IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 16, 2020, accepted December 6, 2020, date of publication December 22, 2020,
date of current version December 31, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3046442

A Comprehensive Study of the IoT Cybersecurity in Smart Cities

ROBERTO OMAR ANDRADE[1], (Member, IEEE), SANG GUUN YOO[1,2], (Senior Member, IEEE), LUIS TELLO-OQUENDO[3], (Member, IEEE), AND IVÁN ORTIZ-GARCÉS[4]

[1]Facultad de Ingeniería de Sistemas, Escuela Politécnica Nacional, Quito 170525, Ecuador
[2]Smart Lab, Escuela Politécnica Nacional, Quito 170525, Ecuador
[3]College of Engineering, Universidad Nacional de Chimborazo, Riobamba 060108, Ecuador
[4]Faculty of Engineering and Applied Sciences, Universidad de las Américas, Quito 170122, Ecuador

Corresponding author: Iván Ortiz-Garcés (ivan.ortiz@udla.edu.ec)

ABSTRACT Smart cities exploit emerging technologies such as Big Data, the Internet of Things (IoT), Cloud Computing, and Artificial Intelligence (AI) to enhance public services management. The use of IoT allows detecting and reporting specific parameters related to different domains of the city, such as health, waste management, agriculture, transportation, and energy. LoRa technologies, for instance, are used to develop IoT solutions for several smart city domains thanks to its available features, but sometimes people (i.e., citizens, information technology administrators, or city managers) might think that these available features involve cybersecurity risks. This study explores the cybersecurity aspects that define an assessment model of cybersecurity maturity of IoT solutions to develop smart city applications. In that sense, we perform a systematic literature review based on a top-down approach of cybersecurity incident response in IoT ecosystems. Besides, we propose and validate a model based on risk levels to evaluate the IoT cybersecurity maturity in a smart city.

INDEX TERMS Bayesian network, cybersecurity, IoT, maturity model, risk assessment, smart city.

I. INTRODUCTION

The cities try to maintain their sustainability and resilience capabilities in front of social, environmental, technological, and economic changes inherent to human evolution. Cities face more significant pollution, more traffic congestion, higher demand for energy and sanitation services due to urban growth. To resolve the problems associated with urbanization, the cities should incorporate *smart* solutions that involve human capital, creativity, and collaboration with various stakeholders [1]. For this reason, several cities in the world have adopted the development an urban planning model called *smart city* based on the digitization of services, automation of processes, and data-based decision making [2].

Adopting *smart city* model allows cities to improve the city's administrative and operational processes, aiming to generate sustainable environments for citizens. The smart city model includes a sensing layer and data analytics processes to understand in real-time the patterns of the city services in different areas such as health, energy, transport, waste management, and environment. In recent years, the development of smart cities has been supported by the evolution of communication systems and the inclusion of emerging technologies such as the Internet of Things (IoT), Big Data, and Cloud Computing [3]–[5]. The integration of these technologies and their direct application to the urban space has promoted urban computing development. Today, sensors, persons, vehicles, buildings, among other elements of the urban space, can be used as components for providing service to people and the city [1].

From a technical perspective, the smart city could be considered as a model to abstract the physical and behavioral aspects of the different elements of the city (citizens, services, and physical infrastructure) to the digital environment through the interoperability of technological subsystems made up of sensors, actuators, and processing capabilities. This allows identifying patterns of the city's social, environmental, and economic aspects for executing real-time decision-making by the city's actors to maintain the city's sustainability and resilience. Related to the objective of digitization of the physical aspects of a city, IoT especially allows obtaining data of several parameters and components of it; for instance, it is feasible to obtain the temperature of a house, the air quality on the streets, or the humidity in an agricultural plantation [6]–[8]. IoT solutions are increasing worldwide, and the projections related to IoT for the following years

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Huang.

are still promising. The number of IoT devices is expected to grow between 25 to 30 billion by 2022 [9]. Gartner indicates that only in the automotive sector, IoT presents a 21% increase by 2020 compared to 2019; this represents 5.1 billion endpoints more in the world [10]. Nevertheless, IoT solutions have fueled economic growth and have also contributed to social, environmental, and commercial aspects. According to the World Economic Forum, IoT projects have contributed to the 17 sustainable development goals (SDG) [11]. This hyper-connectivity and continuous availability of IoT solutions allow the development of smart cities, but they also increment cybersecurity threats and attacks [12]. A Forbes analysis of security events shows that cyberattacks on IoT devices increased by around 300 % in 2019, and according to Hassija [13], the development of IoT solutions raised privacy and security issues. Some cyberattacks that can occur in a smart city are:

- Controlling traffic lights: attackers can manage city lights causing accidents; traffic signals have become susceptible to attacks because of wireless networks [14];
- Attacks against smart vehicles: attackers can inject false routes or simulate other vehicles in the environment to cause collisions [15];
- Collapsing the power grid: attackers can cause power outage in the city [16];
- Water supply: attackers can modify the levels of chemical additives in the water and cause public health problems [17];
- Surveillance cameras: attackers can spy on people and access to personal data [18].

Cities have been targets of security attacks worldwide for some years. For example, in 2015, Kyiv (a Ukraine city) had a power outage caused by cyberattacks; this deprived the people of electricity for one hour approximately [19]. In 2019, the city of Baltimore, USA, was attacked with ransomware infecting the city government's computers and demanding 13 bitcoins in exchange for encrypted files [20]. When cities lose control of their systems due to cyberattacks, it can impact the technological axis, the city's economy, quality of life, and even more, can put in danger people's lives. The inclusion of information and communication technologies (ICTs) has generated concerns for citizens regarding security. Cybersecurity aspects could be one of the limitations in the use of smart city services. Citizens could prefer, in some instances, do not use technological resources for the city services. The study developed by Lytras and Visvizi [21] identified seven factors that are concerned by citizens in the smart city adoption with their corresponding percentages (see Fig. 1). According to such a study, citizens' main concerns are security and protection with 45%, data privacy with 25%, and transparency of services with 8%. The other concerns are equal or below to 5%.

In this context, city managers should consider strategies to improve cybersecurity mechanisms (e.g., policies, guidelines, controls) and support strengthening cybersecurity in the smart city domain. Under this premise, we have raised the following research question at a macro level that motivates the development of this study: *Is there an adequate IoT cybersecurity level for smart city scenarios?*

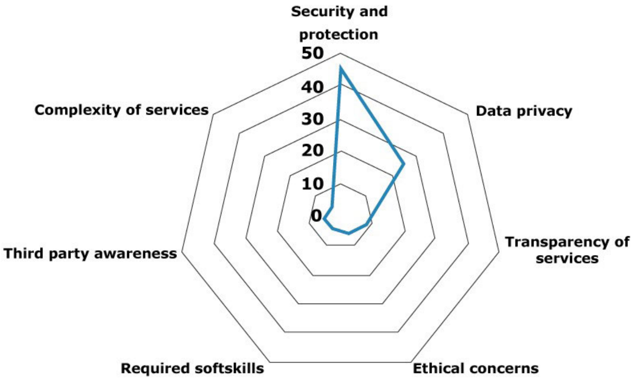

FIGURE 1. Concerns associated with smart city adoption.

Six important pillars of smart cities are the social impact, cognitive intelligence, policy awareness, benchmarking and best practices, smart cities ecosystem, and creation and innovation [1]. This context raises our second research question in this study: *Does IoT cybersecurity level affect to the key pillars of the smart city?*

This study aims to analyze the cybersecurity state from a perspective of IoT inclusion in smart city scenarios. For this, we first performed a systematic literature review (SLR) that allows establishing a baseline to evaluate the cybersecurity maturity of IoT solutions used in a smart city. Then, we propose a Cybersecurity Maturity Model for a smart city based on five phases: (i) Research context, (ii) Design strategy framework, (iii) Conceptualization and specification framework, (iv) Mapping features of the cybersecurity maturity model based on expert panel ranking, and (v) Validation of the initial cybersecurity maturity model. The proposed model aims to cover the cybersecurity aspects produced by the inclusion of IoT to develop the smart city, contemplating the economic, social, and environmental impacts. Applying the cognitive security techniques will allow assessing cybersecurity risk levels in the face of complexity, diversity, and large volumes of data in IoT ecosystems.

The remainder of this paper is structured as follows. Section II presents an overview of works related to the issues of cybersecurity in IoT ecosystems within smart cities. Section III presents the research methodology of the SLR and qualitative analysis. Section IV presents an analysis of the results obtained from the SLR to determine the main aspects of cybersecurity to assess the IoT usage in smart city applications and then discusses cybersecurity proposals for IoT in smart cities. Section V introduces the cybersecurity maturity model development for a smart city. Finally, Section VI concludes this study.

II. OVERVIEW OF CYBERSECURITY IN IoT ECOSYSTEMS

IoT devices communicate among them, using various communication technologies and different kinds of protocols. In IoT ecosystems, the application of cybersecurity methodologies has some challenges due to this heterogeneity. Additionally, the physical capacity of IoT devices and the amount of information generated by IoT devices increase the challenge of cybersecurity.

Attackers take advantage of vulnerabilities to execute cyber-attacks. Recent attacks have taken advantage of IoT systems' vulnerabilities in smart cities. Liu *et al.* [22] identified five primary layers in the IoT system susceptible to vulnerabilities: the network layer, the operating system, software, firmware, and hardware. Capellupo *et al.* [23] mention that IoT devices are compromised because they have default configurations, easy passwords, and unencrypted traffic. Vulnerabilities related to default or trivial passwords in IoT devices that are publicly visible can be detected using tools like SHODAN [24]; this increases the number of attacks. Yu *et al.* [25] mention that the firmware identification method to detect the device type and brand of IoT solutions could be based on weak passwords. English *et al.* [26] contribute to this field, indicating that attackers could develop memory buffer attacks to gain access to the entire system using weak default passwords. Hsu *et al.* [27] mention that an attacker could trigger a privilege escalation attack to change the behavior of IoT systems. IoT systems generally use rules for developing specific actions, but the attacker could manipulate these rules to affect the IoT device. Mishra and Dixit [28] suggest that if an attacker gains access to an IoT device, he/she could obtain privileged information. If the device is part of a mesh network, the attacker could compromise the entire network's confidentiality. Benkahla *et al.* [29] mention that the attacker could take advantage of services implemented in the IoT ecosystem using the spoofing attack. The problem is that the elements' identity is unprotected and transmitted while registering the devices in the server. Benkahla also suggests that some IoT networks (i.e., LoRa Network) can suffer from flipping attacks where the message is modified without being decrypted and can disable data transmission. Ling *et al.* [30] developed a case study for a smart plug system and identified four possible types of attacks to gain access to the entire system: device scanning attack, brute force attack, spoofing attack, and firmware attack.

According to Moustafa *et al.* [31], IoT services operate via network protocols, such as DNS, HTTP, and MQTT, and attackers try to exploit vulnerabilities in such protocols using techniques like polymorphic code, DNS Spoofing, DNS cache poisoning, Denial of Service (DoS), Distributed DoS (DDoS) and URL interpretation. Metongnon and Sadre [32] mention that attackers can obtain successful login on telnet, and once they reached this goal, they can write shellcodes or download script files containing commands. Additionally, IoT solutions consider UPnP for automatic discovering IoT devices connected to a network [33], but this service can become a vulnerability since an attacker can get important information using the UPnP's service discovery protocol [32]. Iacono *et al.* [34] mention that API-keys share the same drawbacks as HTTP basic authentication. The API-key is transferred to the server in plain-text. Additionally, Iacono comments that OAuth v2 (an authorization framework for granting access to end-users' resources for third party applications) does not include any security on its own; instead, the security is merely based on TLS. However, OAuth v2 can be augmented through the OAuth MAC tokens by extending a method for signing an HTTP request. OAuth is used to reduce user privacy exposure, but OAuth v2 could have security vulnerabilities taken advantage of by attackers through replay attacks and Cross-Site Request Forgery (CSRF) [35].

Table 1 shows some relations to explain how attack vectors take advantage of IoT vulnerabilities. The IoT vulnerabilities were selected based on the OWASP IoT Top Ten attacks classification and security requirements of OWASP Application Security Verification Standard.

It is worth noting that the IoT ecosystem is complemented by data analytics and cloud solutions to generate information for decision-making. Nowadays, Microsoft Azure, Google Cloud, or Amazon AWS are the most recognized cloud platforms in the field due to their easy integration with IoT solutions. However, despite being robust commercial solutions, they expand the surface of cybersecurity attacks. Cloud solutions present a shared security management scheme; on the one hand, cloud companies are responsible for securing the infrastructure, storage, and cloud networks. On the other hand, the user or client is responsible for other aspects such as authentication, authorization, or continuous monitoring. In August 2019, there was an attack in which customer data was stolen from a bank cloud infrastructure. It was said that a misconfiguration error at the application layer caused the problem allowing a Server-Side Request Forgery (SSRF) attack. However, the judicial process investigation revealed that there were default configurations that could enable this type of attack [39]. As can be seen, the interaction of various actors increases the complexity of the cybersecurity strategy. In this aspect, it is essential to consider the aspect of a shared security scheme generated by the use of cloud infrastructure to analyze security risks. Figure 2 illustrates the most relevant security problems that we have identified in our complementary study about cloud environments that can be used in conjunction with IoT. The attack vectors expand the attack surface in a smart city.

The metadata on cloud services gives information about a computational instance, e.g., service name or security group that retrieves a cloud resource. This metadata may contain sensitive information, so it is essential not to have information such as a password because it would allow attackers to access resources more quickly. Attackers seek to identify credentials in the metadata using the SSRF vulnerability in the public frontend. A misconfiguration can allow an attacker to access cloud resources, read or overwrite configurations, and access sensitive data. Misconfigurations can occur in both the cloud components and the configuration of third-party solutions used in the cloud (e.g., GitHub or dockers). Errors such as not activating the multiple-factor authentication, not using encryption, or having credentials in files of local directories of the systems can allow the attacks to succeed.

