

Received 21 June 2023, accepted 15 August 2023, date of publication 11 September 2023,  
date of current version 20 September 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3313975

 SURVEY

# Quantifying IoT Security Parameters: An Assessment Framework

SHOUKI A. EBAD 

Department of Computer Science, Faculty of Science, Northern Border University, Arar 91431, Saudi Arabia

e-mail: shouki.abbad@nbu.edu.sa


This work was supported by the Deanship of Scientific Research with Northern Border University, Arar, Saudi Arabia, under Project NBU-FFR-2023-0083.

**ABSTRACT** Several attempts have been made to propose metrics that quantify the parameters of existing solutions to improve the security of IoT systems. This paper presents a framework to classify and compare these metrics based on a set of attributes that can be used to answer the research questions. Forty-six metrics from the literature were analyzed, classified, and compared according to the developed framework. They were divided into two main categories according to the metric's source, i.e., internal and external sources. Then, they were further divided into seven sub-categories: size, time, numbering/scoring, checklist, blockchain, device integration effort, and legislation. There are eight widely used metrics among the existing IoT solutions: throughput, packet loss rate, jitter, password, security transmission rate, resilience, average energy consumption, and blockchain-related metrics (i.e., technical metrics). The simulation technique is the most common validation method among the current IoT solutions. Furthermore, the results revealed a gap in four aspects of proposing metrics for measuring security parameters. These aspects include the network/transport IoT layer, blockchain, legislation, and the use of data science in simulation research methodologies.

**INDEX TERMS** IoT, metrics, security, measurement, blockchain, framework.

## I. INTRODUCTION

The Internet of Things (IoT) is a global system of tools and mechanisms for connecting anything at any time and place. They can be connected to the Internet and other devices [1]. The IoT has developed faster than expected, playing a significant role in the real world [2]. The IoT system comprises a sensing unit with sensors, actuators, and mobile terminals. This simple architecture makes IoT devices vulnerable to security issues due to the heterogeneous nature of the devices and their limited resources, which are drastically increasing [1]. In addition, IoT companies launch their products focusing mainly on innovation and ease of use to capture the market share while paying less attention to security [3]. However, most of the security technologies adopted currently do not identify the source of an attack. They mainly inform users about the technical aspects of the attack [1].

The associate editor coordinating the review of this manuscript and approving it for publication was Byung-Seo Kim .

Also, conventional host-based protection methods, such as anti-virus, IDS, and IPS, cannot be used for smart devices [3]. One of the main gaps observed in this area of study is that less attention is given to standard metrics that represent a qualitative or quantitative level of reporting the security attribute of IoT systems. Therefore, promptly collecting the relevant metrics can benefit IoT technical professionals who regard this process as a preventative measure that will reduce future issues.

This paper defines the criteria for this process by proposing an attributed-based assessment framework that assists security organizations and IoT engineers in measuring the security level of their systems, including smart appliances and wearable devices. The collected metrics can be stored as a log file for further analysis or advanced security testing. They can be divided into two main categories according to their source: (a) metrics from an internal source, i.e., those related to the technical characteristics of IoT systems such as memory usage and transmissions, and (b) metrics from

an external source, i.e., those associated with regulations and laws including the organization or buying IoT solutions.

Nowadays, IoT technologies (first category) are not more important than metrics from an external source (second category). This is because the legal framework should be created before the system is completely operable, allowing an effective introduction to new architecture [4]. Despite the attempts made by different states, no standardized legislation and data security policies have been drafted until recently [3]. The reader is supposed to be familiar with the abbreviations of IoT security, protocols, and standards (e.g., IDS, IPS, BLE, TCP, UDP, MQTT, ISO/IEC, and NIST).

This paper is organized as follows. First, related research is presented in Section II. Next, the research approach, including the research questions (RQs), is discussed in Section III. Section IV presents the analysis results and the answers to this study's RQs. Then, Section V discusses the threats to the validity of this study. Finally, this study's conclusion is discussed in Section VI.

## II. RELATED RESEARCH

Several metrics are used or have been proposed for use in existing IoT solutions. Reference [5] identified the requirements for smart home systems and defined two mechanisms that aid the systems' auto-management: (1) supporting auto-configuration of the system would improve its security, and (2) automatically updating software and firmware is necessary for maintaining the constant and secure operation of the system. Moreover, [6] described the data science challenges encountered when attempting to enhance IoT application quality assurance (QA). They outlined these QA requirements and grouped them into six categories: environment, user, compliance or service agreement, organization, security, and data management. These challenges have four additional categories: defect prevention and analysis, user integration, and organization.

Additionally, [7] reviewed available studies and compared the IoT solutions that are applicable to mobile network security. They also presented various challenges, such as applications, features, technologies, standards, and open issues. Reference [8] reviewed 32 ETSI and 80 ISO/IEC security standards and 37 frameworks, including 7 NIST security publications. The study revealed the lack of assessment frameworks and standards for addressing the security requirements of IoT-based systems. Reference [9] reviewed the current IoT-enabling middleware solutions in terms of their application areas, architecture, components, communication APIs, and security property support, such as access control, filtering, and authorization. This allows developers to select the middleware that best matches their requirements.

Reference [10] conducted a survey and literature review that identified 21 security factors mapped in four domains (i.e., smart cities, homes, wearables, and health care). They used the fuzzy-AHP method, rather than cryptographic algorithms, to rank the factors in order of their importance to IoT

technology security. In addition, [11] presented an EEG signal-based authentication algorithm for remote IoT health-care. The algorithm is fast, robust, and multilayered because it uses feature extraction and requires an extended processing time. Due to its dynamic nature, a modified Euclidean distance pattern algorithm was suggested to match the EEG signal in the identification phase. Then, [12] discussed the economic aspects of IoT systems, including investments, company and consumer benefits, risks, and blockchain use. They also analyzed the top 10 IoT security features from the Open Web Application Security Project (OWASP) and best practices for addressing these issues. Reference [13] provided insight into IoT security and privacy issues and recommended some solutions. They highlighted problems that need to be addressed in the future.

