Advances in Dynamical Systems and Applications.
ISSN 0973-5321, Volume 16, Number 2, (2021) pp. 1671-1692

https://www.ripublication.com/adsa.htm

Systematic Literature Review of Internet of Things (IoT) Security

Abla El bekkali [1 2], Mohammad Essaaidi [1], Mohammed Boulmalf [2], Driss El majdoubi [1]

[1] ENSIAS, Mohammed V University of Rabat.

[2] UIR, International University of Rabat.

Abstract

The Internet of Things (IoT) can be considered one of the most powerful tools for creating, modifying and sharing data. There are now billions of connected objects, and this number is growing more and more. While the proliferation of connected objects could facilitate all aspects of our lives, security concerns are also increasing. It is widely recognized that the IoT is first and foremost a threat to user privacy. Furthermore, there are many solutions and countermeasures are proposed to deal with the security risks of IoT. In this Systematic Literature Review (SLR) we present an in-depth analysis of the security of IoT, considering the most generic architecture with the different layers and their security issues and the solutions proposed to deal with them. Furthermore, this SLR also provides an insight on the current trends and future research directions of IoT security.

Keywords: Internet of things, security, privacy, challenges, architecture.

I. INTRODUCTION

IoT is the acronym for Internet of Things, it was coined in 1999 by Kevin Ashton, defining a system where physical objects are connected to the Internet [1].

The Internet of Things is the convergence of several technologies (physical devices, vehicles and other elements including electronics, software, sensors ...) and network connectivity allowing the collection and exchange of data from and among connected objects. The IoT has become one of the most important technologies of the 21st century, offering possibilities for the physical world to be integrated into computer systems, thus allowing improved efficiency, economic benefits and reduced human efforts [2].

These devices, are powered by a set of sensors (microphones, cameras, GPS,

thermometers, etc.) which constantly collect information about their environment, including sensitive personal information. New smart devices offer a wide range of new features, promising convenience and a better life, however the variety and large amount of user data collected, analyzed, transported and stored in each layer of the IoT architecture presents several vulnerabilities [3].

Indeed, the success of IoT devices has not gone unnoticed and the number of threats and attacks against IoT devices and services is also increasing. However, it is therefore essential to identify the risks and implement security measures to secure IoT devices and to protect people's privacy. The field of research related to IoT security is relatively new. Therefore, we deemed it to be very helpful to carry out a systematic literature review of the most important and significant research work in this field to get an insight on the most important IoT security challenges, the different solutions proposed to address them and to identify the most important current and future research directions in this area.

The remainder of this article is presented as follows: In section 2, we present the different methods used for the selection of primary studies used in this SLR. Section 3 provides an overview of IoT security, the general IoT architecture, the IoT security challenges, the security issues of each layer of the IoT architecture and thus the different protocols of IoT security. Section 4 is dedicated to a review and comparison of the different solutions proposed to address IoT security threats and challenges. Section 5 presents the main conclusions of this SLR.

II. RESEARCH METHODOLOGY

In order to answer the research questions and to achieve an in-depth SLR on IoT security, we adopted an approach based on three stages, namely, planning, conducting, and reporting.

A. Primary studies

In order to increase the emergence of search results, primary studies were selected based on keywords in the search function of a publication or a search engine. The search strings are as follows:

("Internet of things" OR "IoT") AND "security"

("Internet of things" OR "IoT") AND ("cybersecurity" OR "cyber-security")

("Internet of things" OR "IoT") AND "Threats"

We will consider the following publishers online platforms for the papers retained for this SLR: IEEE Xplore, Google Scholar, ScienceDirect, SpringerLink, ACM Digital Library.

Based on the above mentioned inclusion / exclusion criteria (Table 1), we thoroughly searched these platforms for papers that comply with them in their titles or abstracts or keywords.

B. Data extraction

The selected primary studies were grouped after extracting, classifying and storing the data for each study according to certain categories (Table 1):

Table 1. Inclusion and Exclusion criteria

Inclusion criteria	**Exclusion criteria**
Posted in journals, conferences or websites	The study does not address IoT or IoT security
Published after 2008	The study is not written in English
Presents results, challenges or protocols related to IoT security	Electronically inaccessible
Presents IoT security architectures	The study does not contain references

Figure 1 shows the rate of paper selected in the different stages of the process after the search performed on the platforms indicated above.

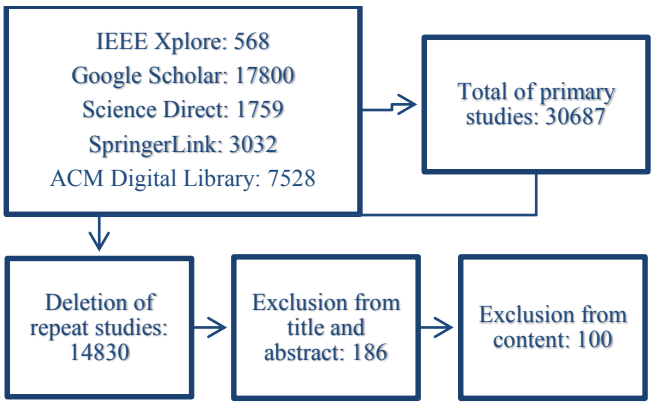

Fig. 1. Selection of papers

Figure 2 presents the distribution of the selected papers by year. We note that more than 70% of the studies have been published over the years (2015-2020).