TABLE 1. Attack vectors based on IoT vulnerabilities.

Security requirements	Vulnerability	Attack vector	IoT Layer	Owasp Classification	Ref.
Authentication	Lack of the implementation of cryptographic algorithms. Lack of password policy management. The average password length on IoT devices is short. Bypassing authentication and authorization. Default passwords and credentials.	Attacker can discover the password using brute force or dictionary attacks. Attacker can eavesdrop the wireless communication. Attacker can gather configuration and authentication credentials from a non-tamper-proofed node, and can replicate it in the network. Impersonation attack in which an adversary is disguised as a legitimate party in the system. Device scanning attack.	Device Layer	Weak, Guessable, or Hard-coded password	[23]–[26], [36], [37]
Access Control	Bypassing access control checks Misconfiguration. Metadata manipulation. Elevation of privilege.	Attacker can emulate the communication behavior of a real IoT node (Spoofing attacks). The attacker can install a malicious firmware on the IoT device and control it remotely.	Device Layer. Network Layer.	Insufficient Authentication or Authorization. Insecure Software and Firmware.	[27]–[30]
Input and Output	Vulnerabilities on HTTP, Telnet and DNS.	DNS Spoofing, DNS cache poisoning, Denial of Service (DoS), Distributed DoS (DDoS) and URL interpretation	Application Layer.	Insecure Network Services.	[31]
Communications	Vulnerabilities on MQTT, CoAP, UPnP, and HNAP.	MQTT does not provide any data encryption by default. The attacker can sniff the data in transit.	Service Layer.	Insecure Network Services.	[32]
Cryptographic	Communication protocols do not rely on cryptographic mechanisms.	Eavesdropping attacks allow to analyze plain-text transmissions between IoT nodes.	Network layer.	Lack of Encryption and Integrity Verification.	[30]
APIs	Security misconfiguration improper asset management security injection access exposure to data broken authentication.	Replay attacks and Cross-Site Request Forgery (CSRF)	Service layer.	Insecure Network Services.	[38]

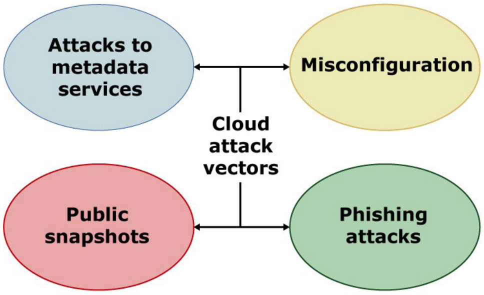

FIGURE 2. Security problems in cloud environments.

By default, a cloud resource's information is private, but users may allow the information to be accessible. Some errors are related to the snapshot's publication in an open way that will allow the attacker to access the information. Attackers can send fake emails trying to get credentials from cloud resources, bypassing security protections such as firewalls, since they could generate exceptions or install some malware. Table 2 presents the security techniques that cloud providers offer to reduce security vulnerabilities.

From this review, we can observe that security problems look for having a more significant extension than the platforms' security configuration. It is essential to use a Role-based Access Control (RBAC) to access cloud resources. This prevents unauthorized users from accessing sensitive data. Access policies must be configured appropriately, considering that in the future, a user may change roles and thus access sensitive data that was not initially allowed. Cloud infrastructures have some tools to manage data security; for instance, Microsoft Azure stores sensitive data in the MS-SQL database and has security tools that encrypt the database's information. Cloud solutions have firewalls that allow restricting authorized IP addresses. Microsoft Azure recommends using firewalls at the database level instead of server firewalls since the former allows more granularity than

TABLE 2. Security Techniques that Cloud Providers Offer.

Technique	*AWS*	*Google Cloud*	*Azure*
Logging trail	CloudTrail	Cloud Audit Logs	Azure Search.
Multi-factor authentication	Amazon Identity and Access Management (IAM)	Cloud identity platform	Azure multi-factor authentication.
Sensitive data	Cloud Data Loss Prevention (DLP).		
Encryption key management	AWS Key Management Service (KMS)	Customer-supplied encryption keys Cloud KMS	Azure key vault
Single Sign-on functionality	Yes	Yes	Yes
Logging trail	Yes	Yes	Yes
Multi-factor authentication	Yes	Yes	Yes
Sensitive data protection (DLP)	Yes	Yes	Yes
Encryption end to end (motion data)	Yes	Yes	Yes
Encryption in Rest-data	Yes	Yes	Yes
Encryption keys	Yes	Yes	Yes
Data masking	Yes	Yes	Yes

the latter. Azure, Google, and AWS allow end-to-end encryption using TLS or HTTPs; however, data-rest encryption can be more challenging, and other tools should be configured in this context. AWS history produced by CloudTrail enables security analysis, resource change tracking, and compliance auditing. On the other hand, Azure Search allows fine-tuned ranking models [40]–[42].

As can be seen in Table 2, the different infrastructures have alternatives to improve security in the deployment of solutions that use the cloud; the importance of shared provider and customer security is again highlighted. There may be limitations in the provider's proposed cloud security solutions; also, the user's security configuration may be little or insufficient. Some cloud providers may have security features disabled by default, which can also create risks since the user does not perceive this status. An in-depth investigation of the security risks from the mechanisms or tools mentioned in this study can model the attack surface in a smart city.

A structured approach to reduce cybersecurity incidents' impact is the prioritization of cybersecurity activities and cybersecurity risk assessment efforts. Organizations such as Computer Emergency Response Team Coordination Center (CERT/CC), National Institute of Standards and Technology (NIST), European Network and Information Security Agency (ENISA), SysAdmin Audit, Networking and Security Institute (SANS), International Organization for Standardization, and International Electro-technical Commission proposed a set of phases for incident response.

For instance, NIST, in its special publication SP 800-61, defines five phases: (i) preparation, (ii) detection and analysis, (iii) containment, (iv) eradication and recovery, and (v) post-incident [3], [43]. In particular, the post-incident phase constitutes the final phase once an incident has been resolved. It is beneficial in improving security measures. It provides a chance to achieve closure concerning an incident by reviewing what occurred, what was done to intervene, and how well the intervention worked. The degree of pro-activeness is switched to high as the relevant personnel must take the initiative to recognize and reflect new threats and improve protection mechanisms. Results from this phase will be used as feedback to improve cybersecurity incident management. The principal activities in this phase include the following [44]:

- Identify the lessons learned from the cybersecurity incident;
- Identify and make improvements to the organization's security architecture;
- Review how effectively the incident response plan was executed.

III. RESEARCH METHODOLOGY

A. RESEARCH QUESTIONS

From our main research question of this study (i.e., *Is there an adequate IoT cybersecurity level for smart city scenarios?*), three secondary research questions have been derived as follows.

RQ1 Are IoT cybersecurity aspects a limitation in the development of a smart city?

RQ2 What is the role of policymakers to strengthen IoT cybersecurity in a smart city?

RQ3 How to measure the level of IoT cybersecurity in a smart city?

B. QUALITATIVE ANALYSIS

Forensics is a procedure in the cybersecurity incident response process related to the post-incident phase specifically. This process allows determining the root-cause of an attack. Knowing the root-cause allows improving security controls in gaps of cybersecurity infrastructure in smart cities. IoT forensics has been defined as a branch within digital forensics; it requires unique methods and perhaps is more complicated than those traditionally used in computer architecture [45].

To understand cybersecurity aspects in a smart city in the context of IoT solutions, we propose a top-down analysis. Determining the root-cause is useful for improving network security and identifying vulnerabilities [46]. In this study, we perform an SLR of the post-incident phase in IoT ecosystems to identify cybersecurity management's critical aspects. We follow the Prisma methodology [47] that consists of four stages: identification, screening, eligibility analysis, and inclusion. To perform these phases, we have used the Rayyan QCRI tool [48], which is designed to carry out a systematic review of the files uploaded to a system. The tool allowed us to execute the screening and eligibility, analysis, and inclusion through the blind peer review process to reduce subjectivity in the research process. Subsequently, with the selected articles, a qualitative analysis was carried out using the Atlas TI tool [49].

1) STAGE 1: IDENTIFICATION

a: STUDY SELECTION

The world population is expected to exceed 60% in urban areas [50], so city planning must consider the problems of social, economic, and environmental growth. The urban agenda for sustainable development, published in 2015, defines the guidelines to cover the social and ecological aspects until 2030, based on the achievement of 17 SDG objectives [11], [51]. In this aspect, IoT represents a critical element in the deployment of smart cities as a strategy for SDG compliance [52]. Based on this context, it is our interest to understand the importance of IoT in the development of smart cities and the security aspects generated with this technology's inclusion. For this reason, we selected research articles from the year 2015, when the Urban Agenda was defined, until May 2020, the date on which this study was presented.

For selecting the research articles, we have used the following databases: Springer, Scopus, IEEE Xplorer, Association for Computing Machinery (ACM), Web of Science, and Science Direct. These databases were chosen since they are the most relevant sources of information corresponding to "Information Systems" and "Technology." We have included the keywords `"(IoT OR smart city)" AND "(Forensics OR post-incident)"` in the search string.

b: INCLUSION AND EXCLUSION CRITERIA

The inclusion criteria consist of: (i) documents published in academic sources after peer-review, and (ii) documents that considered the use of IoT for application development.
The exclusion criteria were: preview surveys about IoT forensics (these works were included in the related works section but were not considered for the quality analysis process). We found 302 papers related to IoT forensics.

2) STAGE 2: SCREENING

a: TITLES AND ABSTRACTS

We have conducted a screening process of the 302 remaining papers for selecting the main contributions. After reading each paper's title and abstract carefully, we have excluded those papers in which the title and abstract did not comply with the inclusion criteria. We also have deleted duplicates articles. At the end of this stage, 176 articles that fulfill the criteria remained in the selected group.

3) STAGE 3: ELIGIBILITY ANALYSIS

a: FULL TEXT READING

After performing the previous stages, a full-text review of each article was done. If the article included cybersecurity aspects in greater detail about vulnerabilities, attacks, and protection mechanisms in IoT environments, they were considered for further qualitative analysis. At the end of this process, 28 articles were considered relevant to structure the initial contextual basis of our study. Table 3 details the selected articles; for each of them, we present the aspects that could generate cybersecurity issues and the main contribution.

4) STAGE 4: INCLUSION

a: DATA EXTRACTION

For each selected paper, we have summarized the following information: (i) IoT component or device, (ii) modeling proposal, (iii) forensics process, and (iv) future works. Therefore, this information was analyzed for each research objective that was presented in the following sections.

IV. RESULTS OF THE ANALYSIS OF THE SELECTED PAPERS

***Research objective 1:* Are IoT cybersecurity aspects a limitation in the development of a smart city?**

The perspective of cybersecurity issues is one of the limitations for the development of smart city solutions. According to Ijaz *et al.* [79], three factors affect information security in a smart city: technological, governance, and socio-economic factors. The technological factor includes IoT, semantic web, cloud computing, databases, software, and artificial intelligence. The governance factor includes city domains such as health, education, infrastructure, transport, energy, environment. Finally, the socio-economic factor includes communication, privacy, business, finance, and commerce.

Technology plays a crucial role in making a smart city functional [79]. However, technologies such as smart grids, biometrics, smartphones, and M2M communications present security issues. These technologies are often used in IoT ecosystems; hence IoT is one of the essential technologies in the development of smart cities; its importance lies in its accelerated growth and its applicability in different smart city domains to implement smart infrastructures [80].

We can observe that cybersecurity attacks in IoT ecosystems are versatile, and different attack vectors are possible due to smart city solutions' components or technologies. Smart cities need to establish cybersecurity strategies to reduce the impact of attacks. The first phase at a strategic level that the smart city must raise is to develop a *cybersecurity situational awareness* that allows it to know the strengths and weaknesses concerning the different factors that may affect its cybersecurity. Considering that one of the limitations is the technological factor and that the technological pillar in the development of the smart city is IoT, in what follows, we establish the cybersecurity situation awareness of this technology [81].

According to security organizations like OWASP (see Table 4) and some researches such as Alkeem *et al.* [82] and Liu *et al.* [22], the following attacks on IoT ecosystems are defined:

- Eavesdropping: This allows attackers to intercept data and help them to obtain sensitive information;
- Data modification: Attackers try to replace the information or modify it with minor changes;

TABLE 3. Results of the SLR. Selected Papers to Review.