Moreover, [14] explored literature related to blockchain-enabling IIoT, its challenges, and solutions. Then, they proposed a blockchain-enabling framework that provides a secure execution environment. Finally, they designed codes and consensus algorithms that supply industrial nodes, streamline transactions, and broadcast content effortlessly. This framework was simulated to validate information exchange among connected IIoT devices with limited resources. Reference [15] outlined security attacks on three-layer IoT architecture (i.e., application, network, and perception) and provided solutions. The paper compared multiple solutions and highlighted the most effective solution for a certain attack on a specific layer. Furthermore, [3] presented an overview of software-defined network (SDN) and SDN-based IoT deployment models (i.e., centralized and decentralized models). They elaborated on SDN-based IoT security frameworks and provided an overview of software-defined security (SDSec) technology. Finally, they highlighted the challenges of IoT applications.

In conclusion, the review articles discussed above did not focus on measuring IoT parameters. The reviews were conducted from a technological perspective [3], [7], [9], [11], [14]. Some studies reviewed a particular application perspective, like smart homes, cities, or healthcare [5], [11]. Certain studies focused on IoT QA [3], [6], [8], while many others performed generic surveys on the factors influencing IoT security [3], [7], [10], [12], [13], [15]. Therefore, as far as we know, this study is the first to compare and discuss the existing metrics that quantify IoT parameters.

## III. RESEARCH APPROACH

This section describes the research approach utilized in this study.

### A. STUDY OBJECTIVES AND RESEARCH QUESTIONS

Interest in IoT and its applications is increasing. IoT companies have been interested in employing metric-based security testing, where application creators can focus more on the creative processes that could advance the IoT experience. Companies prefer this over checking the security manually, which is time- and effort-consuming. Therefore, having an

agent that can automatically measure the attribute security of IoT systems would rapidly increase the system's quality.

This research's key objective is to investigate and compare the measuring mechanisms of IoT security-related parameters and their goals. A critical evaluation and analysis are conducted using an established attribute-based framework to find answers to the RQs. Additionally, this paper discusses some gaps in the literature to extend the work in this field further.

This study helps to find answers to the following RQs:

RQ1: What are the characteristics of the available metrics quantifying the IoT parameters that would benefit attribute security?

RQ2: Which metrics are the most widely used among the existing IoT solutions?

RQ3: How do researchers apply or validate their metrics?

RQ4: Which attack types can the metrics detect?

RQ5: What are the possible directions for future research?

## B. SEARCH STRATEGY

Studies from the relevant scientific literature were collected to answer the above RQs. The focus was on three databases and search engines: Google Scholar, IEEE Explorer, and Semantic Scholar. The following search strings were used to gather the related studies:

(IoT OR IOT OR "internet of things") AND (metrics OR measures) AND security

## C. STUDY SELECTION AND QUALITY ASSESSMENT

This study applies a four-phase approach known as PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) statement. The phases of the PRISMA statement [16] include identification, screening, eligibility analysis, and inclusion.

In the identification phase, resources were collected from the selected databases (i.e., Google Scholar, IEEE Explorer, and Semantic Scholar). Then, the titles and abstracts of publications were reviewed in the screening phase. In the eligibility analysis phase, the selected articles were thoroughly studied. Finally, in the inclusion phase, the articles selected from the eligibility analysis phase were utilized to find the security metrics of IoT parameters.

The final selection process involved using the following quality assessment criteria with inclusion and exclusion policies: (a) The inclusion criteria includes two study types, studies written in English and articles proposing IoT security solutions with mentioned metrics; (b) The exclusion criteria excludes two study types, studies discussing topics unrelated to IoT security, such as stand-alone application security, and studies that are duplicates of other studies.

## D. INFORMATION EXTRACTION

A well-structured comparison framework was established to extract reliable information and manage the extraction process. This process helps with finding answers to the RQs.

In addition, there are specific attributes that the comparison framework examines for each RQ. These attributes are grouped according to the RQs described in Table 1.

## IV. RESULTS AND DISCUSSION

This section describes the results and observations from analyzing the articles and answering the RQs.

### A. RQ1: WHAT ARE THE CHARACTERISTICS OF THE AVAILABLE METRICS QUANTIFYING THE IOT PARAMETERS THAT WOULD BENEFIT ATTRIBUTE SECURITY?

The articles from the literature provided various metrics for quantifying IoT security parameters. To differentiate the metrics, the studies were categorized according to their sources, i.e., internal (i.e., technical) and external sources (i.e., non-technical). The details of the metrics in each category are discussed in this section.

#### 1) THE INTERNAL SOURCE METRICS OR TECHNICAL ASPECTS

Internal source metrics focus on retrieving a value from the IoT technical environment. Unlike software engineering, internal source metrics are sometimes difficult to measure in IoT systems due to their complexity. Many internal source metrics were used in the solutions literature because several IoT products can be tested in an automated manner. This method involves technical metrics, such as memory usage, the number of successful transmissions, and identifying the IoT devices. Although most of the studies focused on detecting IoT security issues, the metrics' goals varied, even though their ultimate goal was to improve IoT security. For instance, some metrics aimed to quantify the Interrupt Service Routine (ISR) latency [18], [19], while others used scoring mechanisms to estimate the difficulty level of implementing certain solutions to an IoT system [1], [20]. In contrast, some metrics employed expiration dates to control interface passwords and update software, middleware, and firmware [1], [21].

#### 2) THE EXTERNAL SOURCE METRICS OR NON-TECHNICAL ASPECTS

As the name suggests, external source metrics are not concerned with IoT's technical aspects. They often arise through user requirements based on organizational rules, the need for interoperability with other enterprises' systems, or external factors such as safety policies and privacy legislation. Several studies proposed external source metrics. For example, [4] proposed several metrics for implementing IoT laws, while others suggested measuring the effort required for integrating IoT devices, including human effort [22]. This metric is difficult to quantify because the responsibilities, meanings, and measurements differ. Besides, there is no consensus regarding the most effective measure for this metric.

