5G Network Security for IoT Implementation: A Systematic Literature Review

Chapter · January 2021

DOI: 10.1007/978-3-030-60467-7_3

Manuel Montaño
Universidad Técnica Particular de Loja

Johana Briceño
Instituto Superior Tecnológico Sudamericano

Fernando Pesántez - Bravo
Instituto Superior Tecnológico Sudamericano

5g network security for IoT implementation: A Systematic Literature Review

Manuel Montaño – Blacio [1][0000-0001-6816-0439], Johana Briceño – Sarmiento[1][0000-0002-1072-1261], and Fernando Pesántez – Bravo[1][0000-0001-9882-9527]

[1] Instituto Superior Tecnológico Sudamericano, Miguel Riofrío 156 – 26, Loja, Ecuador
afpesantez@tecnologicosudamericano.edu.ec

Abstract. Fifth generation (5G) wireless technologies satisfies the growing demand for the Internet of Things (IoT), however, IoT devices are vulnerable to security threats due to the simplicity of their hardware and communication protocols, which imply possible attacks and security challenges. In this work we propose to conduct a systematic review of literature that relates 5G technologies to the internet of things and approach the security that the 5G network for IoT must provide. The Torres – Carrión method is used, raising four research questions: a) information security services, b) types of attacks in 5G-IoT, c) security in the layers of the IoT network architecture, d) strategies for 5G-IoT network security. Semantic search criteria were applied, in the Scopus database, obtaining 23 articles from 18 journals, the main studies were collected, it is evident that the blockchain is an efficient security mechanism that merits further study, that the physical layer is the one that receives the most active and passive attacks, such as denial of service (DoS) that is studied by several authors, together with mechanisms, architectures, protocols and algorithms that provide the security services of a mobile network.

Keywords: security, 5g network, IoT, attacks.

1 Introduction

The growing development of IoT in the last years has admitted a number of connections of devices and objects, the fifth generation of 5G mobile technology, is a fundamental pillar to satisfies the demand for new services and the massive deployment, with this, the security risks increase and the problems of vulnerability and attacks in the different layers of network become more evident. There is still no complete security framework applicable to the 5G-IoT network, studies and tests are carried out to validate some architecture, mechanism or algorithm that ensures the transmission of information; encryption reduces attacks against devices [1], the IoT architecture based on layers on models and security features recognizes possible attacks and, the analysis of the network layer proposes solutions for the IoT industry [2, 3].

Therefore, the objective of this work is to contribute to the knowledge about security research that is implemented for a 5G-IoT network, to publicize existing proposals, vulnerabilities and attacks [4] that in some way affect the integrity, reliability and availability of information [5], devices or network architecture. Consequently, a systematic literature review of the subject is carried out to determine research questions, as well as to identify future research.

In this systematic review of the literature we use the method proposed by Torres-Carrión [6], which divides the process into three parts: planning, review report and presentation of results. We found 70 studies on the security of the 5G-IoT network. No systematic literature reviews were found that specifically address security in the 5G and IoT network together. Next, four research questions are posed related to network security services, establishing the most frequent attacks, knowing in which layer more attacks are carried out and defining the strategies used to control the transmission of information.

To execute the planning of the search process, general and specific inclusion and exclusion criteria were established. Variables that include theoretical support, standard and indicators are determined to organize the answers to each research question. Through the article search process, 23 studies were obtained, which, through the use of the Mendeley bibliography manager, were organized and managed.

Each of the articles is analyzed to list the studies based on the indicators of the proposed variables and determine comparisons with previous work and future research. Finally, the results of the study are presented in tables, together with the argumentation of the answer to each research question, leaving the topic open for future investigations of systematic reviews of literature through this methodological adaptation.

2 Method.

For the SLR, of the Systematic review of the literature proposed by Torres-Carrión [6] adapted from Kitchenham and Bacca is applied, it divides the process into three main phases, planning, review report and presentation of results, which are detailed in Table 1.

