Three dimensions were chosen to be analyzed bibliometrically: publications, authors, and sources. The dimensions of the publications are shown in Figures 3-(a) and 3-(b) which show the evolution of the works published during the selected period and an analysis of citations per study. Regarding the authors' dimension, Figures 4-(a) and 4-(b), weigh the significance of the authors involved in the publications and suggest researchers to whose research should be monitored in order to remain up-to-date in the area. Lastly, the dimension of the data sources is visualized through Figures 5-(a) and 5-(b) enabling the reader to identify the main sources of research within the proposed analysis, their impact factors, and the quantity of publications. It can be concluded that the three dimensions permit the identification of the most relevant studies, the authors which should be followed and the sources to aim for in order to obtain publications.

This work brings a Bibliometric Analysis (BA) of the entire researched area and not just the portfolio list. This analysis was a project choice due to the reduced number of publications in the final portfolio. The authors considered that even if there was no complete adherence to all articles found, the articles still described the area of interest in the last three years, the time frame established at the time of consultation.

The variables collected from the documents allowed for inferences to be drawn from the publications. The following variables were collected: publications per year (1), highest h-index per publication (2), highest i10 per publication (3), publications per conference/journal, the journal impact factor (when available), h-index of each conference (when available) and citations per publication.

$$publicationYear_i = \sum \left(count(publication_i) \right) \quad (1)$$

$$majorHindex_i = Major \left(hindex(author_j, publication_i) \right) \quad (2)$$

$$majorI10_i = Major \left(i10(author_j, publication_i) \right) \quad (3)$$

As is evident in Figure 3-(a), the publications' distribution accumulated (1) more results in the first two years. The year 2020 had fewer results, partly because publications were ongoing. Additionally, some conferences delayed their achievements and resulted in the annals' publication.
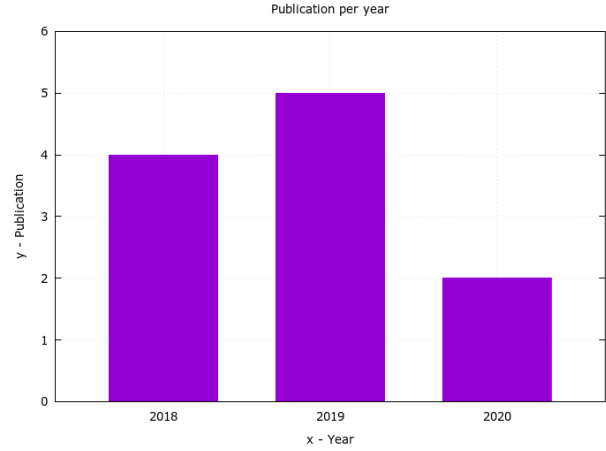
(a) Publications by year
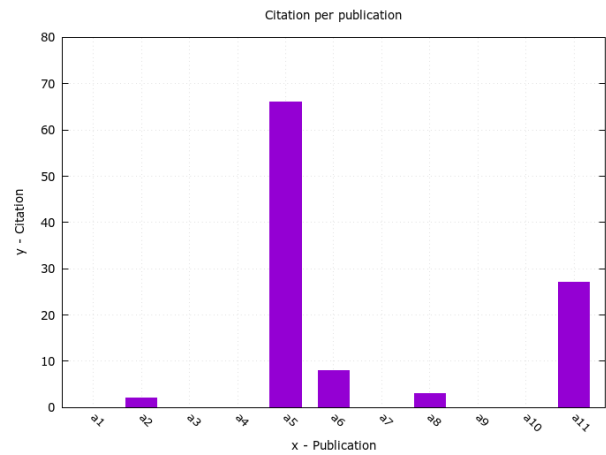
(b) Citations per publication

Fig. 3. Publication Data - bibliometric data on published studies. As can be seen above, ranging from 2018 to 2020, is the distribution of the number of publications per year. Below, the distribution of citations per publication throughout the study period

The number of citations is an essential factor for assessing the impact of a job on the academic community.The highest number of citations was awarded to paper a5 [25] with 66 citations, followed by a11 [23] with 27 citations. Notice that the most recent studies, although relevant, have not yet had the opportunity to generate citations or the citations generated have not been indexed yet.