Although external metrics can be very helpful in preventing future issues, IoT security engineers sometimes regard them as unimportant since they are mainly interested in the IoT's functionality. Table 2 presents the 46 metrics

**TABLE 1. The study’s RQs and corresponding framework’s attributes.**

RQ	The corresponding framework’s attribute	
	Attribute name	Attribute description
RQ1: What are the characteristics of the available metrics quantifying the IoT parameters that would benefit attribute security?	Metric name	This attribute lists the metrics used to measure an IoT security parameter in the proposed solutions of the relevant studies.
	Metric goal	This attribute presents the metric objectives. There might be different objectives for measuring, such as testing the security’s functionalities and enhancing the performance level.
RQ2: Which metrics are the most widely used among the existing IoT solutions?	Quantification	This involves whether the metric captures quantitative (i.e., numbers) or qualitative information (i.e., opinions and beliefs). Expressing the metric as a number makes it more useful [17].
	Source	This attribute determines whether the metric comes from an internal (i.e., the technical aspect) or external source (i.e., the non-technical aspect). IoT is a cross-disciplinary subject with various topics, including technical issues like networks, operating systems, storage, and analytics and non-technical issues like policies.
RQ3: How do researchers apply or validate their metrics?	Underlying Principle	Understanding the metric well involves understanding the underlying principle upon which the solution is built.
	Supportability	This attribute concentrates on the availability of the solution’s code used with the metric, i.e., open or closed source project, real-world system, simulation, supported by automation, or integrated with tools.
RQ4: Which attack types can the metrics detect?	Applicability Layer	This refers to the granularity level, i.e., in which IoT layer does the metric work, the perception, network, or application layers.
	Attack related	This attribute defines whether the metric is defending against specific or general threats.
RQ5: What are the possible directions for future research?	This RQ identifies the research gaps in measuring IoT parameters. It is answered by analyzing the related studies and recommending further research.	

categorized according to their sources, i.e., internal and external. They are further divided into sub-categories. The five sub-categories for internal source metrics include size, time, numbering/scoring, checklist, and blockchain. For external sources, the sub-categories are device integration effort and legal metrics.

**B. RQ2: WHICH METRICS ARE THE MOST WIDELY USED AMONG THE EXISTING IOT SOLUTIONS?**

In this section, we consider the most widely used metrics according to their uses in multiple studies. Table 3 shows the 12 internal source metrics that are the most widely used. These metrics are distributed over three sub-categories. First, the size sub-category includes three metrics: throughput, blockchain transactions per second, and blockchain or block size. The time sub-category includes four metrics: jitter, password dates, and blockchain propagation and generation time. Finally, the mathematical expression sub-category includes five metrics: packet loss and transmission ratio, IoT resilience, average energy consumption, and average number of miners or validators.

More explanations and observations regarding these metrics are provided in the next section.

**1) THE MOST WIDELY USED SIZE-BASED TECHNICAL METRICS**

**• Throughput**

Throughput, the first widely used size-based metric, is the amount of data transmitted and received successfully during

a specific period [23]. In terms of blockchain technology, it is the number of transactions per second [24]. This metric is essential for IoT solutions focused on security because it is the most likely to be affected if the proposed solution requires a computation overhead on the system. In other words, it indicates a solution’s effect on the IoT environment’s efficiency.

**• Transactions per second and block size (i.e., blockchain metrics)**

The other two size-based widely-used metrics, transaction per second and block size are for blockchain-based solutions. The former is equivalent to throughput, while the latter represents the amount of data stored in a block. Block size is a vital metric that should be defined for any blockchain-based IoT solution, as it directly impacts performance. This is because scalability bottlenecks can reduce the throughput, leading to congestion. Finding a suitable block size is still challenging for all blockchain-based IoT solutions [25].

**2) THE MOST WIDELY USED TIME-BASED TECHNICAL METRICS**

**• Jitter**

Jitter is the time it takes for a packet to travel across a network and is often caused by congestion. Although latency is among the existing metrics (i.e., number 10 in Table 2), jitter is more widely used than latency. The main distinction between the two is that latency is a delay through the network, whereas jitter is a change in the latency amount [23].

TABLE 2. List of metrics and their classifications.

#	Class	Sub-class	Used metrics
1	Technical metrics/Internal aspect	Size-based	Throughput
2			Blockchain transactions per second
3			Blockchain size
4		Time-based	Jitter period
5			Password dates
6			Blockchain propagation time
7			Blockchain generation time
8			Size of the encrypted file
9			Encryption time
10			Latency/delay
11			Round trip time (RTT)
12			The time it takes to send security patches and software updates to IoT devices
13			Expiration dates for updating processes
14			The time the attacker’s packet reached the controller
15			The time the victim detected the attack
16			The time the first controller discovered the attacking information
17			The time the flow entries were installed in a switch
18		The time a controller received the attacking information from another controller	
19		The time it detected a threat to when the new defenses were running	
20		Scalability: time needed to start up a new μmbox <sup>1</sup> when changing security states	
21		Authenticating latency	
22		Mathematical expression	Packet loss ratio
23			Packet transmission ratio
24			IoT resilience
25			Average energy consumption
26			Average number of miners/validators
27			The number of login attempts by the user
28			Allocation of resources: The bandwidth ratio of legal traffic to the bandwidth of attack traffic $\text{Allocation of resources} = \frac{\text{legitimate traffic BW}}{\text{attack traffic BW}} \quad (1)$
29			Percentage of failed transactions (pft): This is an attack impact measure for each application’s pft on an IoT device. Formally, pft is defined as $\text{pft} = \frac{\text{failed transactions}}{\text{total number of transactions}} \times 100 \quad (2)$
30			Open port risk: A metric score used to assess the risk level of open ports. The risk level is set as: 0 – safe, <15 – minor risk, 15>&&<30 – major risk, and >30 – critical risk
31			Rank: each node in the network has an assigned rank number
32		Data reputation score: The score of a node is calculated based on a reputation assessment model	
33		Checklist	Utility: - Does an app have access to the camera? - Can an app record audio? - Does an app have access to sensors measuring the user’s attributes (e.g., health condition)? - Does an app recognize when a user performs an activity?  Authentication: - Does an app have access to authentication tokens? - Can an app access or handle the account authenticator?  Location: - Does an app learn the precise location of the user? - Does an app access the approximate location of the user? - Does an app access the user’s location while running in the background? - Does an app have access to any geographic location in the user’s shared collection?  Storage: - Can an app read and write from and to the device’s external storage (e.g., an SD card)?

<sup>1</sup> From an SDN perspective, micro-network security functions (μmbox) act as gateways for each IoT device. All requests to and from the IoT devices must go through this μmbox software, which allows for a central administration policy [15].