Table 1. Phases of the Torres-Carrión Methodology

Planning	Review report	Results presentation
Identification of the need for the review Current security status in 5G *Conceptual mindfact* Semantic Search Structure Research questions Review Protocol Development Related Systematic Reviews Journal selection and Database Definition of analysis categories	Search ID Selection of primary studies Note of study quality Data extraction and tracking Synthesis and data monitoring	Results Conclusions

2.1 Planning.

Current state of security in 5G. The 5G network is considered as a technological evolution, increases coverage, capacity, transmission speed and also carries security risks; the high speed of the connection and the number of devices connected at the same time could generate security gaps at the provider level and of course final users; these gaps would allow denial of service (DDoS) attacks [7], vulnerabilities and privacy issues; it is necessary then to improve the authentication of devices, the integrity of the data and the confidentiality of the information.

Resarch questions. The Internet of Things (IoT) is changing communications and services today, new paradigms have emerged as they move from a conventional industry to an intelligent industry, having its massive development with the implementation of the 5g network. However, due to the heterogeneous environment in 5G networks and the nature of transmission of radio propagation, the guarantee of privacy security, authentication, authorization, control of access to devices and preservation of privacy is a challenging task. We are interested in 5G-IoT security [8] based on security factors such as: integrity, authentication, confidentiality and availability, so we consider the following research questions:

- RQ1 – Of the services that describe information security, which ones apply in the 5G-IoT network?
- RQ2 – In the 5G-IoT network, ¿what attacks can occur?
- RQ3 – Of the network architecture layers, which one has worked the most in the 5G-IoT network security level?

- RQ4 – ¿What strategies have been used in joint investigations for security in the 5G-IoT network?

Conceptual mindfact. According to the Torres – Carrión methodology, the *conceptual mindfact* is carried out, which "allows the researcher to focus his attention on the real theoretical context of the research"[6].