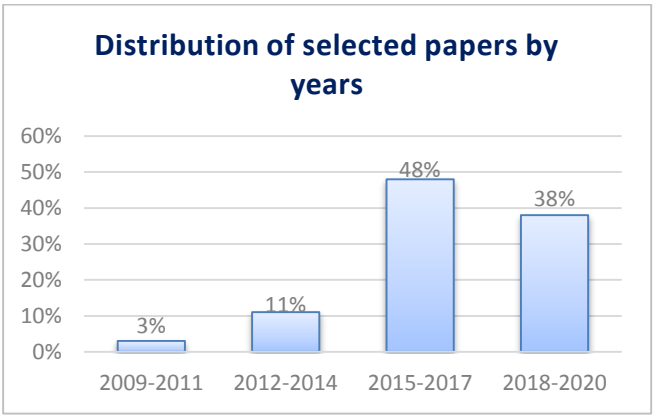

Fig. 2. Distribution of selected papers by years

III. IoT SECURITY

A. Background

The IoT is a system of interconnection between computing devices, machines, objects, animals and even people, equipped with unique identifiers with the ability to transfer data over a network. It uses built-in sensors, processors and communications hardware to send and collect data, as well as process the data it acquires from its environment [4]. The first IoT device was a Coca-Cola machine installed at Carnegie Mellon University in the 1980s, capable of reporting its stock levels through the ARPANET [5]. The IoT has continued to evolve over the years. It was in 2010 that mankind really began to want to connect all devices to the internet to simplify their daily lives. The IoT evolves and offers various applications in all areas, thus making life easier for people. There are many smart systems based on the IoT such as smart health care, smart transportation, smart homes, smart building, etc. Everything can be connected, you just have to find the right sensor that collects the data, the right connectivity that transmits it and the platform that returns it. IoT Analytics predicts that the number of active IoT devices globally is expected to grow from 8.3 billion in 2019 to 21.5 billion by 2025 [6] [7] (Fig. 3).

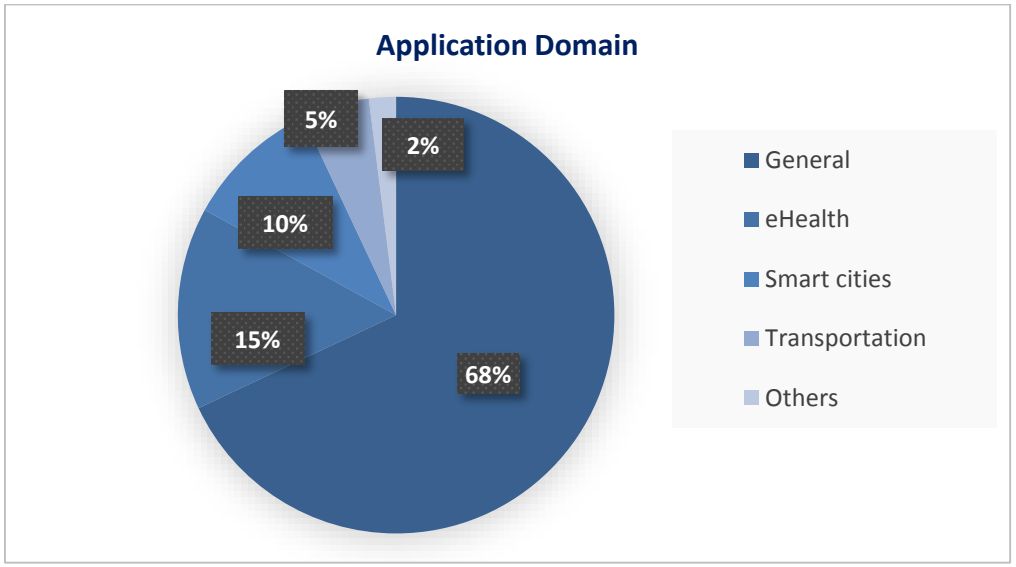

Fig. 3. Distribution of paper

Although it is already producing massive amounts of data, this is nothing compared to what will happen over the next decade. Given the various cyber-attacks and threats targeting IoT platforms, services and applications, cyber-security and privacy are considered among the top challenges and concerns for IoT that require to be addressed by research communities [8-10].

B. Generic architecture of IoT and security issues at each layer

There are several proposed IoT architectures [11-13], but the basic architecture consists of 4 layers, namely the perception, network, middleware and application layers, and despite the many contributions of researchers it remains still challenges and problems to be solved. To this end, it is very important to analyze, examine and resolve the multiple security issues in the different layers as shown in Table 2.

Table 2: IoT architecture and security issues

Application Layer User interface (Smart healthcare,smart transportation,etc)	This layer is an interface for users which is made up of different service areas such as (healthcare, smart homes, connected cars, etc.), so it offers users access to different IoT applications tailored to their needs.	This layer's security issues and challenges depend on the application area: Authentication security issues, data access, data protection and recovery, reliability issues, spear-phishing, cloning and social engineering [14-20].
Middleware Layer Data storage, analytics (Cloud computing, big data, etc)	This layer constitutes technologies such as cloud computing, big data processing and databases, and its role is therefore data storage and analysis.	This layer includes several data storage technologies, exposing it to huge cyber-attacks risks such as: DoS, jamming, unauthorized access, malicious insider, bad output, node modification, malicious-code attacks, handling suspicious information and multi-party authentication [21-25].
Network Layer Communication protocols, transmisión (Wi-Fi, Bluetooth,etc)	It is made up of different technologies such as (Wi-Fi, Bluetooth, etc.), and its role is to transmit the data collected via sensors to any system for processing and filtering.	There are still some vulnerabilities in the network layer despite the security measures it includes, which can expose it to multiple cyber-attacks such as: Spoofing, denial of service (DoS), eavesdropping, man-in-the-middle, sybil attack, cluster security problems, sinkhole attack, sleep deprivation attack, sniffing and altered or replayed routing information [26-32].
Perception Layer Physical devices, sensors (RFID, ZigBee, WSN, GPS, etc)	The perception or recognition layer consists of different types of sensors and actuators (RFID, ZigBee, WSN, GPS, etc.), which collect, detect and process the data collected from the environment and transmit them to the next layer which is the network layer.	This layer includes sensors whith limited storage and computing resources the fact that represents a major challenge. Collected data are transmitted over a wireless network exposing them to several security threats and attacks. This is mainly because physical devices have several vulnerabilities such as: Node capture, unauthorized Access to Tags, Tag cloning, differential power analysis (DPA), mass node authentication, fake node and malicious data, denial of service (DoS), eavesdropping, spoofing, routing attack, RF jamming, replay, and side-channel attack (SCA) [33-36].