Regarding the authors' quality assessment, two indexes were chosen, the h-index(2) and the i10(3). For the i10 index, Figure 4-(b), the highest value is associated with the researcher Wendy Hall (University of Southampton) of the publication a5 [25] with 225 points. As for the H index (h-index), Figure 4-(a), the same author leads with 60 points, followed by Jinjun Chen (Swinburne University of Technology) from a6 [21] with 56 points.

TABLE III
BIBLIOGRAPHIC PORTFOLIO - THE FIRST COLUMN CONTAINS AN INDEX OF THE PUBLICATION WITHIN THE DATABASE USED TO SUPPORT THE
SYSTEMATIC REVIEW AND THE REFERENCE; THE SECOND COLUMN CONTAINS THE TITLE OF THE EVALUATED PUBLICATION

| #	Document	Publication
a1	[18]	A Blockchain-Based OTP-Authentication Scheme for Constrained IoT Devices Using MQTT
a3	[19]	A Blockchain-Based Protocol for Message Exchange in a ICS Network: Student Research Abstract
a4	[20]	Security for Internet of Things: A State of the Art on Existing Protocols and Open Research Issues
a6	[21]	A Survey on Representation Learning Efforts in Cybersecurity Domain
a9	[22]	Implementation and Evaluation of Lightweight Ciphers in MQTT Environment
a11	[23]	Architectural design of token based authentication of MQTT protocol in constrained IoT device
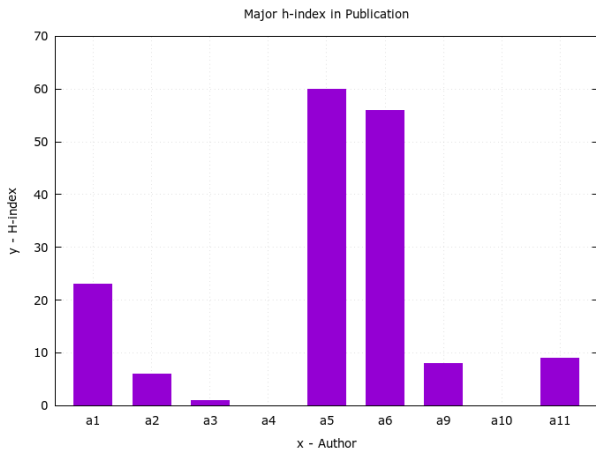
(a) h-index
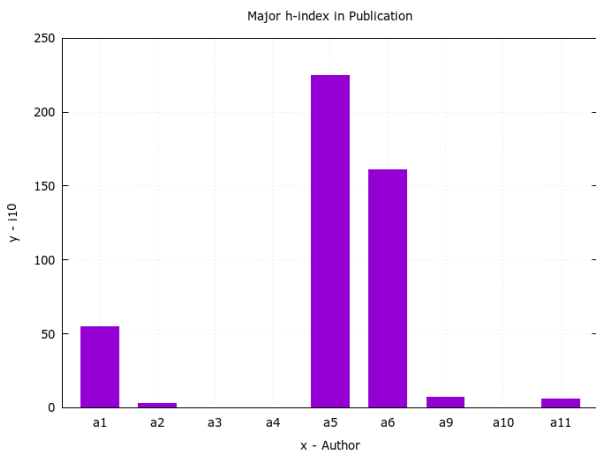
(b) i10

Fig. 4. Highest Indexes among the Authors of Each Publication - in these bibliometric graphs, an analysis of the authors participating in the portfolio is described. In these graphs, the authors are associated with their publications and share the same index as their publications. Above, there is a description of the largest h-index of the publication author. Below, is listed the highest i10 of the author of each publication

Publications were found in 11 different publishing vehicles, as shown in Figure 5-(a). Out of the publications found, only two were journals, being the other conferences. It is quite noticeable that even with only two journals in the list of publications, the publications brought forth important material for discussion (a5, a6, and a10).