Journal	Year	Title	Aspects that could generate cybersecurity issues	Contribution	Reference
IEEE Transactions on Information Forensics and Security	2017	Strategic Trust in Cloud-Enabled Cyber-Physical Systems with an Application to Glucose Control	Advanced persistent threats (APTs) can infiltrate in the network and use obfuscation to remain undetected	Game theory to capture the adversarial and strategic nature of CPS security	[53]
	2018	A Game Theory Based Collaborative Security Detection Method for IoT Systems	IoT systems tend to be established in a distributed manner for saving resource consumption,	Game theoretical analysis framework to collaborative security detection	[54]
	2018	MDSClone: Multidimensional Scaling Aided Clone Detection in IoT	Attacker to gather configuration and authentication credentials from a non-tamper-proof node, and replicate it in the network	Algorithm for clone detection probability	[55]
	2018	Deep Abstraction and Weighted Feature Selection for Wi-Fi Impersonation Detection	Impersonation attack in which an adversary is disguised as a legitimate party in a system	Deep-feature extraction and selection (D-FES), which combines stacked feature extraction and weighted feature selection to attack detection	[56]
	2019	Modeling, Analysis, and Mitigation of Dynamic Botnet Formation in Wireless IoT Networks	Software vulnerabilities in devices, due to low cost and short time-to-market.	An analytical model to study the D2D propagation of malware in wireless IoT networks	[57]
	2019	IoT-NUMS: Evaluating NUMS Elliptic Curve Cryptography for IoT Platforms	Timing and simple side-channel attacks	Evaluating NUMS Elliptic Curve Cryptography	[58]
	2019	Towards Efficient Fine-Grained Access Control and Trustworthy Data Processing for Remote Monitoring Services in IoT	User data privacy attacks by unauthorized parties	Robust and lightweight "heartbeat" protocol to handle the difficult key revocation problem	[59]
	2019	Interdependent Strategic Security Risk Management With Bounded Rationality in the Internet of Things	Users cannot be aware of the security policies taken by all its connected neighbors, so user makes security decisions based on the cyber-risks that perceives by observing a selected number of nodes	Proximal-based iterative algorithm to compute the Gestalt Nash equilibrium (GNE) to characterize the decisions of agents and quantify their risk	[60]
	2019	SafeChain: Securing Trigger-Action Programming From Attack Chains	Attack-privilege escalation and privacy leakage	SafeChain can efficiently and accurately identify attack chains	[27]
	2019	Trust Evaluation Mechanism for User Recruitment in Mobile Crowd-Sensing in the Internet of Things	Unintentionally corrupted and falsified data or intentionally spreading disinformation for malevolent purposes	A novel trust model called experience-reputation (E-R) is proposed for evaluating trust relationships between any two mobile device users	[61]
	2020	A GLRT-Based Mechanism for Detecting Relay Misbehavior in Clustered IoT Networks	Dropping the packets transmitted by the IoT devices and/or by corrupting the packets to be forwarded by the relay	Hybrid intrusion detection systems with semi-analytical approach	
	2020	SLATE: A Secure Lightweight Entity Authentication Hardware Primitive	Lightweight cryptography for resource constrained systems	Secure lightweight entity authentication hardware primitive called SLATE	[62]
	2020	SARA: Secure Asynchronous Remote Attestation for IoT Systems	Remote attestation is particularly important for securing Internet of Things (IoT) systems	A novel Secure Asynchronous Remote Attestation (SARA) protocol that exploits asynchronous communication capabilities among IoT devices and verifies that each IoT device is not compromised	[63]
	2020	An Attack-Resilient Architecture for the Internet of Things	A single vulnerable device can undermine the security of the entire network	An architecture that prevents deceitful messages generated by compromised devices from affecting the rest of the network	[64]
Digital Investigation	2017	Future challenges for smart cities: Cyber-security and digital forensics	Smart city data is generated in vulnerable environments by all data sources, for storage in a back-end Cloud	A holistic view of the security landscape of a smart city, identifying security threats and providing deep insight into digital investigation in the context of the smart city.	[65]
	2019	Leveraging Electromagnetic Side-Channel Analysis for the Investigation of IoT Devices	User's personal information and cloud communication data can be stored in the device directory. Some AI speaker stored all the voice response data without any deletion.	Analysis methodologies for data acquisition through of legitimate analysis process.	[66]
	2019	IoT forensic challenges and opportunities for digital traces	Extraction of user cloud credentials from the application settings.	Extending existing methods for extracting and examining traces from smartphones to IoT device.	[67]
	2019	Comprehending the IoT cyber threat landscape: A data dimensionality reduction technique to infer and characterize Internet-scale IoT probing campaigns	The resource-constrained and heterogeneous nature of IoT devices coupled with the placement of such devices in publicly accessible venues complicate efforts to secure these devices	Identify the issues related with open resolvers that have been specifically generated from IoT devices.	[68]
Advances in Intelligent Systems and Computing.		Attack Detection and Forensics Using Honeypot in IoT Environment.	IoT networks are vulnerable to various security attacks by remote login (like SSH and Telnet).	Employ various machine learning algorithms, namely, Naive Bayes, J48 decision tree, Random Forest and Support Vector Machine (SVM) to classify IoT attacks.	[69]
	2018	Acquiring RFID Tag Asymmetric Key from IOT Cyber Physical Environment.	Radio Frequency Identification (RFID) allow identify and locate objects and record metadata.	A methodology for acquisition of RFID tag asymmetric key for IoT forensic purpose.	[70]
Lecture Notes in Computer Science	2017	Privacy verification Chains for IoT	Privacy and Security by Design for Internet of Things (IoT)	A Privacy Verification Chains (PVC) to enforce a strict separation between data providers and data controllers.	[71]
	2019	Digital Forensics and Privacy-by-Design: Example in a Blockchain-based Dynamic Navigation System.	In a centralized system, insurance companies have access to all the information collected from the user.	Model for Data privacy compatible with General Data Protection Regulation (GDPR).	[72]
IEEE Internet of Things Journal	2019	IoT Forensics: Amazon Echo as a Use Case	Complexity, diversity, and heterogeneity of IoT devices and ecosystems.	IoT-based forensic model that supports the identification, acquisition, analysis, and presentation of potential artifacts of forensic interest.	[73]
	2019	Treasure collection on foggy islands: Building secure network archives for internet of things.	Unprecedentedly huge volumes of network traffic from massive IoT devices.	Trusted hardware and searchable encryption for building trustworthy.	[74]
ACM International Conference Proceeding Series.	2018	IoT forensic: Identification and classification of evidence in criminal investigations.	Heterogeneous nature of the IoT device, lack of IoT standards and the complex IoT architecture affect to the identification of an incident and its evidence.	Tools and techniques to identify and locate IoT devices with the concept "digital footprint."	[75]
	2018	I know what you did last summer: Your smart home internet of things and your iPhone forensically ratting you out	Smart home IoT devices have already been used as culpatory evidence.	Forensic Evidence Acquisition and Analysis System (FEAAS) that can infer user events (like entering or leaving a home) and what triggered an event.	[76]
IEEE Access	2018	IoT Device Forensics and Data Reduction.	The growing volume of devices and data will require newly developed data structures to analyze cyberattacks.	Bulk digital forensic data analysis for disparate device data.	[77]
	2019	Forensics and Deep Learning Mechanisms for Botnets in Internet of Things: A Survey of Challenges and Solutions	Handle diverse data in large volumes, requiring near real-time processing.	Investigate the applicability of deep learning in network forensics.	[78]

- Replay Attack: A part of the valid information can be sent back by the attacker to the original receiver after some time;
- Denial of service: Attackers try to flood the system with traffic that is higher than the system's capacity;

TABLE 4. Attack Vectors in the IoT Ecosystem.

Technology	*Attacks*
Weak, guessable, or Hardcore passwords	Attacker uses default passwords which have not been changed or set account passwords that they choose.
Insecure network services	The communication technology and channel must be secured. When there is weak negotiation, poor handshake practices, or incorrect versions of SSL, the communication is not secure.
Insecure ecosystem interfaces	Components such as Secure Shell (SSH), BusyBox, or web servers are not kept up to date; the threat actor might expose these vulnerabilities and gain access.
Lack of secure update mechanism	Updates and patches to devices are usually done remotely. If the process is not secure, the threat actor could intercept the update and install their malicious update.
Use of insecure or outdated components	Deprecated or insecure software or libraries.
Insufficient privacy protection	Personal information store on an insecure device.
Insecure data transfer and storage	Application Programming Interfaces (APIs) and web applications do not protect data correctly. They may not encrypt data or correctly exchange it with browsers.
Lack of device management	Session management, and authentication can be incorrectly implemented. This allows the threat actor to discover keys and passwords or to masquerade as other users (broken authentication).
Insecure default settings	Devices with insecure default settings.
Lack of physical hardening	Devices located on the outside place without tampering protection.

TABLE 5. Attacks to Technologies Used in the IoT Ecosystem.

Technology	*Attacks*	*Smart City Case*
RFID/NFC	Tag killing. Signal interference. Jamming. DoS. Spoofing. Cryptoanalysis. Eavesdropping.	RFID is used on smart city applications such as smart parking, traffic management, human tracking, and healthcare [85]. In contrast, NFC is used on contactless payment, navigation, information, or couponing [86]. NFC devices can also exchange data with existing card readers and ISO 14443 compliant units. eMarketer estimates there will be 69.4 million NFC mobile payment users by the end of 2020; that number will rise to 80.1 million users by 2023, with people using their mobile devices as travel tickets on metros, subways, and buses. The grown of IoT devices increase this number. In an eavesdropping scenario, the attacker uses an antenna to capture RF signals of the communication between NFC devices, another second method the attacker installs a malicious terminal and wait that the user device touched it. The Interception of an NFC exchange allows theft of sensitive information or allows attackers to manipulate the information to make it useless. Some vulnerabilities like CVE-2019-2114 allow the bypass local privileges using a package installation on Android mobiles.
WSN	Bandwidth degradation. Unauthorized access. Battery exhaustion.	WSNs are used to manage parking lots and lighting infrastructure. The main goal of these attacks is obstruct one or more paths in order to increase the arrival time of the packets from the target leaves, to crash intermediate routing nodes, to decrease node batteries, or to provoke a general DoS [87].
M2M	Physical Attacks. Attacks on authentication. Man-in-the-middle. Side-channel. Node tampering. Relay attacks.	Attacker can use multiple identities for occupy the all channel and prevent legitimate nodes can access to the network. [88].
Smart Grid	Threats to network availability. Message replay. False data attacks. Attacks on privacy. DoS. Breaches in data integrity	An attacker can execute stealthy false data injection attacks on the state estimation of a power grid to steal electricity, cause minor disruption in the grid, induce cascading failures and/or cause large-scale outages [89]. FDI attacks occur when an adversary attempts to inject false measurements into the system. It requires attackers to access the topology and state variables only of an attacked region's boundary buses rather than the whole grid.
Smartphone	Malicious applications. Botnets. Location privacy and GPS. Threats through WiFi. Threats in social network. Privacy issues.	Attackers could infected android APK with the goal of send phishing attacks to citizens or convert smartphones on botnets for DDoS attacks [90].

- Man-in-the-middle attack: It is the type of attack where the attacker positions himself between two parties.

Table 5 shows specific attacks on technologies used with IoT solutions. Building on this, Aydos *et al.* [83] propose a classification of the attacks according to the layers defined in the IoT architecture. Burhan *et al.* [84] mention that security is a critical issue in IoT applications and describe some security mechanisms that can be used in the technologies that enable IoT, as shown in Table 6.

Regarding IoT forensics models, the following were identified:

- FoBI: fog-based IoT forensic framework;
- Forensics-aware IoT (FAIoT) model;
- Forensic State Acquisition from the Internet of Things (FSAIoT);
- FIF-IoT: a forensic investigation framework using a public digital ledger.

In the IoT forensics process [45], at least three layers are considered: Device-level forensics, network forensics, and cloud forensics. At the device-level layer, the data stored in the IoT device memory is considered; at the network level, the aspects related to network logs are considered; and at the cloud level, the stored data of the IoT devices are considered. The model developed in [45] establishes a Secure Evidence Preservation Module. This module will continuously monitor all the registered IoT devices and store evidence securely in an evidence repository. Hossain *et al.* [94] mention some limitations to the forensics process in IoT ecosystems due to the IoT components' features. Table 7 summarizes these constraints in three aspects: Hardware, software, and network.

FUTURE RESEARCH DIRECTIONS ON IoT SECURITY ON SMART CITY

Cybersecurity management in the smart city is more complicated than in traditional information technology systems due to the solutions' heterogeneity and larger attack surface. It can be seen that the layer model is widely used,

TABLE 6. Attacks to the IoT Layer Approach.

Layer	*Attacks*	*Attacks Case*
Application	Social Engineering Broken authentication Virus Unauthorized access Injection Trojan	Session management and authentication can be incorrectly implemented. This allows the threat actor to discover keys and passwords, or to masquerade as other users [91].
Services	Exhaustion Collision Malware	Attacker can extract valuable information from data in-transit of MQTT protocol (plain text), such as: IP broker, data payload, port number of MQTT [38].
Network	Man-in-the-middle De-synchronization Unfairness Wormhole Flooding Spoofing Selective forwarding DDoS	In the IoT ecosystem, a rogue device could masquerade as a legitimate member of an IoT network resulting in significant data theft or falsification. In DDoS attacks, the attacker builds a botnet of zombie hosts. The command-and-control (CnC) server communicates with zombies over a covert channel using Internet Relay Chat (IRC), Peer-to-Peer (P2P), Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), or secure HTTP (HTTPS). When more IoT devices are infected, the botmaster carries out the DDoS attack on the chosen target. [92]
Physical	Tampering Eavesdropping Jamming Denial of Service	Systems offer to debug/boot mode in case the system encounters a problem when starting up. The attacker could access the debug/boot mode using a keystroke or connecting to JTAG or UART interface. After that, the device has been compromised; a backdoor can be installed to execute malicious commands remotely using, for instance, netcat commands [93].

TABLE 7. Attacks to IoT Components.

Component	*Limitations*	*Attacks Case*
Hardware	Computational Energy Memory Tamper-resistant	SD cards and MicroSD cards (µSD) are often used to store data necessary for IoT operation or store collected data. They could even include the entire operating system and configuration files necessary for operation. An SD card could potentially have data stolen or destroyed by an attacker [96].
Software	Embedded software Dynamic patch	IoT devices typically use a trimmed down version of an operating system. Developers can choose from open source and commercial options [97].
Network	Mobility Scalability Multiplicity devices Multiplicity communications Multi-protocol networking Dynamic-network	Threat actors often use amplification and reflection techniques to create DoS attacks. The attacker forwards ICMP echo request messages that contain the source IP address of the victim to a large number of hosts. The number of IoT devices that could be associated with botnet DDoS attacks could improve the damage [92].

but there are no standardized names. In the recommendation Y.4000/Y.2060 by ITU [97], the IoT layers are named as:

- Application Layer, similar to application layer mentioned by Burhan [84].
- Service Layer, similar to application layer mentioned by Burhan [84].
- Network Layer, similar to network layer mentioned by Burhan [84].
- Device Layer, similar to the perception layer mentioned by Burhan [84].