C. IoT security challenges

The most important challenges for IoT can be summarized as follow:

Confidentiality: This is an IoT data security service that prevents unauthorized users from accessing confidential data. There are mechanisms and protocols that ensure the confidentiality of sensitive IoT data, such as: authentication, encryption, authorization [14, 15].

Authentication: Each node in the IoT must be able to authenticate other nodes and objects, and this is a security service that is very difficult compared to the heterogeneity of the IoT [16-27].

Availability: The main goal of IoT is to be able to connect everything and make everything available online, thus enabling users to have all IoT data available all the time [28].

Integrity: In IoT, data is exchanged between multiple devices, so it is mandatory to check if the data come from the right sender and go to the relevant IoT node without any intentional or unintentional interference [29].

Detection: The IoT system needs to be equipped with a detection mechanism to provide information on these devices in the event that there is a device failure within the network. It is therefore mandatory that these IoT systems can detect any loss of connectivity between devices [30].

Heterogeneity: There are many devices or sensors in the IoT belonging to different manufacturers with different capabilities depending on the complex or simple architecture [31].

Lightweight solutions: Knowing that IoT devices have very low computing power and memory capacity, traditional cryptographic algorithms do not apply to the IoT systems. Therefore, it is necessary to have powerful security mechanisms with low cost and minimal overhead [32].

D. IoT protocols and securtity

There are several IoT protocols for messaging, web transfer and other applications and features, including security and privacy, within IoT platforms such as Message Queue Telemetry Transport (MQTT) protocol and Constrained Application Protocol (CoAP). MQTT is a client-server protocol for messaging transport, which is easy to implement and works over TCP / IP [33, 34, 35, 36]. CoAP is a protocol used for Internet devices with limited resources at the application layer [37]. Advanced Message Queuing Protocol (AMQP) is a protocol that is designed for the transfer of business messages between applications. Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) is a protocol designed to protect private data by preventing tampering, eavesdropping, and forgery in communications [38]. It is based on TLS, which is a

protocol that used for computer communications networks security. Extensible Messaging and Presence Protocol (XMPP) is a protocol that is designed for instant messaging, and more generally for a decentralized data exchange architecture [36]. LoRaWAN is a wireless communication protocol, offering low data rate and low power consumption objects connected to the Internet via gateways using LoRa communication technology [39, 40]. IEEE 802.15.4 is a low-data rate wireless personal area network and is the PHY and MAC Layer used by many IoT protocols, such as ZigBee [36, 41, 42]. It is intended for wireless networks of the Low-Rate Wireless Personal Area Network (LR-WPAN) family due to their low power consumption, short range and low device speed.

IV. SOLUTIONS AND DISCUSSIONS

A. Blockchain for IoT

The IoT is a fast growing sector. Connected objects are multiplying to abysmal proportions, and so are security problems. Blockchain, which is a technology for storing and transmitting information that is transparent, secure, and operates without a central control body, could help solve these threats. The Blockchain is a decentralized / distributed network where everyone is connected to the others in one way or another, that is to say it constitutes a database that contains the history of all the exchanges carried out between its users since its creation. This database is secure and distributed: it is shared by its various users, without intermediaries, which allows everyone to check the validity of the chain [66, 67]. The blockchain thus makes it possible to record transactions, signatures ... in a register shared among all its users. The goal is to make sure that no one changes afterwards [68, 69]. The blockchain could therefore add a layer of security by adding a chain associated with the identity of the connected object [70]. Thus, this chain of identification will allow objects to interact with each other without having to communicate via a third party, thereby limiting information outputs or potential attacks from outside [71-73].

The Internet of Things brings huge opportunities in different areas, but also poses many security challenges and risks [74-76]. Many experts recognize that the IoT is above all a threat to user privacy [77, 78].

In this section of our SLR we analyze the most important solutions proposed, specifying the approach, limitations, layers concerned and domain as indicated in Table 2.

Table 3. Analysis of the security solutions in IoT

AUTHOR	PROPOSED SOLUTIONS	LIMITATIONS	LAYERS				DOMAIN	SECURITY ASPECT
			Perception Layer	Network Layer	Middle-ware Layer	Application Layer		
Li et al [79]	PKI-type security mechanism protocol as countermeasures to security threats on IoT nodes.	Limitation of energy, storage space.	Yes	No	No	No	General	Authentication
Aggarwal et al [80]	Radio Frequency Identification (RFID) security protocol, it is efficient in terms of computation and avoids the risks of disclosure and desynchronization.	Data eavesdropping, Privacy, Collision, Expensive, Compatibility.	Yes	No	No	No	RFID	Authentication
Chen et al [81]	Algorithm for detecting faulty sensors compromised in WSNs. This algorithm shows that it can identify faulty sensors with high precision.	Forgery attack, location privacy problem and replay attack.	Yes	No	No	No	General	Detection
Porambage et al [82]	Authentication and key establishment protocol for WSN in distributed IoT applications.	Data eavesdropping, Privacy problem, Time synchronization problem.	Yes	No	No	No	WSN	Authentication
Salami et al [83]	Lightweight Identity-Based Encryption System dedicated to smart homes.	Overhead of handling private key generator.	Yes	No	No	No	Smart homes	Lightweight solution
Raza et al [84]	End-to-End security mechanism for communication between the Internet and IP sensor networks.	DoS attack	No	Yes	No	No	General	Lightweight solution