TABLE 2. (Continued.) List of metrics and their classifications.

			<ul style="list-style-type: none"> <li>- Can an app request and install packages?</li> <li>- Can an app permit mounting or unmounting a removable storage's files?</li> </ul> <p>Phone</p> <ul style="list-style-type: none"> <li>- Can an app read the phone's state, including the cellular network and any active calls the user has made?</li> <li>- Can an app create windows on top of already running apps?</li> <li>- Can an app read or write to and from the user's contacts or device's phone numbers?</li> <li>- Can an app read or write access to the device's system settings?</li> <li>- Can an app retrieve information about current and recent running tasks?</li> <li>- Can an app read from low-level system log files?</li> <li>- Can an app read or write to and from the user's calendar data?</li> </ul> <p>Communication</p> <ul style="list-style-type: none"> <li>- Can an app receive, read, or send SMS/MMS?</li> <li>- Can an app read from the user's call log?</li> <li>- Can an app make a phone call without the user's permission?</li> <li>- Can an app use the Session Initiation Protocol (SIP) service?</li> <li>- Can an app answer phone calls?</li> <li>- Can an app learn the number being dialed for an outgoing call?</li> </ul> <p>Networking</p> <ul style="list-style-type: none"> <li>- Does an app trust the user-installed certificates?</li> <li>- Are there third-party trackers (e.g., for crashing, marketing, ads, and analytics)?</li> <li>- Is there an additional encrypted protocol as a cover for MQTT or CoAP?</li> </ul>
34		Blockchain technology	End-to-end delay: The queuing, processing, and transmission delay average
35			Access time
36			Block transmission rate
37			Mining or reading time per block
38			Blocks per second
39			Transaction latency
40			Transaction packaging time
41			Transaction overhead
42			Transaction throughput
43			Transaction confirmation overhead
44			Hash rate or quality
45	Non-technical metrics/ external aspect	Device integration effort	Device research (i.e., network traffic and vulnerabilities)
			Policy design and implementation
			API understanding and implementation
			Human factors and security experts for adding new device types to the platform
46		Legal metrics (Checklist)	<ul style="list-style-type: none"> <li>- Is international or national state law available?</li> <li>- Are the market laws of the concerned businesses sufficient?</li> <li>- What is the time frame for the new law's implementation?</li> <li>- Can individuals disconnect from their networked environment or deactivate their tags anytime?</li> <li>- Which entity within the IoT architecture can be held liable should privacy or confidentiality violations occur?</li> </ul>

• Password dates

According to the relevant studies, this metric has two forms: (a) password expiration dates and (b) password complexity. This is determined by the time it takes to recover the password, e.g., none, unknown, very low, low, and medium. These two forms reduce the chance of a successful password attack using manual guessing or automated tools [26].

• Block propagation and generation time (i.e., blockchain metrics)

Block propagation and generation time are the final two metrics in this class for blockchain-based solutions. While the first metric represents the time it takes for the block to propagate from node to node, the second is the interval for

inserting a new block into the blockchain. Suppose the block generation time is 10 minutes (as on the Bitcoin platform); a new block will be added to the blockchain approximately every 10 minutes. In general, block generation time should be minimized as much as possible.

3) THE MOST WIDELY USED MATHEMATICAL EXPRESSION-BASED TECHNICAL METRICS

• Packet loss ratio

The packet loss ratio is the packets lost in the transmission to the total number of sent packets [23]. Like jitter, packet loss ratio is an indicator of network congestion.

TABLE 3. The most widely-used metric.

#	Class	Sub-class	Used metrics
1	Technical metrics/Internal aspect	Size-based	Throughput
2			Blockchain transactions per second
3			Blockchain or block size
4		Time-based	Jitter
5			Password dates
6			Blockchain propagation time
7			Blockchain generation time
8		Mathematical expression	Packet loss ratio
9			Packet transmission ratio
10			IoT resilience
11			Average energy consumption
12			Average number of miners or validators

#### • Packet transmission ratio

The packet transmission ratio is the number of successful transmissions to the number of total transmissions. The higher the value of this metric, the stronger the security. For instance, [27] used this metric to measure general security in terms of the transmission rate in the proposed IoT solution, SDN. When the simulation time was increased, the security transmission rate did not show a steep downward trend like the traditional SDN. This is because the proposed security module was inserted among the SDN architecture, which can filter unsafe events and ensure a safe transmission rate.

#### • IoT resilience

Before defining the resilience of a device (the third metric in this class), it is necessary to understand the permeance of the IoT device,  $P_{IoT}$ , against an attack.  $P_{IoT}$  is the total number of packets a device can service while bombarded with attack<sup>2</sup> packets before it stops providing the service. Formally, it is calculated as follows:

$$P_{IoT} = S \times \frac{P_n \times P_a}{T_{RRT}} \quad (3)$$

$P_n$  is the total number of normal packets,  $P_a$  is the number of attack packets,  $T_{RRT}$  is the request-response time of the IoT device, and  $S$  is the resilience constant specific to an IoT device's vulnerability. The unit of permeance is  $\frac{P^2}{S}$ , where  $P$  is the number of packets, including the normal and attack packets. Therefore, an IoT device's resilience indicates whether the platform can detect and react appropriately to the configured attacks. Thus,  $R_{IoT}$  is defined as the reciprocal of the device's permeance:

$$R_{IoT} = \frac{1}{P_{IoT}} \quad (4)$$

where  $R_{IoT}$  is the IoT device's resilience and the unit is  $\frac{S}{P^2}$ .

<sup>2</sup>Specifically, DoS and DDoS attacks.

#### • Average energy consumption

The metric is based on the importance of energy. In 2018, information and communication technology (ICT) was estimated to consume 3% of energy worldwide<sup>3</sup>. This amount is estimated to increase at a rate of 9% per year [28]. More energy is expected to be consumed with IoT systems because they depend on prompt data collection from many wireless sensors that can operate for several years without human intervention. These sensors use batteries as their sole energy source. According to [29], 75.44 billion devices are predicted to be connected to the Internet by 2025, producing approximately 80 zettabytes of data.<sup>4</sup> The relationship with energy consumption has come from the fact that attack-detection systems at the initial stage allow for a reduction of energy consumption so that a malicious node would require more computational power than others.