The journal with the most significant impact factor is ACM Computer Surveys, Figure 5-(b), with an Impact Factor (IF)

of 6.131. From this journal, two articles were analyzed (a5 and a6). Such a journal is renowned for bringing quality and extensive content on several computing areas, serving as a reliable source in the search for evidence to support projects and research choices in the area. This result reinforced the statements previously made.
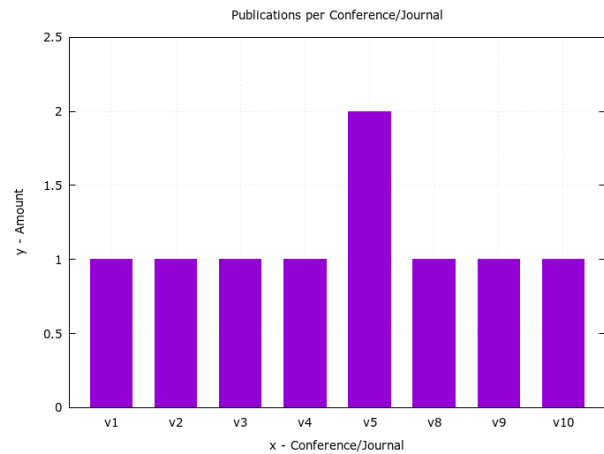
(a) Publications by Conference/Journal
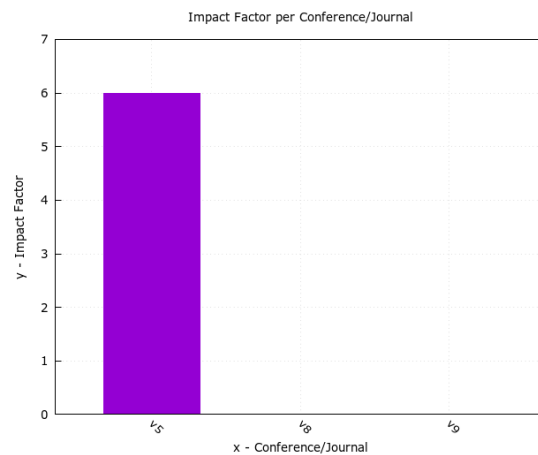
(b) Journal Impact Factor

Fig. 5. Conferences and Journal Data - These graphs represent a description of the sources utilized in this systematic review. on the graphic above, is a description of the number of publications per source. Presented on the below, is a description of the impact factors of the journals which are part of the research

It can be seen through bibliometrics that the theme has grown in many publications over recent years. It is also possible to note relevant researchers' publications in the area.

Such researchers have published in relevant journals and conferences.

IV. DISCUSSION AND RESULTS

For thematic review, the challenge lens and the opportunity lens were chosen. The challenge lens aims to list the challenges encountered by each article in the portfolio, highlighting the challenges of the chosen area. Conversely, the opportunities lens enables the researcher to analyze which solutions are used and which are the research opportunities within the area. Together, the two lenses allowed us to see the research characteristics carried out on Authentication in IoT for message protocols.

In Buccafurri and Romolo [18], the authors proposed an authentication integrating OTP and blockchain (smart contracts in Ethereum) to solve the existing fragility problem of the authentication mechanisms. The authors used MQTT as a message protocol in their experiment. They noted the challenges in which restricted devices often do not support the implementation of security mechanisms and the fragility of existent ones. They commented on the need for future work to implement and validate its proposal and security analysis.