AUTHOR	PROPOSED SOLUTIONS	LIMITATIONS	LAYERS				DOMAIN	SECURITY ASPECT
			Perception Layer	Network Layer	Middle-ware Layer	Application Layer		
Zhang et al [85]	A lightweight algorithm for the prevention of DDoS attacks in an IoT network.	Limitation of storage space.	No	Yes	No	No	General	Lightweight solution
Santos et al [86]	Security architecture based on mutual authentication using DTLS (Datagram Transport Layer) to secure communication between IoT devices.	DoS attack	No	Yes	No	No	General	Authentication
Salman et al [87]	An identity-based authentication scheme using SDN (Software Defined Networking) to integrate protocols into the IoT and address its heterogeneity.	Masquerade attack, replay attack, Man-in-the-middle attack	No	Yes	No	No	General	Authentication
Lui et al. [88]	Authentication and access control method for IoT correcting security holes and data integrity in devices.	Eavesdropping attack, , Man-in-the-middle attack	No	Yes	No	No	General	Authentication, Access control
Hummen et al [89]	A certificate-based authentication technique and lightweight security solutions to solve password authentication issues in IoT.	Overhead of certificate based authentication	No	Yes	No	No	General	Authentication, Lightweight solution
Tsai et al [90]	An efficient authentication scheme for distributed mobile cloud services.	Impersonation attack, Expensive	No	No	Yes	No	General	Authentication
Shafagh et al	Protect IoT data by processing	Expensive, limited	No	No	Yes	No	General	Access control

AUTHOR	PROPOSED SOLUTIONS	LIMITATIONS	LAYERS				DOMAIN	SECURITY ASPECT
			Perception Layer	Network Layer	Middle-ware Layer	Application Layer		
[91]	encrypted requests to store IoT data on the cloud database and enabling processing of requests on encrypted data.	with regards to energy, memory, CPU, and bandwidth.						
Horrow et al [92]	A cloud-based identity management framework for the Internet of Things.	The proposed architecture has not been implemented.	No	No	Yes	No	General	Authentication
Seitz et al [93]	A concept of access control and authorization that is flexible to IoT devices with very limited processing power and memory.	Resource constraints, Expensive.	No	No	No	Yes	General	Access control
Cirani et al [94]	An architecture called IoT-OAS offering an authorization framework targeting HTTP / CoAP services, implemented by invoking an external authorization service based on the oauth (OAS).	Limitation of storage space, DoS attack, Man-in-the-middle attack.	No	No	No	Yes	General	Access control
Cox and Balasingham [95]	A risk-based adaptive security framework for IoT in eHealth that will assess using game theory and context awareness techniques.	Prototyping has not been completed.	No	No	No	Yes	eHealth	Authentication, Detection, Privacy
Park et al [96]	A mutual authentication system and session key distribution framework to secure communication between IoT	The shared key is compromised.	No	No	No	Yes	General	Authentication

AUTHOR	PROPOSED SOLUTIONS	LIMITATIONS	LAYERS				DOMAIN	SECURITY ASPECT
			Perception Layer	Network Layer	Middle-ware Layer	Application Layer		
	devices.							
Tao et al [97]	A preference-based privacy protection mechanism for IoT	Not developed enough	No	No	No	Yes	General	Privacy
Weiss et al. [98]	A Comprehensive Comparative Metric (CCM) approach to providing security functionality is based on a risk management approach.	Accessibility and availability of the data is a challenge to measure security metrics.	No	No	No	Yes	General	Availability, Integrity
Neisse et al [99]	Security policy based on the SecKit model and its integration with the MQ Telemetry Transport (MQTT) protocol layer to enhance the security and privacy of IoT devices.	Battery constraints.	No	No	No	Yes	General	Privacy, Data protection
Pierre de Leusse et al. [100]	A Self-Managed Security Cells (SMSC) model, which is a scalable system for improving the security of distributed resources.	It is not yet validated for specific applications and security objectives.	No	No	No	Yes	General	Access control
Ali et al. [101]	Blockchain-based smart home Gateway network architecture for decentralization and security risk management.	The vulnerability of the gateway to a single point of failure.	No	No	Yes	No	Smart Home	Detection, Data protection, Integrity

We present in figure 5 a statistical study of the different solutions proposed by the researchers in Table 2 according to the security aspects.

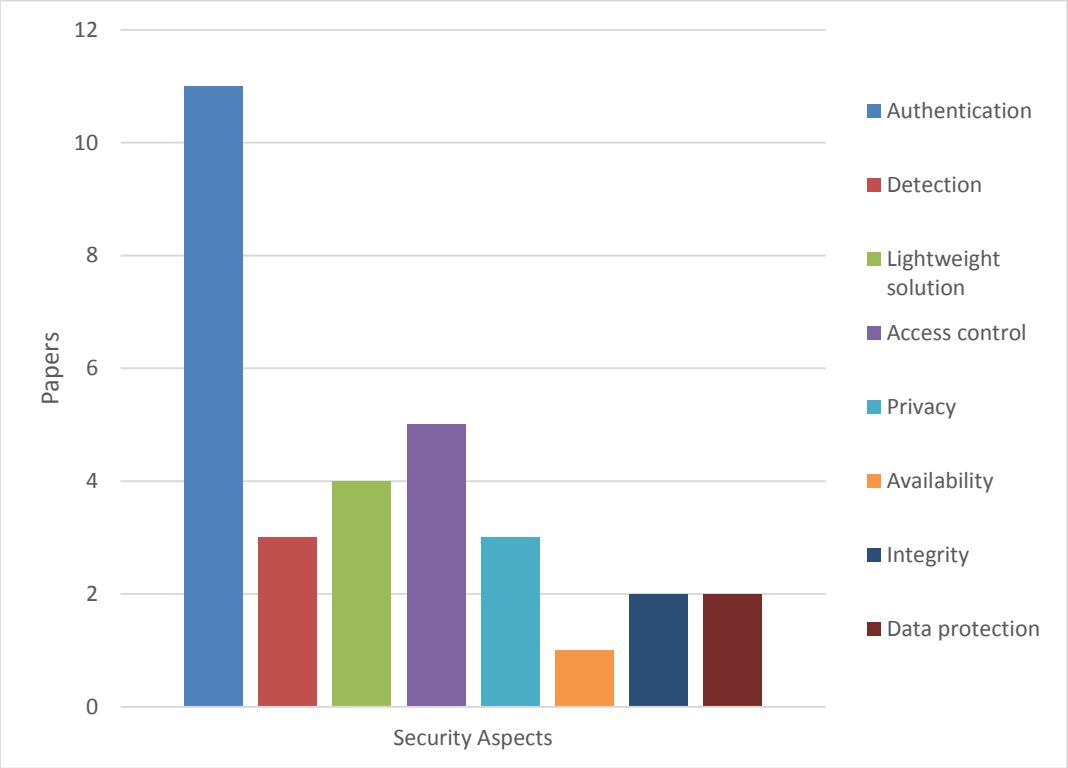

Fig. 5. Security aspects depending on the solutions proposed

V. IoT CYBERSECURITY FUTURE RESEARCH DIRECTION

In this section, we present future research directions regarding IoT security based on our SLR.