Several ongoing attempts have been made to reduce energy consumption while satisfying the latency requirement. These attempts relied on different technologies such as intelligent data compression [30], [31], strategic clustering [32], [33], energy-aware routing [34], mobile fog computing to suppress energy consumption [35], and deep learning [36]. Therefore, IoT systems should monitor the average energy consumption metric periodically, considering all the energy expenditures in the system that can be empirically quantified.

#### • Number of miners (for blockchain solutions)

In a blockchain-based solution, when any transaction needs to be added to the chain, it must be tested by several "miners." One of the most renowned methods for proving a transaction is proof of work (PoW). This solution, suggested by the original PoW-based blockchain (i.e., Bitcoin) [37], avoids the measured attacks, as it needs miners to implement computationally expensive processes to be elected as validators. As mentioned in the previous metric (energy consumption), a victim node is expected to have more computational power than all the others. The "work" necessary for a PoW-based consensus involves performing heavy mathematical operations (i.e., mining). For the Bitcoin model, this metric is measured by finding the average number of miners used to test the data transactions.

#### • Security versus performance metrics

No IoT solution can achieve high performance and security levels, highlighting the trade-off between these quality attributes. In addition, any IoT solution that addresses performance concerns implicitly tackles security issues and vice versa. In other words, several metrics focused on assessing the performance of IoT systems also measure the security attribute. For instance, flow metrics such as packet loss rate,

<sup>3</sup>The shift project. "Lean ICT: Towards Digital Sobriety". Available from: <https://theshiftproject.org/en/article/lean-ict-our-new-report/>, October, 2018

<sup>4</sup><https://www.globaldots.com/resources/blog/41-6-billion-iot-devices-will-be-generating-79-4-zettabytes-of-data-in-2025/> (Accessed on September, 10, 2023)

throughput, jitter, and round trip time (RTT)<sup>5</sup> also measure IoT security. This is because the attack detection mechanism often indicates an attack by increasing the packet loss rate, jitter, or RTT and decreasing the throughput. Similarly, in a blockchain-based solution, the higher the block generation time and transaction latency, the higher the probability of the IoT device being attacked.

### C. RQ3: HOW DO RESEARCHERS VALIDATE THEIR METRICS?

Answering this question requires understanding the available validation methods and when they can be applied. IoT stems from the technical community. Thus, it is expected to explore the validation methods of metrics used for research in networking and software or systems engineering.

All the metrics used in the current IoT security solutions were validated empirically (i.e., not theoretically). This is expected because some of these metrics are well-known and were used before the IoT began in different computing areas like networking, software, and systems engineering. However, most of the studies are limited because they depended on a single empirical validation method, i.e., the simulation strategy [1], [19], [22], [24], [27], [38], [39], [40], [41], [42]. Thus, they neglected theoretical validation. Only one study applied the solution to a real-world IoT system, the Väre building at the Aalto University campus [2]. Some researchers used Eclipse<sup>6</sup> (IV-B3)(IV-B3)(IV-B3)(IV-B3) [27], [39], while others used free RTOS (real-time operating system) [18]. FreeRTOS<sup>7</sup> is a renowned operating system embedded in IoT computers.

In this case, the simulation strategy is used for conducting experiments similar to other technical fields, such as simulating a telecommunication network to assess its performance. In general, working with a real-life system from the market is a common limitation in many ICT research [44]. This system is not available even for research purposes. Consequently, this issue has been classified as one of the top 10 obstacles in empirical software engineering research [44]. The worst happens in an IoT environment because these technologies are still developing. Despite this, 24% of cybersecurity research in the last decade was performed using simulations [45].

### D. RQ: WHICH ATTACK TYPES CAN THE METRIC DETECT?

The basic IoT architecture is triple-layered. It comprises the perception, transport/network, and application layers [15], [46].

1. The perception layer: This layer works as an intermediary between the physical and digital contexts using sensors. Based on the application's requirements, the sensors capture various types of data from the environment, such as

<sup>5</sup>RTT (round time trip), Metric 11 in Table 2, is the time it takes for a signal to be submitted and the time it takes to acknowledge receiving the signal [23].

<sup>6</sup><https://www.eclipse.org/>

<sup>7</sup><https://www.freertos.org/>

temperature, humidity, and brightness. Besides security, this layer focuses on device identification and management.

2. The transport/network layer: This layer connects different devices to share information securely. It uses different communication standards, such as Ethernet, Wi-Fi, Wi-MAX, ZigBee, and BLE.

3. The application layer: This layer functions as a service provider for end users based on the requirements. For example, smart home applications offer home automation, smart farming, and surveillance services (including monitoring older people). This layer uses different protocols such as MQTT, CoAP, and XMPP.

Only a few solutions applied metrics to the transport/network layer (IV-B3)(IV-B3)(IV-B3) [39], [47]. Most solutions focused on the other two layers, perception and application [2], [20], [22], [24], [27], [41], [42], [48], [49], [50]. Security metrics in IoT must be considered for each layer to be reliable.

Because most solutions use metrics working at the IoT device and application layers, the attack types that the above metrics can detect are common, including DoS/DDoS, botnet, man-in-the-middle (MITM), replay, masquerade, home invasions, trespass, unintentional damage or loss, disasters and outages, failures or malfunctions, unsecured wireless network problems, side-channel, identity theft, physical, advanced persistent threats (APT), weak passwords, and software-level attacks including code injection, function creep, and buffer overflow<sup>8</sup> [2], [4], [19], [20], [27], [39], [40], [42], [47], [48], [51]. Only a few studies aim to detect particular types, such as brute-force, TCP and UDP port scans [22], and RPL attacks [49].

### E. RQ5: WHAT ARE THE POSSIBLE DIRECTIONS FOR FUTURE RESEARCH?

This assessment framework has revealed four areas for further research on the measurement of IoT parameters. The following is a brief discussion of each area, as they are not the focus of this paper.