City managers: need to evaluate the cybersecurity risk to provide privacy and quality of life to citizens in building or improving smart city models. Technologies allow to build smart city models for archiving the sustainability goals, but these technologies could expand cities' vulnerability. IoT is one of the critical technologies for building smart cities, and its growth for the next years will be considerable worldwide. City managers need to consider cybersecurity requirements before installing IoT devices, especially on critical infrastructures. City managers need to evaluate the control mechanisms to guarantee the critical infrastructures that prove the city's services against attacks like denial of service and theft of personal information.

They need to participate actively in the culture of cybersecurity to prevent theft of information and keep privacy. Especially, smart home scenarios need to improve their security and avoid default configurations.

Third parties (e.g., manufacturers or standardization organizations): need to develop cybersecurity guidelines for building a security ecosystem on smart city scenarios. IoT solutions need to include security from its design, including quality tests using established standards, e.g., ISO 25000.

Development methodologies to evaluate security on IoT devices, communications protocols, gateways equipment could contribute in a relevant way for improving cybersecurity on smart city scenarios.

Academy: needs to continue in the contributions of research processes on cybersecurity of smart cities. IoT vulnerabilities are present on different layers of the ITU architecture. The academy could contribute to different aspects, such as:

- Methodologies for identifying vulnerabilities on technology components used in a smart city.
- Methodologies for classifying and measuring vulnerabilities
- Methodologies for evaluating cyber-risks on smart cities.
- Literature reviews on emergent attacks on smart cities.

***Research objective 2:* What is the role of policymakers to strengthen IoT cybersecurity in a smart city?**

Policymakers must obtain information that allows establishing a set of policies to strengthen security in the smart city. As mentioned above, there are various IoT solutions, different attack vectors, and many vulnerabilities that can be used by attackers. Policymakers must have the ability to establish the specific cybersecurity situational awareness for a smart city. From the perspective of IoT ecosystems, based on [98], we define four steps for the role of policymakers to strengthen IoT cybersecurity in a smart city.

(i) Establish the dimensions of the attack surface. The following three broad dimensions are considered.
1. Targets and enablers: Any resource in the IoT ecosystem of the smart city that may be of interest to the attacker.

2. Channels and protocols: The means used by the components to interact within the IoT ecosystem of the smart city.

3. Access rights: The rights associated with resources of the IoT ecosystem of the smart city.

(ii) Identify the attack vectors that were more likely to be used for attackers. It is necessary to identify the most relevant attack vectors (see Table 4). We propose to use a risk model to carry out the classification process. Nurse *et al.* [99] mention some risk assessment frameworks that are commonly used in organizations and governments, i.e., NIST SP800-30, ISO/IEC 27001, Operationally Critical Threat Asset and Vulnerability Evaluation (OCTAVE), CCTA Risk Analysis and Management Method (CRAMM). NIST [100] proposes a recommendation for IoT manufacturers to evaluate security aspects before IoT devices are sold to customers. A relevant contribution in [99] is to consider that due to the dynamics of the IoT ecosystems, the risk models described before may need to be adapted; we agree on that.

(iii) Define security metrics to evaluate the cybersecurity maturity of a smart city.

(iv) Define the set of policies to implement jointly with monitoring and improving strategies that prevent the attacks.

FUTURE RESEARCH DIRECTIONS IN POLICY-MAKING

When the present study was developed, a lack of policies or guidelines focused on smart city's cybersecurity was detected. Several proposals of organizations like ISO, NIST, and ITU development for IT systems could be applied to smart city scenarios. However, the complex, dynamic, and diversity of technologies used to build smart cities raise the need for developing specific policies, guidelines, and standards. Policy-makers have the challenge of developing policies in a timely way facing the continuous development of new technologies. Some future research directions in this context are the following:

City managers: establish cybersecurity policies related to:

- Data privacy in a smart city.
- Personal data storage and process in smart city.
- Guidelines for interoperability between technologies and vertical domains of a smart city.
- Data security in vertical domains of a smart city.
- Cybersecurity incident response handling in a smart city.

Third parties: maintain the development of security solutions for technologies used in a smart city according to guidelines and standards for improving the cybersecurity situational awareness. The development of IoT to build smart city solutions is continuously growing, and it needs to cover some cybersecurity aspects:

- Lightweight encryption algorithms for IoT devices.
- Security mechanisms for communication channels.
- Authentication mechanisms for ubiquitous and heterogeneous networks.
- Security requirements validation process for IoT ecosystems.

Academy: development of cybersecurity programs focused on the development of cybersecurity in smart cities scenarios, which could include topics like:

- Data privacy in a smart city.
- Cybersecurity for urban computational models.
- Cybersecurity on smart city technologies.
- Cybersecurity compliance in a smart city.

Research objective 3: **How to measure the level of IoT cybersecurity in a smart city?**

In the conducted SLR, we did not find an assessment model to evaluate the cybersecurity maturity level in a smart city; however, considering that the development of this model can be an essential support to improve the cybersecurity at the smart city level, we have proposed an approach in Section V.

Bear in mind that only assessing each city's security level may not be effective because each city has a different dynamic. Even within the same city, there may be different IoT solutions for the same domain that perform the same functionality, but they could present different security levels. Howard *et al.* [98] propose a relative measure to assess the security between different operating system versions. It is based on the fact that instead of measuring a system's absolute security, it is more useful to assess its relative security. Although it is complex to establish metrics to assess a system's security, how safe one system is concerning another could be established. As several IoT solutions could be developed from the mentioned approach, we can establish if IoT solution A is safer than IoT solution B, considering that the two solutions will be within the same smart city ecosystem. Several researchers have adopted the proposal in [98] to assess the security of information systems. Based on this context, we find it interesting to propose an adaptation of the proposal in [98] to the smart city context. To establish a relative security measurement model based on the attack surface in a smart city, we propose the following four steps:

1) Establish an attack surface formed by the set of elements that make up the system;
2) Identify the set of attack vectors that can allow the attack to that surface;
3) Establish a strategy to reduce the attack surface;
4) Evaluate relative security by establishing security improvements by reducing the attack surface.

FUTURE RESEARCH DIRECTIONS ON SMART CITY CYBERSECURITY MODELS

City managers: need to establish a cybersecurity situational awareness of smart city; for that, it is important to:

- Establish a layer-based model to evaluate a smart city's cybersecurity maturity that includes social, economic, and environmental factors and key pillars.
- Identify the impact value of cyber-attacks on social, economic, and environmental factors in smart cities' different verticals.

- Identify the critical cyber-attacks surfaces for establishing cybersecurity control mechanisms.
- Define cybersecurity indicators of compromise for measuring the level of cybersecurity risk.

Third parties: develop and propose cybersecurity maturity models for evaluating smart city components. Support the development of indicators of cybersecurity vulnerabilities. Approaches like CVSS are adequate resources, but they need to be adapted for the IoT and smart city contexts.

Academy: could contribute to the development of cybersecurity smart city models. The vast amount of data, the heterogeneous and large number of devices, and the administrative process to get data in real-time in a smart city could delay the development of smart city cybersecurity models. The development of simulation scenarios for evaluating cybersecurity models could be an essential contribution from the academic perspective.

A. DISCUSSION

IoT ecosystems support various applications in different smart cities' axes, but they are exposed to new threats from the cybersecurity approach. The challenge of cybersecurity in IoT is the heterogeneity of devices, networks, protocols, and the hyper-connectivity IoT represents. IoT is still considered an emerging technology, and proposals for standardization and security management of IoT have developed. Based on the performed SLR, we have identified four key aspects that should be addressed in IoT ecosystems.

1) *Network security:* Numerous types of networks support the hyper-connectivity of IoT; this allows the vast scope of IoT, its mobility, and adaptability. Perhaps one of the biggest security challenges in IoT ecosystems is that most IoT networks are wireless.
2) *Authentication:* The authentication secures the process of accessing an IoT network by devices, persons, and systems. Establishing one-way authentication mechanisms, e.g., authentication based on a password can be a weak option for IoT ecosystems. The administration of authentication mechanisms can be complicated due to many devices and the process associated with modifying the device's credentials. An API is more common in IoT ecosystems; the authentication process should consider this kind of interface connection.
3) *Encryption:* It ensures security in the storage and transfer of data, and it is essential in IoT security. However, encryption requires important computational resources, which are generally limited in IoT components.
4) *Update:* Keeping IoT devices and systems updated regularly is critical for reducing possible cybersecurity gaps. Due to the enormous number of IoT devices, this can be a complicated process.

Some researchers had made proposals to drive these cybersecurity key aspects in IoT ecosystems. For instance, Cui *et al.* [101] propose five research axes for IoT security:

1) IoT-based network security focuses on modeling patterns of the spread of an attack;
2) Security and privacy in fog systems;
3) User-centric and personalized protection methods;
4) Lightweight security solutions;
5) Theoretical complement.

TABLE 8. Disciplines per Layer for Protecting IoT Applications.

Layer	*Discipline*	*Use*
Application	Ontology	Smart home Mobile computing
Services	Cryptography	Smart transportation Smart grid Smart shopping Smart card
	Blockchain	Smart home Smart transportation
Network	Machine Learning & Data Mining	Smartphone Mobile devices Social networking
	Game Theory	Wireless networks Honeypot-enabled networks
Physical	Biometrics	Mobile sensors Storage devices

Additionally, Cui *et al.* [101] identify six disciplines related to protection methods in a smart city. From the smart city's perspective, it is necessary to evaluate which discipline is adequate to improve its cybersecurity capabilities. We match these disciplines to each stage of the IoT layer model (see Table 8). We also observe that cybersecurity in IoT ecosystems follows a layering approach. The forensics process commonly establishes three layers: device, network, and application, but attacks and threats can occur in four layers: physical, network, services, and application. Therefore, considering cybersecurity risk assessment for a smart city under a layering perspective can be useful. Aydos *et al.* [83] propose a risk-based layered security approach based on the following four stages: (i) securing the layers; (ii) understanding and evaluating layered threats; (iii) measuring the likelihood of layered threats; and (iv) determining the layered risk by combining the probability and impact of the layered threat.

V. SMART CITY CYBERSECURITY MATURITY MODEL DEVELOPMENT BASED ON RISK LEVELS

Based on the proposal by Mbanaso *et al.* [102] that defines a set of steps to develop a conceptual design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework, and the proposal by Weeserik and Spruit [103] which indicates a maturity model to improve risk management operationally, we have established the following five phases for developing an IoT Cybersecurity Maturity Model for a smart city:

Phase 1: Research context

Perform a review of literature and standards related to smart city, cybersecurity, resilience, and sustainability.

Phase 2: Design the strategy framework

Identify technologies or features related to cybersecurity, resilience, and sustainability.

TABLE 9. Cybersecurity Maturity Models for Organizations.

Acronym	*Cybersecurity maturity model*	*Proposed by*	*Maturity levels*	*Ref.*
CCSMM	Community CyberSecurity Maturity Model	White	Five	[107] [108]
COBIT	Control Objectives for Information and related Technology	ISACA	Five	[107]
CSF-NIST	Cybersecurity Framework	NIST	Five	[109] [108]
C2M2	Cybersecurity Capability Maturity Model	Curtis	Four	[110] [107]
ISMS	Information Security Management System-ISO27001	ISO	Five	[107] [108]
ISM3	Information Security Management Maturity Model	ISM3	Five	[107] [108]
-	NICE´s Cyber Security Capability Maturity Model	US DHS	Three	[108]
RMM	Resilience Management Model	CERT	Four	[111]
SSE-CMM	Systems Security Engineering Capability Model	NSA	Five	[112]

Phase 3: Conceptualization and specification of the Framework

Define the cybersecurity maturity model.

Phase 4: Mapping features of the cybersecurity maturity model based on expert panel ranking.

Phase 5: Validation of the initial cybersecurity maturity model.

1) RESEARCH CONTEXT

Several models have been developed to measure the maturity of cybersecurity capabilities in organizations; some of these are shown in Table 9. According to [104], the most widely used model is the SEE-CMM, since it presents details of the cybersecurity processes that must be implemented; it defines 22 areas (11 areas of engineering processes, 11 areas of project management) and establishes five levels of maturity. The second most used model is C2M2 [105]. The most comprehensive and used cybersecurity maturity models are CSF-NIST and C2M2 [106]; however, they have been criticized due to their subjectivity that can be generated when making self-assessment. Although the models are general and focused on organizations, the maturity model can be adapted to specific sectors [104] (e.g., C2M2 has two variants: one developed for the energy sector and another for the gas and fuel sectors).

The C2M2 model was released in 2012, and in 2014, it was updated to support the electrical sector. C2M2 is based on four maturity indicator levels (MIL0 to MIL3) and ten phases:

1) Risk management
2) Asset, change and configuration management
3) Identity and access management
4) Threat and vulnerability management
5) Situational awareness
6) Information sharing and communications
7) Event and incident response
8) Continuity of operations
9) Supply chain and external dependencies management
10) Workforce management and cybersecurity program management.

On the other hand, the CSF-NIST defines five phases: (i) Identify, (ii) Protect, (iii) Detect, (iv) Respond, (v) Recover.

Most of the mentioned models cover generic aspects and can be adapted to specific environments. However, as is the case of IoT ecosystems, certain aspects are not covered completely, or they are not adaptable from the generic models (e.g., risk assessment or continuous monitoring). In the IoT ecosystem, conducting an asset inventory can be quite complex to perform due to many devices and their physical location in the Smart City case. A similar context is the one presented when using C2M2. Generally, both COBIT and C2M2 perform the categorization of critical assets to analyze the security level and subsequently establish countermeasures; this aspect would be more complex to establish in an IoT-Smart City environment since any node attacked can have a high impact on critical city services. The proposed model seeks to prioritize the attack surface, the interrelation between the Smart city IoT nodes, and the probability of a future attack based on a previous attack.