Application Domain: We can notice that the domains of application that are most requested by researchers are smart health care, smart transport, smart homes, smart cities and especially IoT security in general, however we need to approach and study the multitudes of other domains of application to extend the use of IoT.

Security issues and protocols: With the development of IoT new vulnerabilities appear like bad output, etc. However, we must examine them and propose solutions. Regarding the protocols, the most widely used are MQTT, CoAP, AMQP, DTLS, XMPP. It can also be seen from Table 2 that authentication is one of the security aspects most dealt with by researchers. Studying other protocols and security aspects could improve IoT security.

Security: Blockchain technology being a new paradigm of security, its integration with IoT would eliminate the risks and challenges that IoT faces. As a result, it becomes a research and production challenge for researchers. We are therefore studying the implementation of a blockchain-based architecture to strengthen the security of the IoT.

CONCLUSION

The security of the IoT has come under intense scrutiny after a number of incidents. The implementation of security measures is essential to ensure the security of IoT devices. In this SLR we find a presentation of the IoT including its security state, the general architecture of the IoT, the security challenges and protocols, the security issues of each layer of the architecture and also an analysis and a comparison of the most famous solutions proposed by researchers following several characteristics. According to this SLR we can notice the limits of the solutions proposed by the researchers and thus deduce the insecurity of its solutions. However, given the revolutionary promises of iot and its fields of application, it is important to offer more robust security solutions. This SLR could serve as a benchmark for new researchers in this field, providing a comprehensive view of IoT security, and future research direction.

DATA AVAILABILITY

No data were used to support the study.

CONFLICTS OF INTEREST

The authors declare that there are no conflicts of interest regarding the publication of this article.

FUNDING STATEMENT

There is no funding.

REFERENCES

[1] A. Amiruddin, A. A. P. Ratna, et R. F. Sari, « Systematic Review of Internet of Things Security », vol. 11, no 2, p. 8, 2019.

[2] Y. Yang, L. Wu, G. Yin, L. Li, H. Zhao, A survey on security and privacy issues in internet-of-things, IEEE Internet of Things Journal 4 (5) (2017) 1250–1258.

[3] M. A. Obaidat, S. Obeidat, J. Holst, A. Al Hayajneh, et J. Brown, « A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures », Computers, vol. 9, no 2, p. 44, mai 2020, doi: 10.3390/computers9020044.

[4] D. K. Alferidah et N. Jhanjhi, « A Review on Security and Privacy Issues and Challenges in Internet of Things », p. 23, 2020.

[5] IBM, The little-known story of the first IoT device, https://www.ibm.com/blogs/industries/little-known-story-first-iot-device/, accessed on 7 February 2018 (2018).

[6] J. Tournier, F. Lesueur, F. L. Mouël, L. Guyon, et H. Ben-Hassine, « A survey of IoT protocols and their security issues through the lens of a generic IoT stack », Internet of Things, p. 100264, juill. 2020, doi: 10.1016/j.iot.2020.100264.

[7] I. Yaqoob and al., "Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges", IEEE Wireless Communications, vol. 24, no 3, p. 10-16, juin 2017.

[8] A. Y. Khan, R. Latif, S. Latif, S. Tahir, and T. Saba, "Malicious Insider Attack Detection in IoTs Using Data Analytics," IEEE Access, vol. 8, pp. 11743-11753, Jan 2020.

[9] S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari, et A. Kashif Bashir, « A survey of security and privacy issues in the Internet of Things from the layered context », Trans Emerging Tel Tech, mars 2020, doi: 10.1002/ett.3935.

[10] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, B. Sikdar, A survey on iot security: Application areas, security threats, and solution architectures, IEEE Access 7 (2019) 82721–82743.

[11] F. Ali, M. Sulaiman Khan, et H. Akhtar, « Security Review in Internet of Things », IOTCC, vol. 7, no 3, p. 80, 2019, doi: 10.11648/j.iotcc.20190703.14.

[12] A. Tewari et B. B. Gupta, « Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework », Future Generation Computer Systems, vol. 108, p. 909‑920, juill. 2020, doi: 10.1016/j.future.2018.04.027.

[13] E. L. C. Macedo et al., « On the security aspects of Internet of Things: A systematic literature review », J. Commun. Netw., vol. 21, no 5, p. 444‑457, oct. 2019, doi: 10.1109/JCN.2019.000048.

[14] M. Barbosa et al., "SAFETHINGS: Data Security by Design in the IoT," 2017 13th European Dependable Computing Conference (EDCC), Geneva, 2017, pp. 117-120.

[15] Y. Atwady et M. Hammoudeh, « A Survey on Authentication Techniques for the Internet of Things », in Proceedings of the International Conference on Future Networks and Distributed Systems - ICFNDS '17, Cambridge, United Kingdom, 2017, p. 8, doi: 10.1145/3102304.3102312.

[16] A. Murzaeva, B. Kepçeoğlu, and S. Demirci, "Survey of Network Security Issues and Solutions for the IoT," 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), pp. 1-6, Oct 2019.

[17] K. B. C, and V. Alagappan, "The Internet of Things Model Architectures for Customized Applications: A Review," International Journal of Simulation: Systems, science, & technology, vol. 19, no. 6, Feb 2019.

[18] M. Burhan, R. A. Rehman, B. Khan, and B. Kim, "IoT Elements, Layered

Architectures and Security Issues: A Comprehensive Survey," Sensors, vol. 18, no. 9, Aug 2018.