#### 1) LEGAL METRICS

According to Table 2, the non-technical aspect/external source measurements did not receive as much research attention as the technical/internal metrics. Data damage or security breaches can come from technical and non-technical sources, such as policies, procedures, and legislation. For instance, a smart vehicle is operated progressively. Each time an accident occurs, its usage laws must be updated accordingly. Healthcare IoT systems also suffer from harmful user practices (e.g., misusing the devices) that have caused approximately 41% of security issues [9]. These two examples demonstrate the importance of proposing new legal metrics.

<sup>8</sup>For more details about the software-level attacks, interested readers are advised to consult the work of Ebad [45].



The technical community is not responsible for these issues. Instead, the top management officers, such as the high administration, ministries, and governmental authorities, must bear responsibility for these problems.

Certain issues are missing from the literature, such as the organizational and non-technical metrics for quantifying data ownership, human effort, user freedom, and service providers' use of personal information. Some questions arising from metrics 45 and 46 in Table 2 include:

- How can we measure the human effort necessary for adding and integrating new IoT devices into the platform?
- Can individuals disconnect from their networked environment and deactivate their tags anytime?
- Which organization within the IoT architecture can be held liable should privacy or confidentiality violations occur?

New legal responsibilities constantly arise due to IoT's introduction of smart services. Until now, no standardized legislation and data security rules have been drafted. Different entities, such as the Australian National Transport Commission<sup>9</sup> and the General Data Protection Regulation (GDPR<sup>10</sup>), have made several attempts to improve user data security. These regulations should be provided by IoT device manufacturers and software engineers while offering features such as health ones.

Legal metrics for IoT products remain a major challenge that must be addressed. This is because the actual legal regulations cannot always keep up with the rapidly developing IoT solutions and technologies in the market. Users trust manufacturers and developers to secure their IoT solutions. However, manufacturers and developers focus on quickly creating and releasing new products to meet the increasing market demands without having acceptable metrics that quantify security [8]. In addition, as IoT is a very complex and decentralized network, it is challenging to define security liabilities (i.e., unclear liabilities) [9] and derive common metrics.

## 2) BLOCK SIZE AND MINER NUMBERS IN BLOCKCHAIN SOLUTIONS

Scalability is a challenge for blockchain IoT solutions, especially with healthcare data. Therefore, the number of miners should be minimized to include experts for critical cases. While the old security systems check transactions through the available miners, the newly proposed schemes select the miners from various companies and locations. This rule stems from envisioning the transformation of the IoT healthcare system. Thus, integrating several health corporations into one large organization is beneficial for selecting miners from different locations, making the transaction verification more credible and secure. Furthermore, several researchers have

<sup>9</sup><https://www.ntc.gov.au/transport-reform/ntc-projects/changing-driving-laws-support-AVs>

<sup>10</sup><https://gdpr.eu/>

attempted to find the appropriate block size for the application being built.

## 3) PROPOSING NEW METRICS ACCORDING TO THE IOT DOMAIN

Proposing metrics to measure security parameters according to the application domains such as smart home, city, health-care, farming, and wearables is necessary. This is because of the IoT systems' heterogeneous protocols and dynamic characteristics. In other words, these domains have different protocols, standards, models, and characteristics [8], [36]. For example, ZigBee and RFID are two short-range communication standards. The former is useful for applications like smart homes and Industry 4.0, while the latter benefits production monitoring and control and supply chain management [36]. Therefore, developing IoT solutions with various domains provides excellent opportunities for proposing new metrics that monitor a solution project's progress.

## 4) USING DATA SCIENCE IN THE SIMULATION STRATEGY

Regarding the answer to RQ2, most studies used the simulation strategy to conduct experiments. Because IoT systems often produce large amounts of data for timely processing, applying data science techniques provides excellent opportunities for simulating the complex IoT environment. This is essential due to the variety and sheer numbers of IoT devices. Therefore, using mimic sensor data, middleware functionality, and communication is crucial for future IoT QA.

## V. THREATS TO VALIDITY

Certain issues are threatening the validity of this study's results. For example, ensuring that all the available, secure IoT solutions have been included in this study is difficult. There may be other solutions in the literature or industry that were not included. This issue was mitigated by considering studies from the most prominent literature databases (i.e., Google Scholar, IEEE Explorer, and Semantic Scholar) using identical search strings.

In this study, metrics for quantifying IoT security-related parameters were categorized using a creative research and development process. Therefore, the subjective nature of creativity imposes an additional validity risk.

The conclusions derived from this paper relied on a proposed comparison framework and its attribute list, displayed in Table 1. These attributes were used to compare the metrics found in the literature and answer the RQs. Furthermore, the framework and its attributes were proposed to cover the primary properties of IoT metrics used to quantify security parameters. However, others may introduce more attributes to further study and analyze IoT solutions.

## VI. CONCLUSION

This study investigated metrics used to quantify IoT security parameters in the literature. A framework based on several attributes was developed due to an extensive review of current IoT solutions. Accordingly, the considered RQs were

answered using the discussed assessment framework. As a result, 46 metrics found in the literature were analyzed, classified, and compared according to the developed framework. The metrics were divided into two main categories: the technical/internal and the non-technical aspect/external source. Then, they were further classified into six sub-categories: size, time, numbering/scoring, blockchain, human effort, and legislation.

The existing IoT solutions have eight widely used metrics: throughput, packet loss rate, jitter, password, security transmission rate, resilience, average energy consumption, and blockchain-related metrics. Furthermore, the simulation technique was the most common validation method in the current IoT solutions. The findings also revealed a gap in the proposal of metrics for measuring security parameters. This gap extends in four directions: network/transport IoT layer, blockchain, legislation, and use of data science in simulation research methodologies.