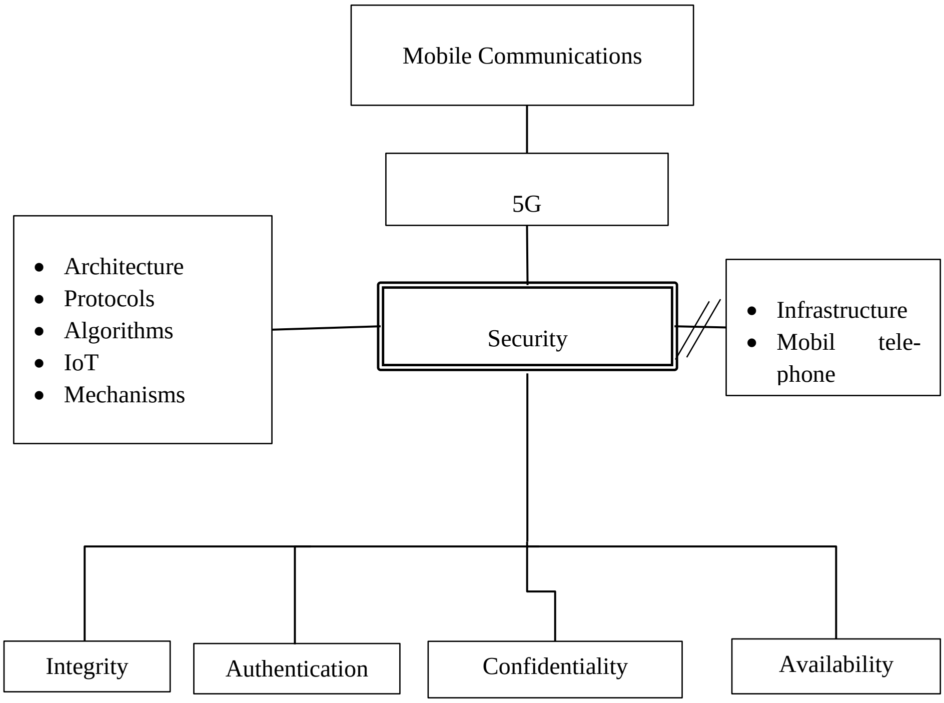

Fig. 1. Conceptual mindfact about the safety of 5G-IoT

In Fig. 1, the conceptual mindfact is presented that detailed schematically the conceptual structure of security in the 5G-IoT network; concept that derives from the areas of mobile communications and fifth generation networks (5G)[9]. Subclasses include integrity, authentication, reliability and availability [5, 10]. The 5G-IoT network security features that are of interest to the study are evident on the left side of the mind: architecture, protocols, algorithms, mechanisms and internet of things (IoT). Other fields of science, which are part of security, that will not be studied are: infrastructure and mobile telephony.

Development of Review Protocols.

- General criteria
  - Studies that involve security in 5G-IoT networks.
  - Publications of the last 5 years, from 2016 to 2020.
  - The Scopus database is considered for the article search
- Specific criteria
  - For the search of services that describe the security of the information that are applied for 5G-IoT networks in RQ1, the ISO 27001 standard was considered.
  - To know what types of attacks 5G-IoT networks can present, according to RQ2, variables such as active and passive attacks have been used.
  - According to the architecture layers network of RQ3, is was considered physic layer, network and application.
  - It is necessary to know if there are joint investigations that propose security solutions in 5G-IoT networks, in order to verify whether a strategy that guarantees a secure network can be used, according to what is expressed in RQ4.
- Exclusion criteria
  - Studies in which reference is made to security in infrastructure and mobile telephony.
  - Only studies published in journals will be taken into account.

Semantic search structure. The semantic structure (Table 2) is elaborated from the conceptual mindset, based on the synonymy and the scientific thesaurus taken from the website [11]. The search structure is organized into three levels: 5G (L1), IoT (L2) and review protocols (L3). A search is carried out grouping L1 and L2 and results in 70 articles that refer to topic 5G-IoT.

Table 2. The semantic structure of the thesaurus for the search of specific articles.

L1	5G	5g security networks	(secur* OR safe OR insur* OR preservation OR surveillance) AND (5g OR "fifth generation" OR "last generation" OR "mobile networks 5g")	2168
		+service security	AND (integrity OR auth* OR disponibility OR confidentiality OR vulnerability OR attacks OR amen* OR threat)	750
L2	IoT	+IoT	AND (iot OR "Internet of things" OR "In-ternet for all" OR ioe)	78428
		+layer	AND (phy OR "Physical Layer" OR "network layer" OR "application layer" OR perception OR mac OR "Media access control")	3728
[L1 AND L2]	[5G AND IoT]			70
L3	PROTOCOLS			
	Year		2016-2020	70
	Subject area		Computer Science	61
	Document Type		Article	23
	Languaje		English	23
	Quality criteria		Detailed reading of each article, to establish its relationship with the research area	19

Following the proposed methodology four revision protocols are applied, it starts considering the last 5 years, then it is limited to the area of computer science, selecting only articles in English, since they represent results of the relevant investigations on the problem raised. Finally, a detailed reading of each article is made to establish its relationship with security in 5G-IoT networks.

Related systematic reviews. The systematic review of related works is essential to achieve an original and especially useful contribution to the scientific community. A search was made in the Scopus database (Table 3) using the Syntax of database. In the works that were found, they did not fully answer the questions proposed in this investigation; in some cases analyzed, only part of the question is addressed and not within the context of this work, the general script was used with filtering oriented to a "review", "slr", "meta-analysis" or "survey".

Table 3. Recent studies of reviews of the literature on security in 5G-IoT networks.