Brandão [19] also introduced a solution using blockchain. Its application area encompasses industrial control systems, specifically in the SCADA system (Supervisory Control and Data Acquisition). Blockchain was used to resolve security and data storage issues on devices. The author presented challenges regarding the number of devices participating; the greater the number of devices, the more expensive the synchronization process.

Mahmoud and Aouag [20] brought a state-of-the-art view on protocols and research opportunities within the scope of security for IoT. They addressed security in 6LoWPAN, RPL, and CoAP, thus bringing a multi-layered view of the protocol stack for IoT systems. This work presented the Sybil attack and the fabrication of identities as a relevant threat to the systems mentioned before. Among the concerning issues in the security area for RPL were blackhole attacks, attack wormholes, and version number attacks. They also showed blockchain as a trend participant in IoT security solutions. Future studies will bring more depth about the attacks, evaluating the solutions with blockchain and how the attacks on the RPL affect the devices' consumption of resources.

Usman *et al.* [21] put forward a study on the representation of learning in the security domain. The authors proposed a set of machine-learning and threat detection techniques. It also analysed the platforms which offer machine-learning in the cloud, which allowed the researcher to have support in choosing the platform used. The most used security data sets on security are also presented. Limitations and challenges were presented on the exposed data sets and techniques.

Iyer *et al.* [22] implemented and evaluated lightweight algorithms for data security in the MQTT protocol. This research established the premise that a lightweight hash function and lightweight symmetric encryption were good combinations for MQTT security with low resource consumption. It also focused on the payload and used SPONGENT[6] as a hash solution to bring confidentiality, integrity, and authenticity to the information transferred.

Bhawiyuga, Data, and Warda [23] altered the standard architecture of publish/subscribe applications, inserting the authentication token server's figure. The server is responsible for authenticating and releasing the authentication token to enable communication between the parties. This solution used the JWT[7] server to distribute the tokens. They also presented a performance test with the proposed new architecture.

Several areas are covered in the bibliographic portfolio. An overview of the challenges was listed in each work, and each set of authors also commented on the proposed solution —discussed in the next section. The systematic review raised the necessary data for the list to be commented in the next section of this paper, the section on Opportunities and Challenges.

A. Opportunities and Challenges

This section presents the main results obtained from the SLR of our work. The results obtained from the bibliographic portfolio are synthesized and discussed. Our work puts forward a list of opportunities and challenges found in SRL. Two lists are presented: initially, the opportunities found are discussed, and subsequently, the challenges listed by some selected works are commented on. First, the **opportunities**:

- wide use of the MQTT protocol [18], [22], [23];
- use of *blockchain* [18]–[20];
- use of lightweight approaches [22], [23];

MQTT message protocol appeared in half of the works in the bibliographic portfolio. This old protocol is a messaging protocol widely used in production and widely accepted in academia. Only one study presented CoAP as a messaging protocol solution. However, this is an option with low impact for networks of restricted devices. This is due to the fact that such constrained protocol (CoAP) travels over UDP.

Technologies associated with blockchain have been recurrent in the works presented. This technology is gaining acceptance as a security solution in smart transactions and contracts, due to the security aspects provided by blockchain as non repudiation, and timeliness. Its use appears in several proposed solutions for IoT security, being a topic of relevance within security research and message protocols.

A constant in the studies presented is the need for a light approach to such devices. The studies which implemented security solutions [22], [23] reached a consensus on preserving computational resources. Another important consensus was that the security which exists in the protocols today is not adequate to the security level required for real IoT systems.

Just as the opportunities were exposed, we also present the **challenges** listed by our portfolio. As per the main challenges, the following can be listed:

- need for further validation and evaluation [18];

---

[6]a lightweight hash function based on a wide PRESENT-type permutation[26]

[7]JSON Web Token - the security JSON token which enables cross security domain sharing of identity and security information[27]

- sync between the biggest number of devices when using blockchain [19];
- analysis of resource consumption and ways to use blockchain [20];
- improvements in datasets and machine-learning techniques used for cybersecurity [21].