The COBIT and C2M2 models propose maturity analysis focused on business objectives, but there is no direct concern in the aspects that may impact these systems' users. However, this reality is the opposite in the context of Smart City. Although there is concern regarding the technological systems used, citizens' concern is more significant, especially about those factors that may affect their sensitive personal information or impact your life. The proposed model seeks to propose an alternative for safety assessment based on the economic, social, and environmental aspects of the smart city in which the citizen and their interactions are included.

From the literature review conducted in this study, we found few cybersecurity maturity proposals applied to IoT; the most relevant are shown in Table 10. These two models include risk assessment and continuous monitoring. However, we cannot identify maturity levels in the proposal by Bugeja *et al.* [113]. Another relevant aspect that these two models consider is Governance.

2) DESIGN THE STRATEGY FRAMEWORK

In this phase, we have consider the BSI PAS 180 standard [115] that addresses the critical aspects of a smart city; it establishes the management of a smart city considering three axes: strategic, tactical, and operational factors as depicted in Fig. 3.

At the *strategic level*, it considers the three pillars on which a smart city is based on economic, environmental, and social factors. Measuring the impact of security attacks on each pillar will give city managers a comprehensive approach for subsequently establishing strategies to minimize the impact.

At the *tactical level*, the aspects to consider are the sustainability and the resilience of the smart city. Sustainability is defined as the city's capacity to manage resources for both current and future generations adequately. The resilience of the city is established as the capacity of the city to adapt to adverse situations. From a security perspective, the model's objective is to measure the maturity of the smart city's cybersecurity capabilities to identify and respond to security

TABLE 10. Cybersecurity Maturity Models Applied to IoT.

Model	*Proposal by*	*Levels*	*Domains*	*Sub-domains*
IoT_SMM	Industrial Internet Consortium [114]	None Minimum Adhoc Consistent Formalized	Governance Enablement Hardening	Strategy and governance Treat modeling and Risk assessment Supply chain and dependencies management Identity and access management Asset protection Data protection Vulnerability and patch management Situation awareness Event and incident response
IOTSM	Bugeja [113]	Not defined	Governance Construction Verification Operations	Security education and awareness Regulations and compliance Security-by-design Continuous and automated risk assessment Data and application threat modeling Security requirements and architecture Artifact Review Security testing Security operations and maintenance Security configuration

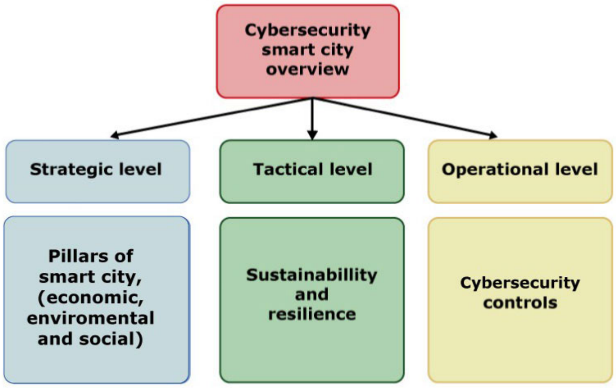
Cybersecurity smart city overview
Strategic level
Tactical level
Operational level
Pillars of smart city, (economic, enviromental and social)
Sustainabillity and resilience
Cybersecurity controls

FIGURE 3. Axes of the design strategy framework.

attacks that may directly or indirectly affect sustainability and resilience.

At the *operational level*, the maturity model would consider several aspects, such as the implemented security controls, the detected vulnerabilities, logging infrastructure, incident response effectiveness, and device access.

Fig. 4 illustrates how these axes interact to define the risk levels in a smart city.

3) CONCEPTUALIZATION AND SPECIFICATION OF THE FRAMEWORK

Table 11 shows the main specific factors of each pillar of the smart city that must be evaluated from the strategic approach. From the tactical approach, two aspects closely related to the smart city are sustainability and resilience, as can be seen in Fig. 5. Focusing on cybersecurity aspects that may affect these two aspects will minimize their impact on the smart city and guarantee the smart city's economic, social, and environmental objectives.

In [102], an adaptation of the CMMI model is proposed considering resilience features; for this development, the following norms or cybersecurity standards are considered as input sources:

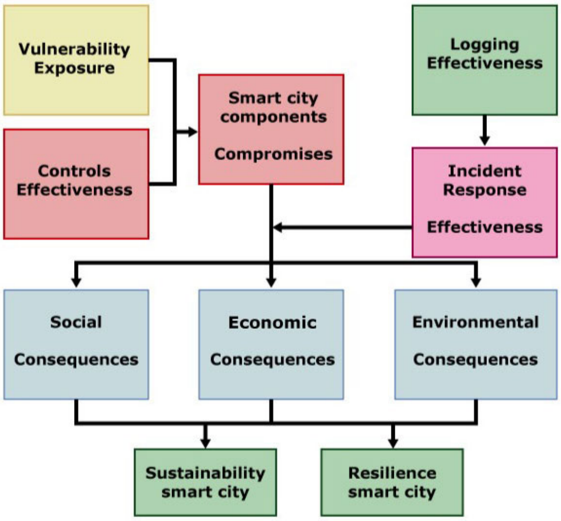

FIGURE 4. Risk levels as a function of the design strategy axes.

- COBIT5;
- CIS Security Control;
- SoGP for IS (Standard of good practice for information security), and
- ISO 27005.

The proposal considers the NIST cybersecurity framework a central element to assess compliance progress, empowering with a percentage of 20% the five functions: Identification, protection, detection, response, and recovery. The model also considers five levels of maturity: Not achieved (no controls), loosely achieved (few controls), partially achieved (some controls), mainly achieved (structured controls implemented), and fully achieved (baseline security).

4) MAPPING FEATURES OF THE CYBERSECURITY MATURITY MODEL BASED ON EXPERT PANEL RANKING

This phase aims to establish the cybersecurity characteristics that allow determining the smart city's risk levels based on the impacts of cybersecurity in each of the three pillars, namely

TABLE 11. Possible Cyberattack Outcomes on Smart City Pillars.

Factor	*Cyberattack outcome*
Social	People can suffer depression, anxiety, and frustration because of a cyberattack [116].
Economic	The loss of information or the disruption of businesses caused by attacks has a direct economic impact. The average costs of malware, web-based, and Denial of Service (DoS) attacks were $1.4 million, $1.4 million, and $ 1.1 million dollars, respectively, in 2018. According to the World Economic Forum, it is estimated a loss of $5.2 trillion dollars due to cyberattacks from 2019 to 2023 [117].
Environmental	Critical infrastructures that directly relate to environmental resources such as water or oil can be affected by cyberattacks. Attackers can take control of services and over saturate their demand or block their distribution. In October 2018, North Caroline's water and sewer service suffered a ransomware attack [118].

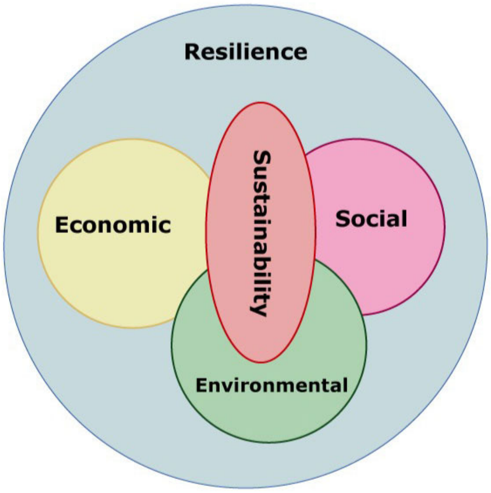

FIGURE 5. Aspects of the tactical level and their relation with the components of the strategic level.

economic, social, and environmental factors. To establish the correlation between the identified characteristics and the risk level, we propose using fuzzy engineering that allows establishing a set of rules and reducing the subjectivity that a panel of experts may have when defining weights for each of the characteristics associated with a certain risk level. Figure 6 presents the system components for mapping the strategic pillars to the risk level.

5) VALIDATION OF THE INITIAL CYBERSECURITY MATURITY MODEL

For the initial evaluation of the model, we used a simulation scheme based on Bayesian networks in which different scenarios of cyber-attacks in smart cities are performed. For that purpose, the Bayesian Server 9.2 Software was utilized.

A. EXPERIMENT

The Smart city contributes to fulfilling the sustainability and resilience objectives in the city's social, economic, and environmental perspectives. From a technological point of view, the Smart city is built through emerging technologies such as IoT, Bigdata (BD), Artificial Intelligence (AI), and Cloud. Their interrelation for the generation of information supports the decision-making processes of the different city factors. To evaluate the impact of cyberattacks on the city's strategic objectives, we conducted a simulation of the Smart city's components to evaluate the dependency relationship of each one's security factors and its impact on the social, economic, and environmental aspects.

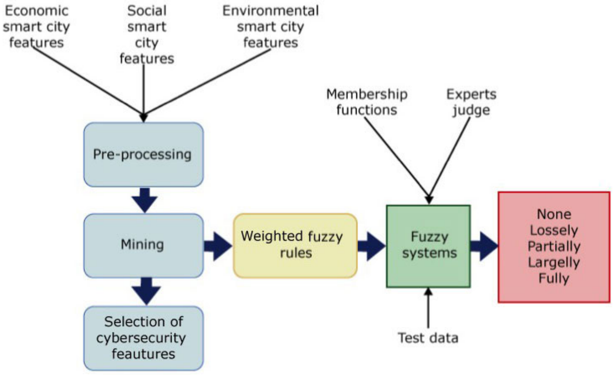

FIGURE 6. Correlation between strategic levels and risk levels as a function of the fuzzy system.

We defined four nodes as parents that represent emerging technologies IoT, BD, AI, and Cloud that can be used to construct the Smart city. Additionally, we have defined four nodes as children that simulate the vertical axes or domains of the city such as Smart health (SH), Smart traffic (ST), Smart agriculture (SA), and Smart grid (SG) that allow services to be covered and city operations and in which the use of emerging technologies is increasingly common. Finally, we have defined four nodes called leaf that represent the Economic (ECO), Environmental (ENV), and Social (SO) factors involved in the sustainability objectives of the city. We aim at evaluating the cybersecurity impact on the city's factors if an attack is performed on one of the parent nodes.

To model the dependency relationships between the different nodes, we have considered the use of Bayesian network as illustrated in Fig. 7. It will allow us to determine the probability of impact on the different nodes based on attack events that may occur at a particular node. The use of Bayesian networks allows us to represent the probability of impact in each relationship of nodes.

We have considered the ECO, ENV, and SO factors as temporal type where $t \in \{0, 1, 2, 3, 4\}$ in all nodes. In the Bayesian network, each node has a boolean type data representing two states: attack or not attack with their respective probabilities. For each time slot in simulation, the Bayesian network does not change (i.e., connections between nodes is permanent, but temporal nodes will have different probabilities associated with the type of attack). After running the model, we have obtained the results shown in Table 12. The results indicate the attack probability of each node of

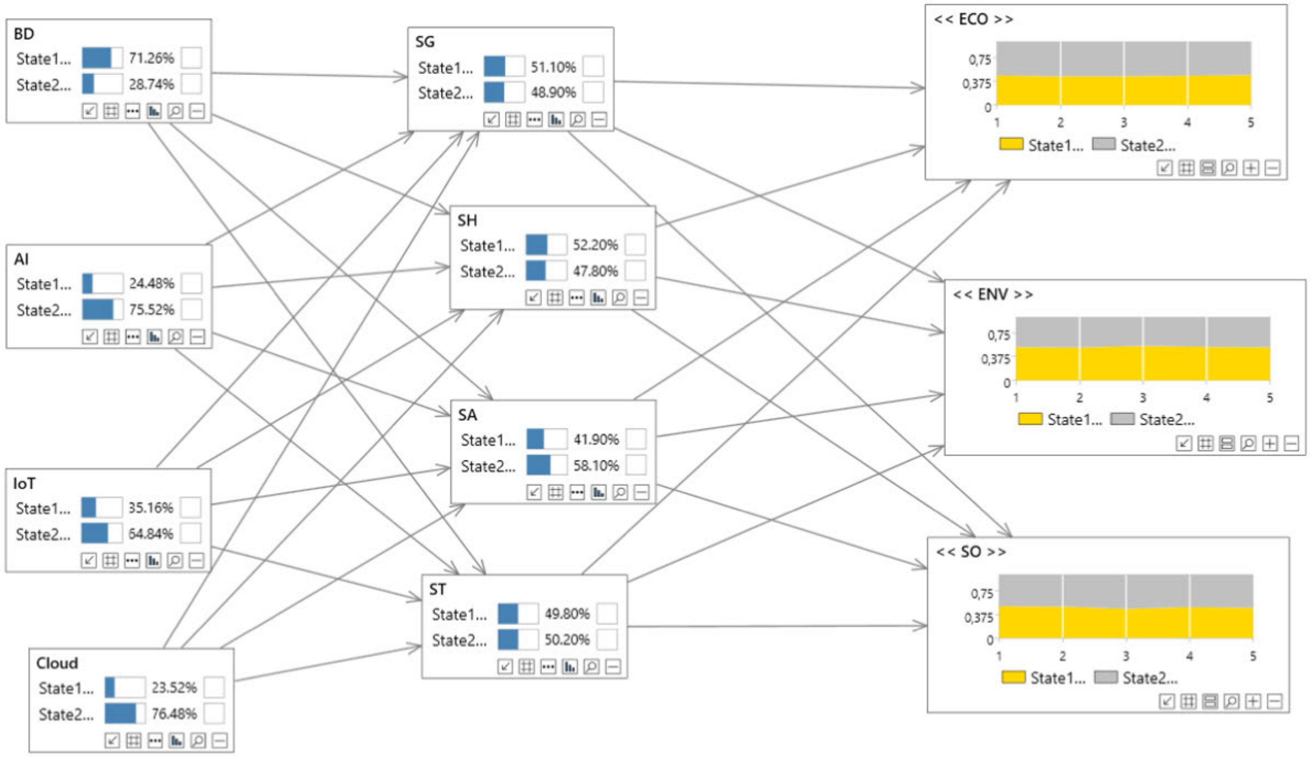

FIGURE 7. Bayesian network model for smart city simulation.