Study	Analysis	Articles reviewed
[2]	The literature review, only at one point focuses on security and privacy for IoT, provides industry solutions from 3GPP. Related studies focus on the network layer to ensure that IoT traffic is delivered securely and efficiently between MTC devices (machine type communication) and mobile networks	>100
[1]	In this article, the authors study what concerns the applications, protocols, vulnerabilities and security of IoT networks. They have made a systematic review of literature in which they have included analysis of articles related to IoT during the period 2015 - 2017 and conclude that the medical application is the most recurrent, in terms of attacks, they argue that the one that goes against The device is the most common and that as a tool to counteract these, encryption is used. By relating this article to the work realized, it can be said that the analysis developed focuses only on IoT, it is quite clear, but does not involve the implementation in 5G networks.	111
[3]	Analyze the IoT architecture based on layered models and security features supported by security requirements such as the CIA triad, confidentiality, integrity and availability and other requirements such as accounting, auditability, non-repudiation, and privacy. It recognizes the possible security attacks of an IoT network in the four main layers, in which it generally proposes countermeasures to detect some security risks but not concrete solutions.	57

Journal selection and Database.

Database. The database selected for the search is Scopus, the same one that has prestige in different fields of science; tools were used that contributed to obtaining 70 articles that refer to security in 5G - IoT networks; after that a selection is made based on the specified criteria

List of journals. The 23 articles found belong to 18 journals. The most relevant journal is IEEE Internet of Things, by its metrics it is located in quartile Q1 with an impact factor of 1.4; reflects a value of 129.36 and according to Google academic, has an h5 index of 70, refer to Table 4. It publishes articles on the latest advances, as well as review articles, on the various aspects of IoT. Topics include the architecture of the IoT system, the technologies that allow IoT, IoT communication and network protocols, such as network coding, IoT services and applications[12].

Table 4. List of journals organized by category according to SJR 2018.

Ord	Journals name	Nro. papers	SJR		h5	Value
			IF	Cuartil	Google	
SJR Science Edition						
1	IEEE Internet Of Things Journal	4	1,4	Q1	70	129,360
2	IEEE Journal On Selected Areas In Communications	1	2,29	Q1	90	68,013
3	IEEE Transactions On Industrial Informatics Transactions	1	1,68	Q1	86	47,678
4	Journal Of Network And Computer Applications	1	0,9	Q1	70	20,790
5	Future Generation Computer Systems	1	0,84	Q1	73	20,236
6	IEEE Access	1	0,61	Q1	89	17,916
7	Cognitive Computa-	1	1,06	Q1	36	12,593
8	Computers And Security	1	0,67	Q1	50	11,055
9	Electronics Switzerland	2	0,46	Q1	1	0,304

Definition of analysis categories. This section defines the categories of analysis for each research question, which facilitate grouping the articles according to the criteria that allow obtaining a response systematically to the questions proposed in 2.1.

- RQ1 – Of the services that describe information security, which ones apply in the 5G-IoT network? variables of ISO 27001 are considered.

  - Categories of the ISO 27001 standard (Information security): integrity, availability, confidentiality and authentication [13].
- RQ2 – In the 5G-IoT networks, what attacks can occur? The variables considered are passive and active attacks.
  - Passive attack categories: release of message contents and traffic analysis [4].
  - Categories active attacks: masquerade, replay, modification of messages and denial of service [4].
- RQ3 – Of the network architecture layers, which one has worked the most in the 5G-IoT network security level? IoT network architecture variables are considered.
  - IoT architecture categories: Physical layer, network and application [14].
- RQ4 – What strategies have been used in joint investigations for security in the 5G-IoT network? It is considered as variable security strategies?.
  - The categories that are taken into account for the analysis are: architectures, mechanisms, protocols and algorithms [15].

3 Review report

3.1 Of the services that describe information security, which ones apply in 5G-IoT network?

From the services that describe information security, studies show that the security of the 5G-IoT network is linked to the services proposed in the ISO 27001 standard, which focuses on confidentiality, authentication, integrity and availability to achieve information security, 45% of the articles reviewed maintain that confidentiality is the most sensitive part of these networks and propose some strategies (RQ4) to guarantee this service, 35% have parallel to confidentiality, authentication as one of the critical services that gives authorized users access to a network [16], regardless of the integrity and availability of the complement for a secure network scheme (Tabla 5).