## REFERENCES

- [1] S. Siboni, V. Sachidananda, Y. Meidan, M. Bohadana, Y. Mathov, S. Bhairav, A. Shabtai, and Y. Elovici, "Security testbed for Internet-of-Things devices," *IEEE Trans. Rel.*, vol. 68, no. 1, pp. 23–44, Mar. 2019.
- [2] N. Yousefnezhad, A. Malhi, T. Keyriläinen, and K. Främpling, "A comprehensive security architecture for information management throughout the lifecycle of IoT products," *Sensors*, vol. 23, no. 6, p. 3236, Mar. 2023.
- [3] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10250–10276, Oct. 2020.
- [4] R. H. Weber and R. Weber, *Internet of Things Legal Perspectives*. Berlin, Germany: Springer, 2010.
- [5] H. Lin and N. Bergmann, "IoT privacy and security challenges for smart home environments," *Information*, vol. 7, no. 3, p. 44, Jul. 2016.
- [6] H. Foidl and M. Felderer, "Data science challenges to improve quality assurance of Internet of Things applications," in *Leveraging Applications of Formal Methods, Verification and Validation: Discussion, Dissemination, Applications*. Cham, Switzerland: Springer, Oct. 2016, pp. 707–726.
- [7] V. Sharma, I. You, K. Andersson, F. Palmieri, M. H. Rehmani, and J. Lim, "Security, privacy and trust for smart Mobile- Internet of Things (M-IoT): A survey," *IEEE Access*, vol. 8, pp. 167123–167163, 2020.
- [8] N. M. Karie, N. M. Sahri, W. Yang, C. Valli, and V. R. Kebande, "A review of security standards and frameworks for IoT-based smart environments," *IEEE Access*, vol. 9, pp. 121975–121995, 2021.
- [9] R. Kalaska and P. Czarnul, "Some security features of selected IoT platforms," *TASK Quart.*, vol. 24, no. 1, pp. 29–61, 2020.
- [10] M. A. Akbar, A. Alsanad, S. Mahmood, and A. Alothaim, "A multicriteria decision making taxonomy of IoT security challenging factors," *IEEE Access*, vol. 9, pp. 128841–128861, 2021.
- [11] S. Afsaneh, A. Sepideh, M. Ali, and A. Salah, "A two-layer attack-robust protocol for IoT healthcare security: Two-stage identification-authentication protocol for IoT," *IET Commun.*, vol. 15, no. 19, pp. 2390–2406, Dec. 2021.
- [12] M. M. Anghel, P. Ianc, M. Ileana, and L. I. Modi, "The influence of privacy and security on the future of IoT," *Inf. Economica*, vol. 24, no. 2, pp. 42–53, 2020.
- [13] P. Chauhan, S. Ahmad, P. R. Khan, and N. A. Khan, "Investigating the IoT security and privacy challenges: Summary and recommendations," *EAI Endorsed Trans. Cloud Syst.*, vol. 7, no. 22, p. e5, Aug. 2022.
- [14] A. Ayub Khan, A. A. Laghari, Z. A. Shaikh, Z. Dacko-Pikiewicz, and S. Kot, "Internet of Things (IoT) security with blockchain technology: A state-of-the-art review," *IEEE Access*, vol. 10, pp. 122679–122695, 2022.
- [15] M. S. Akhtar and T. Feng, "A systemic security and privacy review: Attacks and prevention mechanisms over IoT layers," *EAI Endorsed Trans. Secur. Saf.*, vol. 8, no. 30, pp. 1–12, 2022.
- [16] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *BMJ*, vol. 339, Jun. 2009, Art. no. b2535.
- [17] N. Fenton and J. Bieman, *Software Metrics: A Rigorous and Practical Approach*. Boca Raton, FL, USA: CRC Press, 2014.
- [18] N. Klingensmith and S. Banerjee, "Hermes: A real time hypervisor for mobile and IoT systems," in *Proc. 19th Int. Workshop Mobile Comput. Syst. Appl.*, Feb. 2018, pp. 101–106.
- [19] D. V. Medhane, A. K. Sangaiah, M. S. Hossain, G. Muhammad, and J. Wang, "Blockchain-enabled distributed security framework for next-generation IoT: An edge cloud and software-defined network-integrated approach," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6143–6149, Jul. 2020.
- [20] A. Koivu, L. Koivunen, S. Hosseinzadeh, S. Laurén, S. Hyrynsalmi, S. Rauti, and V. Leppänen, "Software security considerations for IoT," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Chengdu, China, Dec. 2016, pp. 15–18.
- [21] M. Sarrab and S. M. Alnaeli, "Critical aspects pertaining security of IoT application level software systems," in *Proc. IEEE 9th Annu. Inf. Technol., Electron. Mobile Commun. Conf. (IEMCON)*, Nov. 2018, pp. 960–964.
- [22] S. Echeverría, G. Lewis, C. Mazzotta, C. Grabowski, K. O'Meara, A. Vasudevan, M. Novakowski, M. McCormack, and V. Sekar, "KaKi: A software-defined IoT security platform," in *Proc. IEEE Virtual World Forum Internet Things*, New Orleans, LA, USA, Jun. 2020, pp. 2–16.
- [23] L. L. Peterson and B. S. Davie, *Computer Networks: A Systems Approach*. 5th ed. San Mateo, CA, USA: Morgan Kaufmann, 2011.
- [24] D. Na and S. Park, "IoT-chain and monitoring-chain using multilevel blockchain for IoT security," *Sensors*, vol. 22, no. 21, p. 8271, Oct. 2022.
- [25] N. Singh and M. Vardhan, "Computing optimal block size for blockchain based applications with contradictory objectives," *Proc. Comput. Sci.*, vol. 171, pp. 1389–1398, Jan. 2020.
- [26] S. A. Ebad, "Lessons learned from offline assessment of security-critical systems: The case of microsoft's active directory," *Int. J. Syst. Assurance Eng. Manage.*, vol. 13, no. 1, pp. 535–545, Feb. 2022.
- [27] X. Zuo, X. Pang, P. Zhang, J. Zhang, T. Dong, and P. Zhang, "A security-aware software-defined IoT network architecture," in *Proc. IEEE Comput., Commun. IoT Appl. (ComComAp)*, Beijing, China, Dec. 2020, pp. 20–22.
- [28] L. Guegan and A.-C. Orgerie, "Estimating the end-to-end energy consumption of low-bandwidth IoT applications for WiFi devices," in *Proc. IEEE Int. Conf. Cloud Comput. Technol. Sci. (CloudCom)*, Dec. 2019, pp. 287–294.
- [29] S. N. Swamy and S. R. Kota, "An empirical study on system level aspects of Internet of Things (IoT)," *IEEE Access*, vol. 8, pp. 188082–188134, 2020.
- [30] G. Li, S. Peng, C. Wang, J. Niu, and Y. Yuan, "An energy-efficient data collection scheme using denoising autoencoder in wireless sensor networks," *Tsinghua Sci. Technol.*, vol. 24, no. 1, pp. 86–96, Feb. 2019.
- [31] H. Harb and A. Makhoul, "Energy-efficient sensor data collection approach for industrial process monitoring," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 661–672, Feb. 2018.
- [32] R. Velmani and B. Kaarthick, "An efficient cluster-tree based data collection scheme for large mobile wireless sensor networks," *IEEE Sensors J.*, vol. 15, no. 4, pp. 2377–2390, Apr. 2015.
- [33] S. Chen, J. Zhou, X. Zheng, and X. Ruan, "Energy-efficient data collection scheme for environmental quality management in buildings," *IEEE Access*, vol. 6, pp. 57324–57333, 2018.
- [34] W. Wen, S. Zhao, C. Shang, and C.-Y. Chang, "EAPC: Energy-aware path construction for data collection using mobile sink in wireless sensor networks," *IEEE Sensors J.*, vol. 18, no. 2, pp. 890–901, Jan. 2018.
- [35] T. Wang, L. Qiu, A. K. Sangaiah, G. Xu, and A. Liu, "Energy-efficient and trustworthy data collection protocol based on mobile fog computing in Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3531–3539, May 2020.
- [36] F. Xu, H.-C. Yang, and M.-S. Alouini, "Energy consumption minimization for data collection from wirelessly-powered IoT sensors: Session-specific optimal design with DRL," *IEEE Sensors J.*, vol. 22, no. 20, pp. 19886–19896, Oct. 2022.
- [37] P. K. Gupta, B. T. Maharaj, and R. Malekian, "A novel and secure IoT based cloud centric architecture to perform predictive analysis of users activities in sustainable health centres," *Multimedia Tools Appl.*, vol. 76, no. 18, pp. 18489–18512, Sep. 2017.