[19] A. Assiri, and H. Almagwashi, "IoT Security and Privacy Issues," 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), pp. 1-5, Apr 2018.

[20] A. Diro, H. Reda, N. Chilamkurti, A. Mahmood, N. Zaman and Y. Nam, "Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication," in IEEE Access, vol. 8, pp. 60539-60551, 2020.

[21] Kraijak S, Tuwanut P. A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends. Paper presented at: Proceedings of the IEEE 16th International Conference on Communication Technology (ICCT); 2015:26-31; IEEE.

[22] M. Ahmad, T. Younis, M. A. Habib, R. Ashraf, et S. H. Ahmed, « A Review of Current Security Issues in Internet of Things », in Recent Trends and Advances in Wireless and IoT-enabled Networks, M. A. Jan, F. Khan, et M. Alam, Éd. Cham: Springer International Publishing, 2019, p. 11‑23.

[23] A. M. Nia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," IEEE Transactions on Emerging Topics in Computing, vol. PP, pp. 1-1, 2017.

[24] S. R. Moosavi, T. N. Gia, E. Nigussie, A. M. Rahmani, S. Virtanen, H. Tenhunen, et al., "Session Resumption-Based End-to-End Security for Healthcare Internet-of-Things," in 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, pp. 581- 588, 2015.

[25] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," Journal of Network and Computer Applications, vol. 88, pp. 10-28, 2017.

[26] A. Mathur, T. Newe, W. Elgenaidi, M. Rao, G. Dooly, and D. Toal, "A secure end-to-end IoT solution," Sensors and Actuators A: Physical, vol. 263, pp. 291-299, 2017.

[27] L. Nastase, "Security in the Internet of Things: A Survey on Application Layer Protocols," in 2017 21st International Conference on Control Systems and Computer Science (CSCS), pp. 659-666, 2017.

[28] Kraijak, S., & Tuwanut, P. (2015). A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends, 6–6.

[29] S. Tomasin, S. Zulian, and L. Vangelista, "Security Analysis of LoRaWAN Join

Procedure for Internet of Things Networks," in 2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), pp. 1-6, 2017.

[30] A. K. Das, S. Zeadally, D. He, Taxonomy and analysis of security protocols for internet of things, Future Generation Computer Systems 89 (2018) 110–125.

[31] S. Tomasin, S. Zulian, and L. Vangelista, "Security Analysis of LoRaWAN Join Procedure for Internet of Things Networks," in 2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), pp. 1-6, 2017.

[32] S. Sahraoui and A. Bilami, "Efficient HIP-based approach to ensure lightweight end-to-end security in the internet of things," Computer Networks, vol. 91, pp. 26-45, 2015.

[33] P. P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, and X. Yi, "Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation," Future Generation Computer Systems, vol. 76, pp. 540-549, 2017.

[34] M. Vučinić, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, "OSCAR: Object security architecture for the Internet of Things," Ad Hoc Networks, vol. 32, pp. 3-16, 2015.

[35] B.-C. Chifor, I. Bica, V.-V. Patriciu, and F. Pop, "A security authorization scheme for smart home Internet of Things devices," Future Generation Computer Systems, 2017.

[36] R. D. Chamberlain, M. Chambers, D. Greenwalt, B. Steinbrueck, and T. Steinbrueck, "Layered Security and Ease of Installation for Devices on the Internet of Things," in 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI), pp. 297-300, 2016.

[37] Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266–2279.

[38] S. N. Matheu, J. L. Hernandez-Ramos, A. F. Skarmeta, Toward a cybersecurity certification framework for the internet of things, IEEE Security & Privacy 17 (3) (2019) 66–76.

[39] S. Muthuramalingam, A. Bharathi, N. Gayathri, R. Sathiyaraj, B. Balamurugan, et al., IoT based intelligent transportation system IoT-ITS for global perspective: A case study, in: Internet of Things and Big Data Analytics for Smart Generation, Springer, 2019, pp. 279–300.

[40] P. H. Griffin, "Security for Ambient Assisted Living: Multifactor Authentication in the Internet of Things," in 2015 IEEE Globecom Workshops (GC Wkshps), pp. 1-5, 2015.

[41] P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang, and X. Yao, "Security and Privacy

Preservation Scheme of Face Identification and Resolution Framework Using Fog Computing in Internet of Things," IEEE Internet of Things Journal, vol. PP, pp. 1-1, 2017.

[42] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog Computing for the Internet of Things: Security and Privacy Issues," IEEE Internet Computing, vol. 21, pp. 34-42, 2017.

[43] H. Lee;, O. Na;, Y. Kim;, and H. Chang, "A Study on Designing Public Safety Service for Internet of Things Environment," Wireless Personal Communication, vol. 93, pp. 447–459, 2017.

[44] P. A. H. Williams and V. McCauley, "Always connected: The security challenges of the healthcare Internet of Things," in 2017 IEEE 3rd World Forum on Internet of Things (WF-IoT), pp. 30-35, 2016.

[45] D. Mukhopadhyay, "PUFs as Promising Tools for Security in Internet of Things," IEEE Design & Test, vol. 33, pp. 103- 115, 2016.

[46] P. K. Dhillon and S. Kalra, "A lightweight biometrics based remote user authentication scheme for IoT services," Journal of Information Security and Applications, vol. 34, pp. 255- 270, 2017.

[47] Bhabad Mayuri A, Bagade ST. Internet of things: architecture, security issues and countermeasures. Int J Comput Appl. 2015;125(14).

[48] K. Fazal, H. Shehzad, A. Tasneem, A. Dawood, and Z. Ahmed, ‘‘A systematic literature review on the security challenges of Internet of Things and their classification,’’ Int. J. Technol. Res., vol. 5, no. 2, pp. 40–48, 2017.

[49] P. I. Radoglou Grammatikis, P. G. Sarigiannidis, et I. D. Moscholios, « Securing the Internet of Things: Challenges, threats and solutions », Internet of Things, vol. 5, p. 41‑70, mars 2019, doi: 10.1016/j.iot.2018.11.003.