TABLE 12. Bayesian probabilities for simulated smart city attack.

BD	*AI*	*Cloud*	*IoT*	*ECO-False*	*ECO-True*	*ENV-False*	*ENV-True*	*SO-False*	*SO -True*
False	False	False	False	0.571	0.429	0.6	0.4	0.615	0.385
False	False	False	True	0.606	0.394	0.645	0.355	0.385	0.615
False	False	True	False	0.612	0.388	0.675	0.325	0.604	0.396
False	False	True	True	0.382	0.618	0.452	0.548	0.404	0.596
False	True	False	False	0.459	0.541	0.581	0.419	0.444	0.556
False	True	False	True	0.461	0.539	0.675	0.325	0.415	0.585
False	True	True	False	0.528	0.472	0.45	0.55	0.409	0.591
False	True	True	True	0.489	0.511	0.596	0.404	0.534	0.466
True	False	False	False	0.714	0.286	0.5	0.5	0.5	0.5
True	False	False	True	0.529	0.471	1	0	0.313	0.688
True	False	True	False	0.565	0.435	0.222	0.778	0.591	0.409
True	False	True	True	0.419	0.581	0.5	0.5	0.405	0.595
True	True	False	False	0.462	0.538	0.478	0.522	0.357	0.643
True	True	False	True	0.367	0.633	0.714	0.286	0.522	0.478
True	True	True	False	0.508	0.492	0.396	0.604	0.453	0.547
True	True	True	True	0.32	0.68	0.416	0.584	0.48	0.52

the smart city (SO, ECO, ENV) based on the parent nodes' possible state. According to Bayesian values, the highest probability of attack to the social node is 63.3% when the attacker affect BD, AI, and IoT nodes; the results also indicate that there is an attack probability of 68.8% to the economic node, if the attacker affects BD and IoT; finally, there is an attack probability of 71.4% to the ENV node, if the attacker focus on cloud and AI. One attack to all nodes has more relevance in the ECO node than the other two. According to our Bayesian model, if an attacker decides to affect only the IoT node, the attack probability is 61.5%, whereas the same attack event to other nodes executed on a separate way is equal or fewer than 50%. This simulation indicates that The IoT node presents a more significant probability of being attacked.

Another simulation scenario shows the probability of a smart traffic node (ST) being attacked based on the parent nodes' information, i.e., IoT, BD, AI, and Cloud. If an attacker decides not to take any action, the attack probability on the ST node is lower than 30%. In the opposite case, if the attacker tries to damage all the parent nodes' systems, the attack probability on the ST node is 96%. According to Bayesian values, the highest probability of ST attack is 95% when an attacker focuses on IoT and cloud. There are no

TABLE 13. Bayesian probabilities for simulated smart traffic attack.

BD	*AI*	*Cloud*	*IoT*	*ST-False*	*ST-True*
False	False	False	False	0.70	0.30
False	False	False	True	0.44	0.56
False	False	True	False	0.85	0.15
False	False	True	True	0.05	0.95
False	True	False	False	0.36	0.63
False	True	False	True	0.70	0.30
False	True	True	False	0.38	0.62
False	True	True	True	0.89	0.11
True	False	False	False	0.28	0.72
True	False	False	True	0.32	0.68
True	False	True	False	0.54	0.46
True	False	True	True	0..31	0.69
True	True	False	False	0.98	0.02
True	True	False	True	0.14	0.86
True	True	True	False	0.47	0.53
True	True	True	True	0.04	0.96

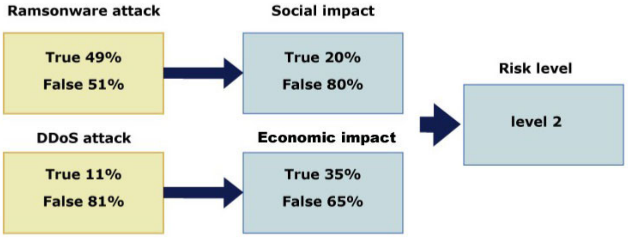

FIGURE 8. Determining the cybersecurity risk level by a Bayesian network analysis.

substantial difference in results when attacks are performed against all parents nodes together (see Table 13).

Cybersecurity risk level could be determined based on the conditional dependence of several attacks to environmental, social, and economic impact of smart city nodes. For instance, Fig. 8 illustrates the data from our simulation scenario where a ransomware attack represents a impact on the social node of 20%, while a DDoS attack affects the economic node in 35 %. These results individually could be considered of low impact for an smart city, but when they are combined, it generates an risk level of 2 in a scale of risk of 1 to 5. Fig 9 presents the lineal regression to corroborate of results obtained of simulation data of possibles attacks to smart city nodes using R software. According to Laugé *et al.* [119], dependencies create vulnerabilities that could cause a cascade of failures on critical infrastructures; for this reason, it is important that operators understand the complexity and dependencies of the critical infrastructures. Additionally, Laugé mentions that the dependencies of critical infrastructures (CI) could vary according to factors like the time period when failure happened and the duration of the failure.

To obtain a more accurate cyber-risk for smart cities, it is necessary to identify the dependencies among critical nodes and the level of impact of the attack to the economic, social and environmental nodes. The Bayesian model could be used for modeling the smart city attacks, but the identification of all possible relation among nodes is required. This could be a vast network because of all possible cybersecurity attacks related to IoT devices, AI algorithms, and cloud platforms in the city. Another challenge is to identify the impact of cyber-attack on economic, environmental, and social factors. The impact of each factor could be different for each vertical smart city domain. However, the Bayesian model allows understanding the relation of cyber-attack with parent nodes (IoT, Cloud, BD, and AI) with the smart city nodes (ECO, SO, and ENV factors).

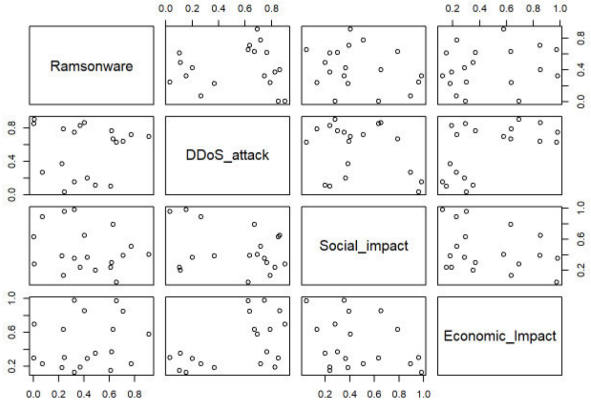

FIGURE 9. Classification model of dependencies of cyber-attacks with smart city nodes.

VI. CONCLUSION

Internet of Things (IoT) is a crucial component for the development of a smart city. In the next years, IoT will grow to billions of devices, as confirmed by international consulting firms. However, since IoT is vulnerable to cybersecurity attacks, this situation could impact smart cities' security. In this work, we have conducted a systematic literature review to identify the proposals for improving IoT cybersecurity in smart cities. Building on this, we have proposed an assessment model to evaluate the cybersecurity maturity level of IoT solutions used in a smart city. This model represents essential support for improving cybersecurity at the smart city level and ensuring its functionality. Furthermore, by applying cognitive security techniques, it would be possible to assess cybersecurity risk levels in the face of complexity, diversity, and large volumes of data in IoT ecosystems.

The large number of IoT devices found in the smart city and the various possible security attacks pose a challenge in risk analysis. To obtain a more accurate value of cyber-risk on smart cities, it is necessary to identify a more significant number of possible cyber-attacks and vulnerabilities and analyze the impacts and their relationships on the social, economic, and environmental domains. Relevant aspects when considering cybersecurity in IoT ecosystems are the relationships and dependencies of different nodes, e.g., Cloud. In cloud platforms, they have some cybersecurity parameters that can be used to minimize the impact of cyber attacks on smart cities.

At the time of study, we have identified a limitation of knowledge of the values of the impact of cyber-attacks on the social, economic, and environmental aspects of smart cities. Although there are some studies in this context, most of them are focused on the economic aspects, and they only analyze the social and environmental contexts superficially. The smart city's direct interaction with people encourages us to consider the present research on the social impacts generated by cyber-attacks; for example, when there are attacks on critical infrastructures that handle health, water, or energy aspects, it would directly affect the people's life.

Future works include evaluating the selected discipline's effectiveness as a protection method in each IoT ecosystem layer. To evaluate, improve, and measure the cybersecurity on IoT solutions used in smart cities, we could focus on the IoT network layer, and we could combine the proposals of risk-based layered security with machine learning or data mining solutions. We should also consider the limitations of IoT forensics and privacy issues in IoT ecosystems. In the forensic process, it is essential to determine the root-cause of cybersecurity attacks. Based on this SLR, it could be determined that no formal process has been established yet. Several IoT forensic models are based on ISO 27037 standard; however, there are gaps in applying the forensic process in IoT ecosystems. In future work, we will develop a model to identify the dependencies of a cybersecurity attack focused on IoT and their probabilities of impact on the smart city's social, economic, and environmental aspects. We have initially considered the Bayesian model to represent the dependencies among the smart city nodes because they describe the causality of relationships.

REFERENCES

[1] M. D. Lytras, A. Visvizi, M. Torres-Ruiz, E. Damiani, and P. Jin, "IEEE access special section editorial: Urban computing and well-being in smart cities: Services, applications, policymaking considerations," *IEEE Access*, vol. 8, pp. 72340–72346, 2020.

[2] F. Sivrikaya, N. Ben-Sassi, X.-T. Dang, O. C. Gorur, and C. Kuster, "Internet of smart city objects: A distributed framework for service discovery and composition," *IEEE Access*, vol. 7, pp. 14434–14454, 2019.

[3] R. Andrade, J. Torres, and L. Tello-Oquendo, "Cognitive security tasks using big data tools," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2018, pp. 100–105.

[4] L. Tello-Oquendo, S.-C. Lin, I. F. Akyildiz, and V. Pla, "Software-defined architecture for QoS-aware IoT deployments in 5G systems," *Ad Hoc Netw.*, vol. 93, Oct. 2019, Art. no. 101911. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870518309016

[5] L. Tello-Oquendo, I. F. Akyildiz, S.-C. Lin, and V. Pla, "SDN-based architecture for providing reliable Internet of Things connectivity in 5G systems," in *Proc. 17th Annu. Medit. Ad Hoc Netw. Workshop (Med-Hoc-Net)*, Jun. 2018, pp. 1–8.

[6] R. O. Andrade and S. G. Yoo, "A comprehensive study of the use of LoRa in the development of smart cities," *Appl. Sci.*, vol. 9, no. 22, p. 4753, Nov. 2019.

[7] A. Calvopinna, F. Tapia, and L. Tello-Oquendo, "Weather monitoring architecture for smart home using Alexa, Raspberry Pi, and DarkSky API," in *Proc. 8th Int. Conf. Softw. Process Improvement (CIMPS)*, Oct. 2019, pp. 1–5.

[8] A. Calvopiña, F. Tapia, L. Tello-Oquendo, "Uso del asistente virtual Alexa como herramienta de interacción para el monitoreo de clima en hogares inteligentes por medio de raspberry pi y DarkSky API," *RISTI-Revista Ibérica de Sistemas e Tecnologias de Informaçao*, vol. 36, pp. 102–115, Mar. 2020.

[9] I. Tanseer, N. Kanwal, M. N. Asghar, A. Iqbal, F. Tanseer, and M. Fleury, "Real-time, content-based communication load reduction in the Internet of multimedia things," *Appl. Sci.*, vol. 10, no. 3, p. 1152, Feb. 2020. [Online]. Available: https://www.mdpi.com/2076-3417/10/3/1152

[10] S. Singh and N. Singh, "Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce," in *Proc. Int. Conf. Green Comput. Internet Things (ICGCIoT)*, Oct. 2015, pp. 1577–1581.

[11] A. Lopez-Vargas, M. Fuentes, and M. Vivar, "Challenges and opportunities of the Internet of Things for global development to achieve the united nations sustainable development goals," *IEEE Access*, vol. 8, pp. 37202–37213, 2020.

[12] F. Ullah, H. Naeem, S. Jabbar, S. Khalid, M. A. Latif, F. Al-Turjman, and L. Mostarda, "Cyber security threats detection in Internet of Things using deep learning approach," *IEEE Access*, vol. 7, pp. 124379–124389, 2019.

[13] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[14] A. Laszka, B. Potteiger, Y. Vorobeychik, S. Amin, and X. Koutsoukos, "Vulnerability of transportation networks to traffic-signal tampering," in *Proc. ACM/IEEE 7th Int. Conf. Cyber-Phys. Syst. (ICCPS)*, Apr. 2016, pp. 1–10.

[15] P. Bagga, A. K. Das, M. Wazid, J. J. P. C. Rodrigues, and Y. Park, "Authentication protocols in Internet of vehicles: Taxonomy, analysis, and challenges," *IEEE Access*, vol. 8, pp. 54314–54344, 2020.

[16] S. Soltan, M. Yannakakis, and G. Zussman, "REACT to cyber attacks on power grids," *IEEE Trans. Netw. Sci. Eng.*, vol. 6, no. 3, pp. 459–473, Jul. 2019.