- [38] W. Rafique, X. He, Z. Liu, Y. Sun, and W. Dou, "CFADefense: A security solution to detect and mitigate crossfire attacks in software-defined IoT-edge infrastructure," in *Proc. IEEE 21st Int. Conf. High Perform. Comput. Commun., IEEE 17th Int. Conf. Smart City, IEEE 5th Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Aug. 2019, pp. 500–509.
- [39] A. Thantharate, C. Beard, and P. Kankariya, "COAP and MQTT based models to deliver software and security updates to IoT devices over the air," in *Proc. Int. Conf. Internet Things (iThings), IEEE Green Comput., Commun. (GreenCom), IEEE Cyber, Phys., Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Atlanta, GA, USA, Jul. 2019, pp. 14–17.
- [40] G. Grigoryan, Y. Liu, L. Njilla, C. Kamhoua, and K. Kwiat, "Enabling cooperative IoT security via software defined networks (SDN)," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.
- [41] P. Krishnan, K. Jain, R. Buyya, P. Vijayakumar, A. Nayyar, M. Bilal, and H. Song, "MUD-based behavioral profiling security framework for software-defined IoT networks," *IEEE Internet Things J.*, vol. 9, no. 9, pp. 6611–6622, May 2022.
- [42] O. Said, "LBSS: A lightweight blockchain-based security scheme for IoT-enabled healthcare environment," *Sensors*, vol. 22, no. 20, p. 7948, Oct. 2022.
- [43] O. Dieste, N. Juristo, and M. D. Martínez, "Software industry experiments: A systematic literature review," in *Proc. 1st Int. Workshop Conducting Empirical Stud. Ind. (CESI)*, May 2013, pp. 2–8.
- [44] C. Wohlin, "Empirical software engineering research with industry: Top 10 challenges," in *Proc. 1st Int. Workshop Conducting Empirical Stud. Ind. (CESI)*, May 2013, pp. 43–46.
- [45] S. A. Ebad, A. A. Darem, and J. H. Abawajy, "Measuring software obfuscation quality—A systematic literature review," *IEEE Access*, vol. 9, pp. 99024–99038, 2021.
- [46] C.-L. Zhong, Z. Zhu, and R.-G. Huang, "Study on the IoT architecture and gateway technology," in *Proc. 14th Int. Symp. Distrib. Comput. Appl. Bus. Eng. Sci. (DCABES)*, Aug. 2015, pp. 196–199.
- [47] D. Stefanescu, L. Montalvillo, P. Galán-García, J. Unzilla, and A. Urbieto, "A systematic literature review of lightweight blockchain for IoT," *IEEE Access*, vol. 10, pp. 123138–123159, 2022.
- [48] E. Chatzoglou, G. Kambourakis, and C. Smiliotopoulos, "Let the cat out of the bag: Popular Android IoT apps under security scrutiny," *Sensors*, vol. 22, no. 2, p. 513, Jan. 2022.
- [49] M. Bouzidi, N. Gupta, F. A. Cheikh, A. Shalaginov, and M. Derawi, "A novel architectural framework on IoT ecosystem, security aspects and mechanisms: A comprehensive survey," *IEEE Access*, vol. 10, pp. 101362–101384, 2022.
- [50] Ş.-C. Arseni, B.-C. Chifor, M. Coca, M. Medvei, I. Bica, and I. Matei, "RESFIT: A reputation and security monitoring platform for IoT applications," *Electronics*, vol. 10, no. 15, p. 1840, Jul. 2021.
- [51] E. Abinaya, K. Aishwarva, C. Prabhaker, M. Lordwin, G. Kamatchi, and I. Malarvizhi, "A performance aware security framework to avoid software attacks on Internet of Things (IoT) based patient monitoring system," in *Proc. Int. Conf. Current Trends Towards Converging Technol. (ICCTCT)*, Mar. 2018, pp. 1–6.



**SHOUKI A. EBAD** received the Ph.D. degree in computer science and engineering from the King Fahd University of Petroleum and Minerals, Saudi Arabia, in 2012. Currently, he is an Associate Professor with the Department of Computer Science, Faculty of Science, Northern Border University, Saudi Arabia. Before that, he held several positions: a Lecturer, the Head of the Department, the Vice-Dean, the Assistant Dean of Technical Affairs at IT Deanship, and a General Secretary of Scientific Council with Northern Border University. He is also a Sun Certified Programmer for the Java 2 Platform. His current research interests include software engineering, IT project management, and information security. He has published a number of articles in these areas.

• • •