[50] Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis on the security concerns of internet of things (IoT). International Journal of Computer Applications, 111(7), 1–6.

[51] B. K. Mohanta, D. Jena, U. Satapathy, et S. Patnaik, « Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology », Internet of Things, vol. 11, p. 100227, sept. 2020, doi: 10.1016/j.iot.2020.100227.

[52] E. Ahmed, I. Yaqoob, I. A. T. Hashem, I. Khan, A. I. A. Ahmed, M. Imran, et al., "The role of big data analytics in Internet of Things," Computer Networks, 2017.

[53] B. C. Chifor, I. Bica, and V. V. Patriciu, "A Participatory Verification security scheme for the Internet of Things," in 2016 International Conference on Communications (COMM), pp. 267-270, 2016.

[54] R. A. Gheorghiu and V. Iordache, "Analysis of the Possibility to Implement ZigBee Communications in Road Junctions," Procedia Engineering, vol. 181, pp. 489-495, 2017.

[55] A. Punia, D. Gupta and S. Jaiswal, "A perspective on available security techniques in IoT," 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, 2017, pp. 1553-1559.

[56] M. Hayashi, and Á. Vázquez-Castro, "Physical Layer Security Protocol for Poisson Channels for Passive Manin-the-Middle Attack," EEE Transactions on Information Forensics and Security, vol. 15, pp. 2295-2305, Jan 2020.

[57] Z. A. Baig, S. Sanguanpong, S. N. Firdous, T. G. Nguyen, C. So-In, et al., Averaged dependence estimators for dos attack detection in IoT networks, Future Generation Computer Systems 102 (2020) 198–209.

[58] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2483-2495, Aug 2018.

[59] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of Things (IoT): Taxonomy of security attacks," in 2016 3rd International Conference on Electronic Design (ICED), pp. 321-326, 2016.

[60] P.Anu, and Dr.S.Vimala, "A survey on sniffing attacks on computer networks," 2017 International Conference on Intelligent Computing and Control (I2C2), pp. 1-5, June 2017.

[61] Razouk W, Sgandurra D, Sakurai K. A new security middleware architecture based on fog computing and cloud to support IoT constrained devices. Paper presented at: Proceedings of the 1st International Conference on Internet of Things and Machine Learning; 2017:35; ACM.

[62] B. C. Chifor, I. Bica, and V. V. Patriciu, "A Participatory Verification security scheme for the Internet of Things," in 2016 International Conference on Communications (COMM), pp. 267-270, 2016.

[63] Kumar SA, Vealey T, Srivastava H. Security in internet of things: challenges, solutions and future directions. Paper presented at: Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS); 2016:5772-5781; IEEE.

[64] L. Malina, J. Hajny, R. Fujdiak, and J. Hosek, "On perspective of security and privacy-preserving solutions in the internet of things," Computer Networks, vol. 102, pp. 83-95, 2016.

[65] Ishu1, V. Lohan, P. Gupta, D. Goyal, and M. Goyal, "To Review the Concept of Security in Internet of Things," International Journal of Computer Science &

Management Studies (IJCSMS), vol. 39, no. 1, Jun 2018.

[66] M. Khan, and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” Future Generation Computer Systems, vol. 82, pp. 395–411, May 2018.

[67] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, “A Survey of IoT Applications in Blockchain Systems: Architecture, Consensus, and Traffic Modeling,” ACM Computing Surveys, vol. 53, no. 1, Feb 2020.

[68] A. Dorri, S. S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: The case study of a smart home, in: 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops), IEEE, 2017, pp. 618–623.

[69] S. Dhar et I. Bose, « Securing IoT Devices Using Zero Trust and Blockchain », Journal of Organizational Computing and Electronic Commerce, p. 1‑17, nov. 2020, doi: 10.1080/10919392.2020.1831870.

[70] A. Reyna, C. Mart´ın, J. Chen, E. Soler, M. D´ıaz, On blockchain and its integration with IoT. challenges and opportunities, Future Generation Computer Systems 88 (2018) 173–190.

[71] V. Dedeoglu, R. Jurdak, A. Dorri, R. Lunardi, R. Michelin, A. Zorzo, S. Kanhere, Blockchain technologies for iot, in: Advanced Applications of Blockchain Technology, Springer, 2020, pp. 55–89.

[72] B. K. Mohanta, D. Jena, U. Satapathy, et S. Patnaik, « Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology », Internet of Things, vol. 11, p. 100227, sept. 2020, doi: 10.1016/j.iot.2020.100227.

[73] M. Anwer, A. saad, et A. Ashfaque, « Security of IoT Using Block chain: A Review », in 2020 International Conference on Information Science and Communication Technology (ICISCT), KARACHI, Pakistan, févr. 2020, p. 1‑5, doi: 10.1109/ICISCT49550.2020.9079943.

[74] Y. Perwej, F. Parwej, M. M. Mohamed Hassan, et N. Akhtar, « The Internet-of-Things (IoT) Security : A Technological Perspective and Review », IJSRCSEIT, p. 462‑482, févr. 2019, doi: 10.32628/CSEIT195193.

[75] S. M. Mohammad, « Security and Privacy Concerns of the „Internet of Things“ (IoT) in IT and its Help in the Various Sectors across the World », IJCTT, vol. 68, no 4, p. 266‑272, avr. 2020, doi: 10.14445/22312803/IJCTT-V68I4P142.

[76] Mohab Aly, Foutse Khomh, Mohamed Haoues, Alejandro Quintero, Soumaya Yacout, Enforcing security in Internet of Things frameworks: A Systematic Literature Review, Internet of Things, Volume6, 2019, 100050, ISSN25426605, https://doi.org/10.1016/j.iot.2019.100050.

[77] Farhan Ali, He Yigang, and Ruan Yi, "A Novel Security

Architecture of Internet of Things," International Journal of Computer Theory and Engineering vol. 11, no. 5, pp. 89-96, 2019. DOI: 10.7763/IJCTE.2019. V11.1249.