Due to the wide variety of IoT application scenarios, the evaluation and validation of solutions present themselves as challenges. It is impossible to validate a solution which performs optimally in all situations. Thus, reassessing the solutions in each scenario is the best solution.

The increase in the number of solutions involving blockchain is unquestionable. However, it is necessary to evaluate its adoption in each area. The issue of synchronization between the parties can cause a delay in the development of tasks and make the system unfeasible. Some areas have a better supply of resources and access to more robust hardware, but this is not the reality in all areas of the IoT. An approach that fits resource consumption needs would be the most favorable solution in these areas.

Improved and more specific datasets would help in training solutions which use machine learning. The improvement and optimization of the techniques used would also provide better means for research in the IoT area. Algorithms which consider devices' limitations or avoid such limitations with a different approach.

Many other challenges exist in the literature to be listed along with these. Our work provides an overview of recent articles. Further research must be carried out for the researcher's challenges in a specific IoT area. As cited, changes in areas can change solutions' performance or even make them inadequate [28].

V. Conclusion

The SLR successfully brought the desired answers, presenting the opportunities and challenges for the authentication of IoT devices in Fog Computing. A bibliographic portfolio, a quantitative analysis of the documents, and a discussion of the works found were also raised. As a result, this work presented some research material that can be reused in future technology research and development.

In future works, we propose a more comprehensive search and meta-analysis of the *corpus* of documents found. Also, develop work for continuous monitoring of opportunities so that they are better used; and the challenges for its mitigation.

Referências

[1] J. Zhang, S. Rajendran, Z. Sun, R. Woods e L. Hanzo, "Physical layer security for the Internet of Things: Authentication and key generation," *IEEE Wireless Communications*, v. 26, n. 5, pp. 92–98, 2019.

[2] S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari e A. Kashif Bashir, "A survey of security and privacy issues in the Internet of Things from the layered context," *Transactions on Emerging Telecommunications Technologies*, e3935, 2020.

[3] J. Cao, M. Ma, H. Li et al., "A Survey on Security Aspects for 3GPP 5G Networks," *IEEE Communications Surveys & Tutorials*, 2019.

[4] S. Yi, Z. Hao, Z. Qin e Q. Li, "Fog computing: Platform and applications," em *2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)*, IEEE, 2015, pp. 73–78.

[5] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen e Y. Koucheryavy, "Multi-factor authentication: A survey," *Cryptography*, v. 2, n. 1, p. 1, 2018.

[6] L. C. Chaves, L. Ensslin, S. R. Ensslin, S. M. Petri e F. S. Da Rosa, "Gestão do processo decisório: mapeamento ao tema conforme as delimitações postas pelos pesquisadores," *Revista Eletrônica de Estratégia & Negócios*, v. 5, n. 3, pp. 3–27, 2012.

[7] B. A. Kitchenham, T. Dyba e M. Jorgensen, "Evidence-based software engineering," em *Proceedings. 26th International Conference on Software Engineering*, IEEE, 2004, pp. 273–281.

[8] L. Machado e L. G. L. Vergara, "Uma análise sistemática da literatura acerca dos métodos de usabilidade aplicáveis a dispositivos móveis," *Gepros: Gestão da Produção, Operações e Sistemas*, v. 15, n. 1, p. 42, 2020.

[9] D. Moher, A. Liberati, J. Tetzlaff e D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement," *Annals of internal medicine*, v. 151, n. 4, pp. 264–269, 2009.

[10] J. Reiswig, "Mendeley," *Journal of the Medical Library Association: JMLA*, v. 98, n. 2, p. 193, 2010.

[11] H. Zaugg, R. E. West, I. Tateishi e D. L. Randall, "Mendeley: Creating communities of scholarly inquiry through research collaboration," *TechTrends*, v. 55, n. 1, pp. 32–36, 2011.