Table 5. Items that had the ISO 27001 standard.

RQ1	From the services that describe information security, are they considered 5G-IoT network?		*f*
ISO 27001	Integrity	[17–19]	3
	Disponibility	[18]	1
	Confidentiality	[17–25]	9
	Authentication	[16–18, 23, 25–27]	7

3.2 RQ2 – In the 5G-IoT network, what attacks can occur?

The attacks present in a network, Stallings [4] classify them into passive and active attacks; in the reviewed articles it is mentioned that in the 5G-IoT network, the most frequent attacks in this type of networks are, denial of service (DoS), replay, masquerade and traffic analysis. In [20] it presents a routing attack due to the dynamic infrastructure of the IoT network, analyzes and proposes measures to counteract the sinkhole and selective forwarding. An important effort is the analysis in [28, 29] to avoid the denial attack of service (DoS). In [18], it mentions a considerable contribution in defining possible security attacks and services based on the new service requirements and 5G network uses (Table 6).

Table 6. Articles that refer to passive and active attacks.

RQ2	In the 5G-IoT network, ¿which attcks can occurs?		*f*
Passive attacks	Release of message contents	[26, 30]	2
	Traffic analysis	[23–25]	3
Active attacks	Masquerade	[16, 23, 28]	3
	Replay	[20, 22, 23, 30]	4
	Modification of messages	[25, 30]	2
	Denial of service	[20],[23, 28–30]	5

3.3 RQ3 – Of the layers of network architecture, which has worked more in the level of network security 5G-IoT?

Traditionally network security has been implemented in the upper layers, however, with the development of new types of services to support a large number of users and connected devices, IoT networks evolve and massify, making the physical layer (PHY) a more attractive target for hackers. The articles analyzed show that the physical layer (PHY) in the 5G-IoT network is the most considered to develop security strategies, in [31], it is mentioned that the study of physical capacity has received a growing interest and analyzes possible safety techniques; PHY presents security breaches that cause problems when applying techniques such as multiple entry, multiple exit (MIMO) [24], In addition, it is expressed that problems may occur due to dynamic infrastructure, protocols and heterogeneity of mobile objects [20]. Other authors have focused their study on improving the safety of physical capacity, proposing new strategies (Table 7).

Table 7. Articles that mention vulnerabilities in network layers.

RQ3	De las capas de arquitectura de red ¿Cuáles son las más vulnerables dentro de red 5G-IoT?		*f*
Network architecture	Physical	[18, 21, 22, 24, 31, 32]	6
	Network	[16, 17, 20]	3
	Application	[16, 29]	2

3.4 RQ4 – What strategies have been used in joint investigations for security in 5G-IoT networks?

Security in the 5g-IoT network is a crucial point, several authors have proposed different strategies to ensure that the information that is transmitted has confidentiality, availability, integrity and of course it reaches the user who requires it; solutions such as blockchain [33] applied to IoT are proposed to solve problems of interoperability, privacy, security, traceability and network reliability through a distributed environment; as a mechanism is proposes crowdsourcing to mitigate local and remote attacks; The authors also present authentication systems, encryption and algorithms that complement the security frameworks (Table 8).

Table 8. Articles that analyze and / or propose network security strategies.