[78] M. Abdur Razzaq, M. A. Qureshi, S. H. Gill, and S. Ullah, "Security Issues in the Internet of Things (IoT): A Comprehensive Study," International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 8, No. 6, pp. 383-388, Jan 2017.

[79] Zhihua Li et al., « Research on PKI-like Protocol for the Internet of Things », in 2013 Fifth International Conference on Measuring Technology and Mechatronics Automation, Hong Kong, janv. 2013, p. 915-918, doi: 10.1109/ICMTMA.2013.227.

[80] R. Aggarwal et M. L. Das, « RFID security in the context of "internet of things" », in Proceedings of the First International Conference on Security of Internet of Things - SecurIT '12, Kollam, India, 2012, p. 51‑56, doi: 10.1145/2490428.2490435.

[81] J. Chen, S. Kher, et A. Somani, « Distributed fault detection of wireless sensor networks », in Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks - DIWANS '06, Los Angeles, CA, USA, 2006, p. 65, doi: 10.1145/1160972.1160985.

[82] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, et M. Ylianttila, « PAuthKey: A Pervasive Authentication Protocol and Key Establishment Scheme for Wireless Sensor Networks in Distributed IoT Applications », *International Journal of Distributed Sensor Networks*, vol. 10, nº 7, p. 357430, juill. 2014, doi: 10.1155/2014/357430.

[83] S. Al Salami, J. Baek, K. Salah, et E. Damiani, « Lightweight Encryption for Smart Home », in 2016 11th International Conference on Availability, Reliability and Security (ARES), Salzburg, août 2016, p. 382‑388, doi: 10.1109/ARES.2016.40.

[84] S. Raza, S. Duquennoy, T. Voigt, et U. Roedig, « Demo abstract: Securing communication in 6LoWPAN with compressed IPsec », in 2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS), Barcelona, Spain, juin 2011, p. 1‑2, doi: 10.1109/DCOSS.2011.5982146.

[85] C. Zhang et R. Green, « Communication Security in Internet of Thing: Preventive Measure and Avoid DDoS Attack Over IoT Network », p. 9.

[86] G. Lessa dos Santos, V. T. Guimaraes, G. da Cunha Rodrigues, L. Z. Granville, et L. M. R. Tarouco, « A DTLS-based security architecture for the Internet of Things », in 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, juill. 2015, p. 809‑815, doi: 10.1109/ISCC.2015.7405613.

[87] O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab, et A. Kayssi, « Identity-based

authentication scheme for the Internet of Things », in 2016 IEEE Symposium on Computers and Communication (ISCC), Messina, Italy, juin 2016, p. 1109‑1111, doi: 10.1109/ISCC.2016.7543884.

[88] J. Liu, Y. Xiao, et C. L. P. Chen, « Authentication and Access Control in the Internet of Things », in 2012 32nd International Conference on Distributed Computing Systems Workshops, Macau, China, juin 2012, p. 588‑592, doi: 10.1109/ICDCSW.2012.23.

[89] Hummen R, Ziegeldorf JH, Shafagh H, Raza S, Wehrle K. Towards viable certificate-based authentication for the internet of things. Paper presented at: Proceedings of the 2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy; 2013:37-42; ACM.

[90] J.-L. Tsai et N.-W. Lo, « A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services », IEEE Systems Journal, vol. 9, no 3, p. 805‑815, sept. 2015, doi: 10.1109/JSYST.2014.2322973.

[91] H. Shafagh, A. Hithnawi, A. Droescher, S. Duquennoy, et W. Hu, « Talos: Encrypted Query Processing for the Internet of Things », in Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems - SenSys '15, Seoul, South Korea, 2015, p. 197‑210, doi: 10.1145/2809695.2809723.

[92] S. Horrow et A. Sardana, « Identity management framework for cloud based internet of things », in Proceedings of the First International Conference on Security of Internet of Things - SecurIT '12, Kollam, India, 2012, p. 200‑203, doi: 10.1145/2490428.2490456.

[93] L. Seitz, G. Selander, et C. Gehrmann, « Authorization framework for the Internet-of-Things », in 2013 IEEE 14th International Symposium on « A World of Wireless, Mobile and Multimedia Networks » (WoWMoM), Madrid, juin 2013, p. 1‑6, doi: +10.1109/WoWMoM.2013.6583465.

[94] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, et G. Ferrari, « IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios », IEEE Sensors J., vol. 15, no 2, p. 1224‑1234, févr. 2015, doi: 10.1109/JSEN.2014.2361406.

[95] H. Abie et I. Balasingham, « Risk-Based Adaptive Security for Smart IoT in eHealth », présenté à 7th International Conference on Body Area Networks, Oslo, Norway, 2012, doi: 10.4108/icst.bodynets.2012.250235.

[96] N. Park et N. Kang, « Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle », Sensors, vol. 16, no 1, p. 20, déc. 2015, doi: 10.3390/s16010020.

[97] H. Tao et W. Peiran, « Preference-Based Privacy Protection Mechanism for the Internet of Things », in 2010 Third International Symposium on Information Science and Engineering, Shanghai, China, déc. 2010, p. 531‑534, doi: 10.1109/ISISE.2010.135.

[98] S. Weiß, O. Weissmann, et F. Dressler, « A Comprehensive and Comparative Metric for Information Security », p. 10.

[99] R. Neisse, G. Steri, et G. Baldini, « Enforcement of security policy rules for the Internet of Things », in 2014 IEEE 10th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Larnaca, Cyprus, oct. 2014, p. 165‑172, doi: 10.1109/WiMOB.2014.6962166.

[100] P. de Leusse, P. Periorellis, T. Dimitrakos, et S. K. Nair, « Self Managed Security Cell, a Security Model for the Internet of Things and Services », in 2009 First International Conference on Advances in Future Internet, Athens, juin 2009, p. 47‑52, doi: 10.1109/AFIN.2009.15.

[101] Jawad Ali, Ahmad Shahrafidz Khalid, Eiad Yafi, Shahrulniza Musa, and Waqas Ahmed. Towards a secure behavior modeling for iot networks using blockchain. arXiv preprint arXiv:2001.01841, 20