[17] R. Taormina, S. Galelli, N. O. Tippenhauer, E. Salomons, and A. Ostfeld, "Characterizing cyber-physical attacks on water distribution systems," *J. Water Resour. Planning Manage.*, vol. 143, no. 5, May 2017, Art. no. 04017009.

[18] I. Butun, P. Osterberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 616–644, 1st Quart., 2020.

[19] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," in *Proc. 70th Annu. Conf. Protective Relay Eng. (CPRE)*, Apr. 2017, pp. 1–8.

[20] M. Ozer, S. Varlioglu, B. Gonen, and M. Bastug, "A prevention and a traction system for ransomware attacks," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2019, pp. 150–154.

[21] M. Lytras and A. Visvizi, "Who uses smart city services and what to make of it: Toward interdisciplinary smart cities research," *Sustainability*, vol. 10, no. 6, p. 1998, Jun. 2018.

[22] X. Liu, C. Qian, W. G. Hatcher, H. Xu, W. Liao, and W. Yu, "Secure Internet of Things (IoT)-based smart-world critical infrastructures: Survey, case study and research opportunities," *IEEE Access*, vol. 7, pp. 79523–79544, 2019.

[23] M. Capellupo, J. Liranzo, M. Z. A. Bhuiyan, T. Hayajneh, and G. Wang, "Security and attack vector analysis of IoT devices," in *Security, Privacy, and Anonymity in Computation, Communication, and Storage*, G. Wang, M. Atiquzzaman, Z. Yan, and K.-K. R. Choo, Eds. Cham, Switzerland: Springer, 2017, pp. 593–606.

[24] A. Albataineh and I. Alsmadi, "IoT and the risk of Internet exposure: Risk assessment using shodan queries," in *Proc. IEEE 20th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2019, pp. 1–5.

[25] D. Yu, L. Zhang, Y. Chen, Y. Ma, and J. Chen, "Large-scale IoT devices firmware identification based on weak password," *IEEE Access*, vol. 8, pp. 7981–7992, 2020.

[26] K. V. English, I. Obaidat, and M. Sridhar, "Exploiting memory corruption vulnerabilities in connman for IoT devices," in *Proc. 49th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Jun. 2019, pp. 247–255.

[27] K.-H. Hsu, Y.-H. Chiang, and H.-C. Hsiao, "SafeChain: Securing trigger-action programming from attack chains," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 10, pp. 2607–2622, Oct. 2019.

[28] A. Mishra and A. Dixit, "Resolving threats in IoT: ID spoofing to DDoS," in *Proc. 9th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2018, pp. 1–7.

[29] N. Benkahla, B. Belgacem, and M. Frikha, "Security analysis in enhanced LoRaWAN duty cycle," in *Proc. 7th Int. Conf. Commun. Netw. (ComNet)*, Nov. 2018, pp. 1–7.

[30] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, and X. Fu, "Security vulnerabilities of Internet of Things: A case study of the smart plug system," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1899–1909, Dec. 2017.

[31] N. Moustafa, B. Turnbull, and K.-K.-R. Choo, "An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4815–4830, Jun. 2019.

[32] L. Metongnon and R. Sadre, "Beyond telnet: Prevalence of IoT protocols in telescope and honeypot measurements," in *Proc. Workshop Traffic Meas. Cybersecurity*, New York, NY, USA: Association Computing Machinery, Aug. 2018, pp. 21–26, doi: 10.1145/3229598.3229604.

[33] J. Mitsugi, S. Yonemura, H. Hada, and T. Inaba, "Bridging UPnP and ZigBee with CoAP: Protocol and its performance evaluation," in *Proc. Workshop Internet Things Service Platforms (IoTSP)* New York, NY, USA: Association Computing Machinery, 2011, pp. 1–8, doi: 10.1145/2079353.2079354.

[34] L. Lo Iacono, H. Nguyen, and P. Gorski, "On the need for a general REST-security framework," *Future Internet*, vol. 11, no. 3, p. 56, Feb. 2019, doi: 10.3390/fi11030056.

[35] D.-H. Lee and I.-Y. Lee, "Oauth-based access control scheme against replay attacks in IoT environment," in *Advances in Computer Science and Ubiquitous Computing*. Singapore: Springer, 2018, pp. 350–355.

[36] T. Chen, L. Li, S. Wang, G. Chen, and Z. Wang, "Improved group management protocol of RFID password method," in *Proc. 2nd Int. Conf. Internet Things, Data Cloud Comput.* New York, NY, USA: Association Computing Machinery, Mar. 2017, pp. 1–4, doi: 10.1145/3018896.3018937.

[37] A. Wang, R. Liang, X. Liu, Y. Zhang, K. Chen, and J. Li, "An inside look at IoT malware," in *Industrial IoT Technologies and Applications*, F. Chen and Y. Luo, Eds. Cham, Switzerland: Springer, 2017, pp. 176–186.

[38] S. Andy, B. Rahardjo, and B. Hanindhito, "Attack scenarios and security analysis of MQTT communication protocol in IoT system," in *Proc. 4th Int. Conf. Electr. Eng., Comput. Sci. Informat. (EECSI)*, Sep. 2017, pp. 1–6.

[39] *Amazon Tells Senators it Isn't to Blame for Capital One Breach*. Accessed: Nov. 21, 2019. [Online]. Available: https://www.cnet.com/news/amazon-tells-senators-it-isnt-to-blame-for-capital-one-breach/

[40] Z. Tari, "Security and privacy in cloud computing," *IEEE Cloud Comput.*, vol. 1, no. 1, pp. 54–57, May 2014.

[41] N. J. Mitchell and K. Zunnurhain, "Vulnerability scanning with Google cloud platform," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2019, pp. 1441–1447.

[42] F. M. Okikiola, A. M. Mustapha, A. F. Akinsola, and M. A. Sokunbi, "A new framework for detecting insider attacks in cloud-based E-Health care system," in *Proc. Int. Conf. Math., Comput. Eng. Comput. Sci. (ICMCECS)*, Mar. 2020, pp. 1–6.

[43] R. Andrade, J. Torres, and S. Cadena, "Cognitive security for incident management process," in *Proc. Int. Conf. Inf. Technol. Syst.* Cham, Switzerland: Springer, 2019, pp. 612–621.

[44] L. Tello-Oquendo, F. Tapia, W. Fuertes, R. Andrade, N. Erazo, J. Torres, and A. Cadena, "A structured approach to guide the development of incident management capability for security and privacy," in *Proc. 21st Int. Conf. Enterprise Inf. Syst.*, 2019, pp. 328–336.

[45] S. Zawoad and R. Hasan, "FAIoT: Towards building a forensics aware eco system for the Internet of Things," in *Proc. IEEE Int. Conf. Services Comput.*, Jun. 2015, pp. 279–284.

[46] V. Kumar, G. Oikonomou, and T. Tryfonas, "Traffic forensics for IPv6-based wireless sensor networks and the Internet of Things," in *Proc. IEEE 3rd World Forum Internet Things (WF-IoT)*, Dec. 2016, pp. 633–638.

[47] D. Moher, A. Liberati, J. Tetzlaff, D. G. Altman, and G. Prisma, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *Ann. Internal Med.*, vol. 151, no. 4, pp. 264–269, 2009.

[48] M. Ouzzani, H. Hammady, Z. Fedorowicz, and A. Elmagarmid, "Rayyan—A Web and mobile app for systematic reviews," *Systematic Rev.*, vol. 5, no. 1, p. 210, Dec. 2016.

[49] M. Puig, R. Vila, and M. Sandín Esteban, "El análisis cualitativo de datos con atlas ti," *REIRE. Revista d'Innovació i Recerca en Educació*, vol. 7, pp. 119–133, Jul. 2014.

[50] Y. Zhou, A. C. G. Varquez, and M. Kanda, "High-resolution global urban growth projection based on multiple applications of the SLEUTH urban growth model," *Sci. Data*, vol. 6, no. 1, p. 34, Apr. 2019.

[51] M. Cohen and G. Habron, "How does the new urban agenda align with comprehensive planning in U.S. cities? A case study of Asheville, North Carolina," *Sustainability*, vol. 10, no. 12, p. 4590, Dec. 2018, doi: 10.3390/su10124590.

[52] A. Visvizi, M. D. Lytras, E. Damiani, and H. Mathkour, "Policy making for smart cities: Innovation and social inclusive economic growth for sustainability," *J. Sci. Technol. Policy Manage.*, vol. 9, no. 2, pp. 126–133, Jul. 2018.

[53] J. Pawlick and Q. Zhu, "Strategic trust in cloud-enabled cyber-physical systems with an application to glucose control," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 12, pp. 2906–2919, Dec. 2017.

[54] H. Wu and W. Wang, "A game theory based collaborative security detection method for Internet of Things systems," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 6, pp. 1432–1445, Jun. 2018.

[55] P.-Y. Lee, C.-M. Yu, T. Dargahi, M. Conti, and G. Bianchi, "MDSClone: Multidimensional scaling aided clone detection in Internet of Things," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 2031–2046, Aug. 2018.

[56] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, "Deep abstraction and weighted feature selection for Wi-Fi impersonation detection," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 3, pp. 621–636, Mar. 2018.

[57] M. J. Farooq and Q. Zhu, "Modeling, analysis, and mitigation of dynamic botnet formation in wireless IoT networks," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 9, pp. 2412–2426, Sep. 2019.

[58] Z. Liu and H. Seo, "IoT-NUMS: Evaluating NUMS elliptic curve cryptography for IoT platforms," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 3, pp. 720–729, Mar. 2019.

[59] Y. Chen, W. Sun, N. Zhang, Q. Zheng, W. Lou, and Y. T. Hou, "Towards efficient fine-grained access control and trustworthy data processing for remote monitoring services in IoT," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 7, pp. 1830–1842, Jul. 2019.

[60] J. Chen and Q. Zhu, "Interdependent strategic security risk management with bounded rationality in the Internet of Things," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 11, pp. 2958–2971, Nov. 2019.

[61] N. B. Truong, G. M. Lee, T.-W. Um, and M. Mackay, "Trust evaluation mechanism for user recruitment in mobile crowd-sensing in the Internet of Things," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 10, pp. 2705–2719, Oct. 2019.

[62] W.-C. Wang, Y. Yona, Y. Wu, S. N. Diggavi, and P. Gupta, "SLATE: A secure lightweight entity authentication hardware primitive," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 276–285, 2020.

[63] E. Dushku, M. M. Rabbani, M. Conti, L. V. Mancini, and S. Ranise, ''SARA: Secure asynchronous remote attestation for IoT systems,'' *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3123–3136, 2020.

[64] H. M. J. Almohri, L. T. Watson, and D. Evans, ''An attack-resilient architecture for the Internet of Things,'' *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3940–3954, 2020.

[65] Z. A. Baig, P. Szewczyk, C. Valli, P. Rabadia, P. Hannay, M. Chernyshev, M. Johnstone, P. Kerai, A. Ibrahim, K. Sansurooah, N. Syed, and M. Peacock, ''Future challenges for smart cities: Cyber-security and digital forensics,'' *Digit. Invest.*, vol. 22, pp. 3–13, Sep. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1742287617300579

[66] A. Sayakkara, N.-A. Le-Khac, and M. Scanlon, ''Leveraging electromagnetic side-channel analysis for the investigation of IoT devices,'' *Digit. Invest.*, vol. 29, pp. S94–S103, Jul. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1742287619301616

[67] F. Servida and E. Casey, ''IoT forensic challenges and opportunities for digital traces,'' *Digit. Invest.*, vol. 28, pp. S22–S29, Apr. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1742287619300222

[68] M. S. Pour, E. Bou-Harb, K. Varma, N. Neshenko, D. A. Pados, and K.-K. R. Choo, ''Comprehending the IoT cyber threat landscape: A data dimensionality reduction technique to infer and characterize Internet-scale IoT probing campaigns,'' *Digit. Invest.*, vol. 28, pp. S40–S49, Apr. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1742287619300246

[69] R. K. Shrivastava, B. Bashir, and C. Hota, ''Attack detection and forensics using honeypot in IoT environment,'' in *Distributed Computing and Internet Technology*, G. Fahrnberger, S. Gopinathan, and L. Parida, Eds. Cham, Switzerland: Springer, 2019, pp. 402–409.

[70] M. T. A. Razak, N. A. Abdullah, and N. H. A. Rahman, ''Acquiring RFID tag asymmetric key from IoT cyber physical environment,'' in *Recent Trends in Data Science and Soft Computing*, F. Saeed, N. Gazem, F. Mohammed, and A. Busalim, Eds. Cham, Switzerland: Springer, 2019, pp. 538–547.

[71] N. Foukia, D. Billard, and E. Solana, ''Privacy verification chains for IoT,'' in *Network and System Security*, Z. Yan, R. Molva, W. Mazurczyk, and R. Kantola, Eds. Cham, Switzerland: Springer, 2017, pp. 737–752.

[72] D. Billard and B. Bartolomei, ''Digital forensics and privacy-by-design: Example in a blockchain-based dynamic navigation system,'' in *Privacy Technologies and Policy*, M. Naldi, G. F. Italiano, K. Rannenberg, M. Medina, and A. Bourka, Eds. Cham, Switzerland: Springer, 2019, pp. 151–160.

[73] S. Li, K.-K.-R. Choo, Q. Sun, W. J. Buchanan, and J. Cao, ''IoT forensics: Amazon echo as a use case,'' *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6487–6497, Aug. 2019.

[74] H. Duan, Y. Zheng, C. Wang, and X. Yuan, ''Treasure collection on foggy islands: Building secure network archives for Internet of Things,'' *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2637–2650, Apr. 2019.

[75] F. Bouchaud, G. Grimaud, and T. Vantroys, ''IoT forensic: Identification and classification of evidence in criminal investigations,'' in *Proc. 13th Int. Conf. Availability, Rel. Secur.*, New York, NY, USA: Association Computing Machinery, Aug. 2018, pp. 1–9, doi: 10.1145/3230833.3233257.