RQ4	What strategies have been used in joint investigations for security in 5G-IoT networks?		*f*
Security strategies	Architecture	[18, 23, 29, 33]	4
	Mechanisms	[18, 20, 22, 26, 27, 29–31, 34]	9
	Protocols	[16, 23, 25–27, 30]	6
	Algorithms	[17, 20, 23, 24, 30, 33]	6

4 Discussion

To ensure the communication of IoT devices in a 5G network, [17] - [25] it maintains that confidentiality must be taken into account to guarantee that the data is available only for users who are authorized and do not have interference or are heard by others not authorized; in [16] - [18], [23], [25] - [27] it is stated that authentication is one of the information security services that allow the data delivered to be genuine like devices or applications, these services together with the availability [18] that guarantees that the data and devices are available in real-time, and the integrity [17] - [19] that means that the data is not manipulated by intentional or unintentional interference during the delivery of Information on the network are critical aspects that must be considered when establishing a security framework for a 5G - IoT network.

Attacks on network security are analyzed by each of the layers, in the physical or perception layer [18], [21], [22], [24], [31], [32] responsible for collecting data from devices such as sensors or activators, there are attacks such as modification of messages in which malicious code or false data can be injected that allow the attacker to access the functions of the IoT devices and also send false data to users or applications, directly false information and therefore erroneous IoT services; In the replay attack [20], [22], [23], [30] in IoT, the attacker uses a device to send the final element true identification information, and to make it recognized as another component of the network.

The network layer is responsible for routing information to the destination and its security is focused on the availability of resources; In this capacity, there are attacks such as masquerade [16], [23], [28] which is an attack that fraudulently takes the identity of an authorized user of a computer system using stolen passwords or logins to access information. from an IoT device; the DoS (denial of service) attack [20], [23], [28] - [30] that denies the availability of IoT services due to the massive transmission of information to the red; in [20] they present a routing attack, the sinkhole in which a node like the one that transmits the information is passed and the neighboring nodes recognize it, sending data, breaking confidentiality and facilitating additional attacks such as DoS; traffic analysis [23] - [25] in which the attacker intercepts the messages sent, placing itself between the communication, also, the release message [26], [30] the attacker can read and capture the message, but cannot modify it.

The application layer [16], [29] is the one that stays the services for the end-user and its security is focused on software attacks, among which are the attack that involves the end-user to obtain their passwords, passwords through emails or web pages, malicious virus that obtain or modify confidential data and malicious scripts that spoil the functions of the IoT network.

To mitigate the attacks that occur in the 5G - IoT network, solutions are proposed in [18], [23], [29], [33], [18], [20], [26], [27], [29] - [31], [34], [16], [23], [25] - [27], [30], [17], [20], [23], [24], [30] focused on architectures, protocols, mechanisms and algorithms, among the most relevant to solve security problems are the blockchain [33] that allows red interoperability, privacy, traceability and reliability through a distributed environment and, as a mechanism, propose crowdsourcing [22] to mitigate local and remote attacks; The authors also present authentication, encryption and algorithm systems that complement the security frameworks.

5 Conclusions and future work

Security in the 5G - IoT network is a research paradigm, some studies analyze network security, others the IoT security requirements; Few related studies refer to the 5G - IoT network within a security framework, which guarantees authentication, availability, and confidentiality [5], therefore, this article provides an analysis of information security services, the possible attacks that They present in the layers of IoT architecture (perception, network, and application), as well as frameworks for the secure implementation of IoT, among which blockchain technology [33] is effective in stopping denial of service (DoS) attacks [29], Because it is the most recurrent due to the number of interconnected devices in the network, crowdsourcing [22] is proposed to mitigate local and remote attacks.

The physical layer has been the one that presents the most attacks of different types [21], [24], [31], these include passive and active attacks and, of course, related to the information security services analyzed. Finally, the strategies proposed in the articles are based on architectures, mechanisms, protocols, and algorithms that are aimed at providing security to IoT in 5G, allowing offering greater speed and efficiency to control IoT devices. It is important to delve into several of the proposed strategies and continue adapting some already known in the 5G - IoT network, achieving more reliable security frameworks, devices without risks and information without interruptions and intruders, it would be important to take advantage of artificial intelligence technologies to combat the network security issues.