[12] J. Gamalielsson e B. Lundell, "Sustainability of Open Source software communities beyond a fork: How and why has the LibreOffice project evolved?" *Journal of Systems and Software*, v. 89, pp. 128–145, 2014.

[13] T. Williams, C. Kelley, R. Lang, D. Kotz e J. Campbell, "1 gnuplot," 2004.

[14] Z. Wang, R. Wu, Q. Sa et al., "An Improved Cluster Routing Structure of IOT," em *2016 International Conference on Communications, Information Management and Network Security*, Atlantis Press, 2016, pp. 326–328.

[15] Z. Wang, G. Cui, P. Li, W. Wang e Y. Zhang, "Design and implementation of NS3-based simulation system of LEO satellite constellation for IoTs," em *2018 IEEE 4th international conference on computer and communications (ICCC)*, IEEE, 2018, pp. 806–810.

[16] J. Y. Corona-Ventura, O. Lobato-Nostroza, G. M. Chávez-Campos et al., "Correlation Study between Photovoltaic Power Output and Environmental Variables Using an Embedded IoT System," em *2019 IEEE International Autumn Meeting on Power, Electronics and Computing (ROPEC)*, IEEE, 2019, pp. 1–6.

[17] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey e S. Linkman, "Systematic literature reviews

in software engineering–a systematic literature review," *Information and software technology*, v. 51, n. 1, pp. 7–15, 2009.

[18] F. Buccafurri e C. Romolo, "A Blockchain-Based OTP-Authentication Scheme for Constrainded IoT Devices Using MQTT," em *Proceedings of the 2019 3rd International Symposium on Computer Science and Intelligent Control*, 2019, pp. 1–5.

[19] R. Brandão, "A blockchain-based protocol for message exchange in a ICS network: student research abstract," em *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, 2020, pp. 357–360.

[20] C. Mahmoud e S. Aouag, "Security for Internet of Things: A State of the Art on existing Protocols and Open Research issues," em *Proceedings of the 9th International Conference on Information Systems and Technologies*, 2019, pp. 1–6.

[21] M. Usman, M. A. Jan, X. He e J. Chen, "A survey on representation learning efforts in cybersecurity domain," *ACM Computing Surveys (CSUR)*, v. 52, n. 6, pp. 1–28, 2019.

[22] S. Iyer, G. Bansod, P. Naidu e S. Garg, "Implementation and Evaluation of Lightweight Ciphers in MQTT Environment," em *2018 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT)*, IEEE, 2018, pp. 276–281.

[23] A. Bhawiyuga, M. Data e A. Warda, "Architectural design of token based authentication of MQTT protocol in constrained IoT device," em *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, IEEE, 2017, pp. 1–4.

[24] M. Dabić, J. Maley, L.-P. Dana, I. Novak, M. M. Pellegrini e A. Caputo, "Pathways of SME internationalization: a bibliometric and systematic review," *Small Business Economics*, v. 55, n. 3, pp. 705–725, 2020.

[25] E. Siow, T. Tiropanis e W. Hall, "Analytics for the internet of things: A survey," *ACM Computing Surveys (CSUR)*, v. 51, n. 4, pp. 1–36, 2018.

[26] A. Bogdanov, M. Knežević, G. Leander, D. Toz, K. Varıcı e I. Verbauwhede, "SPONGENT: A lightweight hash function," em *International Workshop on Cryptographic Hardware and Embedded Systems*, Springer, 2011, pp. 312–325.

[27] M. Jones, B. Campbell e C. Mortimore, "JSON Web Token (JWT) profile for OAuth 2.0 client authentication and authorization Grants," *May-2015.[Online]. Available: https://tools. ietf. org/html/rfc7523*, 2015.

[28] W. dos Reis Bezerra e C. B. Westphall, "Ambiente de experimentação para avaliação protocolos de mensagem para IoT na Fog," em *Anais do Workshop de Pesquisa Experimental da Internet do Futuro*, SBC, 2020, pp. 1–6.