[76] G. Dorai, S. Houshmand, and I. Baggili, ''I know what you did last summer: Your smart home Internet of Things and your iPhone forensically ratting you out,'' in *Proc. 13th Int. Conf. Availability, Rel. Secur.* New York, NY, USA: Association Computing Machinery Aug. 2018, pp. 1–10, doi: 10.1145/3230833.3232814.

[77] D. Quick and K.-K.-R. Choo, ''IoT device forensics and data reduction,'' *IEEE Access*, vol. 6, pp. 47566–47574, 2018.

[78] N. Koroniotis, N. Moustafa, and E. Sitnikova, ''Forensics and deep learning mechanisms for botnets in Internet of Things: A survey of challenges and solutions,'' *IEEE Access*, vol. 7, pp. 61764–61785, 2019.

[79] S. Ijaz, M. Ali, A. Khan, and M. Ahmed, ''Smart cities: A survey on security concerns,'' *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 2, pp. 612–625, 2016.

[80] E. Park, A. del Pobil, and S. Kwon, ''The role of Internet of Things (IoT) in smart cities: Technology roadmap-oriented approaches,'' *Sustainability*, vol. 10, no. 5, p. 1388, May 2018.

[81] R. O. Andrade and S. G. Yoo, ''Cognitive security: A comprehensive study of cognitive science in cybersecurity,'' *J. Inf. Secur. Appl.*, vol. 48, Oct. 2019, Art. no. 102352.

[82] E. Al Alkeem, C. Y. Yeun, and M. J. Zemerly, ''Security and privacy framework for ubiquitous healthcare IoT devices,'' in *Proc. 10th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2015, pp. 70–75.

[83] M. Aydos, Y. Vural, and A. Tekerek, ''Assessing risks and threats with layered approach to Internet of Things security,'' *Meas. Control*, vol. 52, nos. 5–6, pp. 338–353, Jun. 2019.

[84] M. Burhan, R. Rehman, B. Khan, and B.-S. Kim, ''IoT elements, layered architectures and security issues: A comprehensive survey,'' *Sensors*, vol. 18, no. 9, p. 2796, Aug. 2018.

[85] A. Fahmy, H. Altaf, A. Al Nabulsi, A. Al-Ali, and R. Aburukba, ''Role of RFID technology in smart city applications,'' in *Proc. Int. Conf. Commun., Signal Process., Appl. (ICCSPA)*, Mar. 2019, pp. 1–6.

[86] E. Ronay and R. Egger, ''NFC smart city: Cities of the future—A scenario technique application,'' in *Information and Communication Technologies in Tourism 2014*, Z. Xiang and I. Tussyadiah, Eds. Cham, Switzerland: Springer, 2013, pp. 565–577.

[87] V. Garcia-Font, C. Garrigues, and H. R. Pous, ''Attack classification schema for smart city WSNs,'' *Sensors*, vol. 17, no. 4, p. 771, Apr. 2017.

[88] F. Hussain, L. Ferdouse, L. Karim, and I. Woungang, ''Security threats in M2M networks: A survey with case study,'' *Int. J. Comput. Syst. Sci. Eng.*, vol. 32, no. 2, pp. 1–18, Mar. 2017.

[89] M. Ashrafuzzaman, S. Das, Y. Chakhchoukh, S. Shiva, and F. T. Sheldon, ''Detecting stealthy false data injection attacks in the smart grid using ensemble-based machine learning,'' *Comput. Secur.*, vol. 97, Oct. 2020, Art. no. 101994. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404820302674

[90] S. K. Tidke, P. P. Karde, and V. Thakare, ''Detection and prevention of Android malware thru permission analysis,'' in *Proc. 4th Int. Conf. Comput. Commun. Control Autom. (ICCUBEA)*, Aug. 2018, pp. 1–6.

[91] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, ''A survey of Internet of Things (IoT) authentication schemes,'' *Sensors*, vol. 19, no. 5, p. 1141, Mar. 2019.

[92] A. Marzano, D. Alexander, O. Fonseca, E. Fazzion, C. Hoepers, K. Steding-Jessen, M. H. P. C. Chaves, I. Cunha, D. Guedes, and W. Meira, ''The evolution of bashlite and mirai IoT botnets,'' in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jun. 2018, pp. 00813–00818.

[93] G. Vishwakarma and W. Lee, ''Exploiting JTAG and its mitigation in IoT: A survey,'' *Future Internet*, vol. 10, no. 12, p. 121, Dec. 2018, doi: 10.3390/fi10120121.

[94] M. Hossain, Y. Karim, and R. Hasan, ''FIF-IoT: A forensic investigation framework for IoT using a public digital ledger,'' in *Proc. IEEE Int. Congr. Internet Things (ICIoT)*, Jul. 2018, pp. 33–40.

[95] H. Mohammed, T. A. Odetola, S. R. Hasan, S. Stissi, I. Garlin, and F. Awwad, ''(HIADIoT): Hardware intrinsic attack detection in Internet of Things; leveraging power profiling,'' in *Proc. IEEE 62nd Int. Midwest Symp. Circuits Syst. (MWSCAS)*, Aug. 2019, pp. 852–855.

[96] C. Profentzas, M. Gunes, Y. Nikolakopoulos, O. Landsiedel, and M. Almgren, ''Performance of secure boot in embedded systems,'' in *Proc. 15th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, May 2019, pp. 198–204.

[97] *Overview of the Internet of Things*. Accessed: Sep. 23, 2019. [Online]. Available: https://www.itu.int/rec/T-REC-Y.2060-201206-I/es

[98] M. Howard, J. Pincus, and J. M. Wing, ''Measuring relative attack surfaces,'' in *Computer Security in the 21st Century*. Boston, MA, USA: Springer, 2005, pp. 109–137.

[99] J. R. C. Nurse, S. Creese, and D. De Roure, ''Security risk assessment in Internet of Things systems,'' *IT Prof.*, vol. 19, no. 5, pp. 20–26, 2017.

[100] M. Fagan, K. Megas, K. Scarfone, and M. Smith, ''Core cybersecurity feature baseline for securable IoT devices: A starting point for IoT device manufacturers,'' Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 825919, 2019.

[101] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, ''Security and privacy in smart cities: Challenges and opportunities,'' *IEEE Access*, vol. 6, pp. 46134–46145, 2018.

[102] U. M. Mbanaso, L. Abrahams, and O. Z. Apene, ''Conceptual design of a cybersecurity resilience maturity measurement (CRMM) framework,'' *Afr. J. Inf. Commun.*, no. 23, pp. 1–26, Jun. 2019.

[103] B. P. Weeserik and M. Spruit, ''Improving operational risk management using business performance management technologies,'' *Sustainability*, vol. 10, no. 3, p. 640, Feb. 2018.

[104] A. M. Rea-Guaman, I. D. Sanchez-Garcia, T. S. Feliu, and J. A. Calvo-Manzano, ''Maturity models in cybersecurity: A systematic review,'' in *Proc. 12th Iberian Conf. Inf. Syst. Technol. (CISTI)*, Jun. 2017, pp. 1–6.

[105] J. D. Christopher, D. Gonzalez, D. W. White, J. Stevens, J. Grundman, N. Mehravari, and T. Dolan, "Cybersecurity capability maturity model (C2M2)," Dept. Homeland Secur., Washington, DC, USA, Tech. Rep. CMU/SEI-2015-TR-009, 2014, pp. 1–76.

[106] S. N. G. Gourisetti, M. Mylrea, T. Ashley, R. Kwon, J. Castleberry, Q. Wright-Mockler, P. McKenzie, and G. Brege, "Demonstration of the cybersecurity framework through real-world cyber attack," in *Proc. Resilience Week (RWS)*, vol. 1, Nov. 2019, pp. 19–25.

[107] M. D. E.-C. E. Kettani and T. Debbagh, "NCSECMM: A national cyber security maturity model for an interoperable national cyber security framework," in *Proc. 9th Eur. Conf. E-Government*. London, U.K.: UnivWestminister Business School, 2009, pp. 236–247.

[108] A. Aliyu, L. Maglaras, Y. He, I. Yevseyeva, E. Boiten, A. Cook, and H. Janicke, "A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom," *Appl. Sci.*, vol. 10, no. 10, p. 3660, May 2020, doi: 10.3390/app10103660.

[109] P. Katsumata, J. Hemenway, and W. Gavins, "Cybersecurity risk management," in *Proc. Mil. Commun. Conf.*, 2010, pp. 890–895.

[110] P. D. Curtis and N. Mehravari, "Evaluating and improving cybersecurity capabilities of the energy critical infrastructure," in *Proc. IEEE Int. Symp. Technol. Homeland Secur. (HST)*, Apr. 2015, pp. 1–6.

[111] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for SCADA systems," *Comput. Secur.*, vol. 56, pp. 1–27, Feb. 2016.

[112] S. Ahuja and J. Goldman, "Integration of cobit, balanced scorecard and SSE-CMM as a strategic information security management (ISM) framework," in *Proc. CEUR Workshop*, vol. 456, 2009, p. 1.

[113] J. Bugeja, B. Vogel, A. Jacobsson, and R. Varshney, "IoTSM: An end-to-end security model for IoT ecosystems," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2019, pp. 267–272.

[114] S. Schneider, "The industrial Internet of Things (IIoT) applications and taxonomy," in *Internet of Things and Data Analytics Handbook*. Hoboken, NJ, USA: Wiley, 2017.

[115] B. Bsi, *PAS 180: 2014-Smart Cities–VocabularyBSI Standards Publication, 2014a*, Standard PAS 180:2014, BSI, Feb. 2014, p. 40.

[116] M. Bada and J. R. Nurse, "The social and psychological impact of cyberattacks," in *Emerging Cyber Threats and Cognitive Vulnerabilities*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 73–92.

[117] R. Ch, T. R. Gadekallu, M. H. Abidi, and A. Al-Ahmari, "Computational system to classify cyber crime offenses using machine learning," *Sustainability*, vol. 12, no. 10, p. 4087, May 2020, doi: 10.3390/su12104087.

[118] N. Nicolaou, D. G. Eliades, C. Panayiotou, and M. M. Polycarpou, "Reducing vulnerability to cyber-physical attacks in water distribution networks," in *Proc. Int. Workshop Cyber-Phys. Syst. Smart Water Netw. (CySWater)*, Apr. 2018, pp. 16–19.

[119] A. Laugé, J. Hernantes, and J. M. Sarriegi, "Critical infrastructure dependencies: A holistic, dynamic and quantitative approach," *Int. J. Crit. Infrastruct. Protection*, vol. 8, pp. 16–23, Jan. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S187454821400081X

ROBERTO OMAR ANDRADE (Member, IEEE) received the degree in electronics and telecommunications engineering from Escuela Politécnica Nacional (EPN), in 2007, and the master's degree in network and telecommunications management from the Army Polytechnic School (ESPE), in 2013. He is currently pursuing the Ph.D. degree in security systems with the School of Systems Engineering, EPN. He worked in the security areas of the Ministry of Education of Ecuador (MINEDUC) SENPLADES. He has been a certified Technical Instructor of CCNA, CCNP, and CCNA Security with EPN, since 2010.

SANG GUUN YOO (Senior Member, IEEE) received the Ph.D. degree from the Department of Computer Science and Engineering, Sogang University, Seoul, South Korea, in 2013. From 2005 to 2007, he collaborated as a Professor with the Department of Computer Science and Multimedia, International University of Ecuador. From 2006 to 2007, he also worked as an IT Consultant with the Army Intelligence Agency of Ecuador. He also had the opportunity to work as a Chief Research Engineer with LG Electronics, South Korea. He is currently a Professor with the Departamento de Informática y Ciencias de la Computación, Escuela Politécnica Nacional. He is also working as the Director of the SmartLab. He is one of the co-founders of ExtremoSoftware (Microsoft Gold Certified Partner), where worked as the CTO from 2001 to 2005. He is also a National Contact Point of European Commission's H2020 Programme and SCIEI Senior Member.

LUIS TELLO-OQUENDO (Member, IEEE) received the degree (Hons.) in electronic and computer engineering from the Escuela Superior Politécnica de Chimborazo (ESPOCH), Ecuador, in 2010, the M.Sc. degree in telecommunication technologies, systems, and networks, and the Ph.D. degree *(cum laude)* in telecommunications from the Universitat Politècnica de València (UPV), Spain, in 2013 and 2018, respectively.

In 2011, he was a Lecturer with the Facultad de Ingeniería Electrónica, ESPOCH. From 2013 to 2018, he was a Graduate Research Assistant with the Broadband Internetworking Research Group, UPV. From 2016 to 2017, he was a Research Scholar with the Broadband Wireless Networking Laboratory, Georgia Institute of Technology, Atlanta, GA, USA. He is currently an Associate Professor with the College of Engineering, National University of Chimborazo, Ecuador. His research interests include wireless communication, software-defined networks, 5G and beyond cellular systems, the Internet of Things, and machine learning. He is a member of ACM. He received the Best Academic Record Award from the Escuela Técnica Superior de Ingenieros de Telecomunicación, UPV, in 2013, and the IEEE ComSoc Award for attending the IEEE ComSoc Summer School at The University of New Mexico, Albuquerque, NM, USA, in 2017.

IVÁN ORTIZ-GARCÉS received the master's degree in communications networks from the Pontificia Universidad Católica del Ecuador (PUCE). He is currently pursuing the Diploma degree in forensic informatics with UNIR, Spain. He also works as a Lecturer with the Information Technology Engineering Career, Universidad de las Américas. He has more than 20 years of professional experience in information technology in private and public institutions, such as the Judicial Council, the Ministry of Education, and the Electricity Corporation of Ecuador (CELEC EP).