References

1. Amiruddin, A., Ratna, A.A.P., Sari, R.F.: Systematic review of internet of things security. Int. J. Commun. Networks Inf. Secur. 11, 248–255 (2019)
2. Zhang, S., Wang, Y., Zhou, W.: Towards secure 5G networks: A Survey. Comput. Networks. 162, 106871 (2019). https://doi.org/10.1016/j.comnet.2019.106871
3. Gafurov, K., Chung, T.M.: Comprehensive survey on internet of things, architecture, security aspects, applications, related technologies, economic perspective, and future directions. J. Inf. Process. Syst. 15, 797–819 (2019). https://doi.org/10.3745/JIPS.03.0125
4. Stallings, W.: Cryptography and Network Security Principles and practice. Fifth Edition. Prentice Hall (2011)
5. Calder, A.: Information Security based on ISO 27001/ISO 27002. van Haren Publishing (2009)
6. Torres-Carrion, P.V., Gonzalez-Gonzalez, C.S., Aciar, S., Rodriguez-Morales, G.: Methodology for systematic literature review applied to engineering and education. In: IEEE Global Engineering Education Conference, EDUCON. pp. 1364–1373. IEEE Computer Society (2018)
7. Gurusamy, D., Deva Priya, M., Yibgeta, B., Bekalu, A.: DDoS risk in 5G enabled iot and solutions. Int. J. Eng. Adv. Technol. 8, 1574–1578 (2019)
8. Li, S., Xu, L. Da, Zhao, S.: 5G Internet of Things: A survey, https://linkinghub.elsevier.com/retrieve/pii/S2452414X18300037, (2018)
9. Liyanage, M., Ahmad, I., Abro, A.B., Gurtov, A., Ylianttila, M.: A Comprehensive Guide to 5G Security. Wiley (2018)
10. Iso.org: ISO/IEC 30141:2018(en), Internet of Things (loT) — Reference Architecture, https://www.iso.org/obp/ui/es/#iso:std:iso-iec:30141:ed-1:v1:en
11. thesaurus.com: Thesaurus, https://www.thesaurus.com
12. Wang, H.: IEEE Internet of Things Journal, https://ieeexplore.ieee.org/xpl/aboutJournal.jsp?punumber=6488907
13. Romero Castro, M.I., Figueroa Morán, G.L., Vera Navarrete, D.S., Álava Cruzatty, J.E., Parrales Anzúles, G.R., Álava Mero, C.J., Murillo Quimiz, Á.L., Castillo Merino, M.A.: Introducción a la seguridad informática y el análisis de vulnerabilidades. (2018)
14. Chaudhuri, A.: Internet of Things, for Things, and by Things. CRC Press (2018)
15. UIT: La seguridad de las telecomunicaciones y las tecnologías de la información. 136 (2006)
16. Ouaissa, M., Ouaissa, M., Rhattoy, A.: An efficient and secure authentication and key agreement protocol of LTE mobile network for an IoT system. Int. J. Intell. Eng. Syst. 12, 212–222 (2019). https://doi.org/10.22266/ijies2019.0831.20
17. Heigl, M., Doerr, L., Tiefnig, N., Fiala, D., Schramm, M.: A resource-preserving self-regulating Uncoupled MAC algorithm to be applied in incident detection. Comput. Secur. 85, 270–287 (2019). https://doi.org/10.1016/j.cose.2019.05.010
18. Fang, D., Qian, Y., Hu, R.Q.: Security for 5G Mobile Wireless Networks. IEEE Access. 6, 4850–4874 (2017). https://doi.org/10.1109/ACCESS.2017.2779146
19. Militano, L., Orsino, A., Araniti, G., Iera, A.: NB-IoT for D2D-enhanced content uploading with social trustworthiness in 5G systems. Futur. Internet. 9, (2017). https://doi.org/10.3390/fi9030031

20. Santos, A.L., Cervantes, C.A.V., Nogueira, M., Kantarci, B.: Clustering and reliability-driven mitigation of routing attacks in massive IoT systems. J. Internet Serv. Appl. 10, (2019). https://doi.org/10.1186/s13174-019-0117-8
21. Wang, N., Wang, P., Alipour-Fanid, A., Jiao, L., Zeng, K.: Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities. IEEE Internet Things J. 6, 8169–8181 (2019). https://doi.org/10.1109/JIOT.2019.2927379
22. Nieto, A., Acien, A., Fernandez, G.: Crowdsourcing Analysis in 5G IoT: Cybersecurity Threats and Mitigation. Mob. Networks Appl. 24, 881–889 (2019). https://doi.org/10.1007/s11036-018-1146-4
23. Cao, J., Yu, P., Ma, M., Gao, W.: Fast authentication and data transfer scheme for massive NB-IoT Devices in 3GPP 5G Network. IEEE Internet Things J. 6, 1561–1575 (2019). https://doi.org/10.1109/JIOT.2018.2846803
24. Xu, L., Chen, J., Liu, M., Wang, X.: Active eavesdropping detection based on large-dimensional random matrix theory for massive MIMO-enabled IoT. Electron. 8, (2019). https://doi.org/10.3390/electronics8020146
25. Sharma, V., You, I., Leu, F.Y., Atiquzzaman, M.: Secure and efficient protocol for fast handover in 5G mobile Xhaul networks. J. Netw. Comput. Appl. 102, 38–57 (2018). https://doi.org/10.1016/j.jnca.2017.11.004
26. Arul, R., Raja, G., Almagrabi, A.O., Alkatheiri, M.S., Chauhdary, S.H., Bashir, A.K.: A quantum-safe key hierarchy and dynamic security association for LTE/SAE in 5G scenario. IEEE Trans. Ind. Informatics. 16, 681–690 (2020). https://doi.org/10.1109/TII.2019.2949354
27. Huang, X., Craig, P., Lin, H., Yan, Z.: SecIoT: a security framework for the Internet of Things. Secur. Commun. Networks. 9, 3083–3094 (2016). https://doi.org/10.1002/sec.1259
28. Safkhani, M., Shariat, M.: Implementation of secret disclosure attack against two IoT lightweight authentication protocols. J. Supercomput. 74, 6220–6235 (2018). https://doi.org/10.1007/s11227-018-2538-8
29. Salva-Garcia, P., Alcaraz-Calero, J.M., Wang, Q., Bernabe, J.B., Skarmeta, A.: 5G NB-IoT: Efficient Network Traffic Filtering for Multitenant IoT Cellular Networks. Secur. Commun. Networks. 2018, (2018). https://doi.org/10.1155/2018/9291506
30. Fu, Y., Yan, Z., Cao, J., Koné, O., Cao, X.: An Automata Based Intrusion Detection Method for Internet of Things. Mob. Inf. Syst. 2017, (2017). https://doi.org/10.1155/2017/1750637
31. Zhang, S., Xu, X., Peng, J., Huang, K., Li, Z.: Physical layer security in massive internet of things: Delay and security analysis. IET Commun. 13, 93–98 (2019). https://doi.org/10.1049/iet-com.2018.5570
32. Memon, M.L., Saxena, N., Roy, A., Shin, D.R.: Backscatter Communications: Inception of the battery-free era—A comprehensive survey. Electron. 8, (2019). https://doi.org/10.3390/electronics8020129
33. Dai, H.N., Zheng, Z., Zhang, Y.: Blockchain for Internet of Things: A Survey. IEEE Internet Things J. 6, 8076–8094 (2019). https://doi.org/10.1109/JIOT.2019.2920987
34. Ni, J., Lin, X., Shen, X.S.: Efficient and Secure Service-Oriented Authentication Supporting Network Slicing for 5G-Enabled IoT. IEEE J. Sel. Areas Commun. 36, 644–657 (2018). https://doi.org/10.1109/JSAC.2018.2815418