International Journal of Service Science, Management, Engineering, and Technology
Volume 16 • Issue 1 • January-December 2025

Evaluating IoT Data Security Metrics and Emerging Trends

Hamed Taherdoost
https://orcid.org/0000-0002-6503-6739
School of Arts, Science and Technology, University Canada West, Canada & GUS Institute, Global University Systems, UK & Q Minded Inc., Canada & College of Technology and Engineering, Westcliff University, USA & Research and Development Department, Hamta Business Corporation, Canada

Nachaat Mohamed
Rabdan Academy, UAE

Yousef Farhaoui
Moulay Ismail University, Morocco

ABSTRACT

A new era of connectivity has begun with the introduction of the Internet of Things (IoT), which has altered how we perceive and interact with technology. Concerns regarding data security have been significantly heightened as IoT ecosystems continue to grow and generate an unprecedented volume of data from interconnected devices. It is of the utmost importance to protect sensitive data within these extensive networks to guarantee the dependability and credibility of IoT applications. This article investigates the quantification of IoT data security metrics in literature. This paper evaluates current metrics, including their merits and practicality, while also considering emerging trends and advancements that will shape the trajectory of IoT security metrics in the future.

KEYWORDS

Authentication Protocols, Data Integrity Measurement, Confidentiality Safeguards, Availability Assessment, Non-Repudiation Techniques, Cybersecurity Analysis

INTRODUCTION

Network automation has been a popular topic and trend for a while now. Internet of Things (IoT) technology complements it and makes it possible to supply that component (Rachit et al., 2021). The broad use of IoT technologies relies heavily on trust (Malarvizhi et al., 2024; Tewari & Gupta, 2020). The majority of people are using these gadgets and equipment because they are easily accessible and within a normal price range, making them extremely cost-effective in terms of development costs (Montenegro-Marin et al., 2017). Since more industries are using IoT apps, there will be a rise in the quantity of IoT devices and apps (Lata & Kumar, 2021; Taherdoost, 2023b). IoT studies show how the technology is being used more and more in business analytics (Gupta et al., 2020), healthcare (Goyal et al., 2021), education (Belkeziz & Jarir, 2020; McRae et al., 2018), and other areas.

The IoT has also demonstrated its value and promise in a developing nation's industrial and economic development. In the world of commerce and the stock market, it is also seen as a groundbreaking development. Data and information security, however, is a big problem that needs fixing because it is both desirable and crucial (Minoli et al., 2017). IoT devices frequently collect

DOI: 10.4018/ijssmet.388708

sensitive and private data, such as user behavior patterns (Porambage et al., 2016) and health information (Shahid et al., 2022). Unauthorized access to this data may lead to privacy violations, which may result in financial fraud, identity theft, or, in some cases, bodily harm (Guerbouj et al., 2019; Stoyanova et al., 2020).

The complexity of interconnected systems and the abundance of insecure IoT devices increase the attack surface, making security a major concern (Axon et al., 2022; Stellios et al., 2021; M. U. Tariq, 2024). Financial losses and service disruptions are just a few of the far-reaching economic consequences that can result from security breaches in IoT systems (Khanam et al., 2020; Kinnunen et al., 2018; Masoodi & Pandow, 2021). The interconnectedness of systems and the knock-on effects on reliant industries make it difficult to quantify the economic consequences of security breaches in the IoT (Clim et al., 2022; George et al., 2024; Sagay & Jahankhani, 2020).

There is now a larger attack surface to work with thanks to the IoT's rapid expansion and integration with other technologies (Anand et al., 2020; Malhotra et al., 2021). Furthermore, because of the limited resources and unattended environments inherent in IoT nodes, it is difficult to maintain the security requirements of an IoT system (Rana et al., 2021). There can be serious repercussions from manipulating or tampering with data transmitted by IoT devices, such as compromised decision-making processes (Akbar et al., 2021), operational disruptions (Vetrivel et al., 2024), and safety risks (Estrada, 2022; Wolf & Serpanos, 2020). Data integrity in IoT ecosystems is vulnerable due to a lack of strong encryption methods and secure communication protocols (Abosata et al., 2021).

Owing to the quick development of IoT ecosystems and the exponential rise in data produced by connected devices, it is critical to evaluate and improve the security protocols used in these networks. The purpose of this paper is to examine the state of IoT security metrics at the moment, assess their effectiveness, and pinpoint new developments and trends that will influence IoT security measurement going forward.

This work advances the field of IoT security in several ways:

- it provides a review of existing IoT security metrics, highlighting their practical implications;
- it develops a taxonomy of IoT security metrics and evaluation approaches, providing a structured framework for understanding and categorizing these measures;
- it proposes an evaluation for assessing the effectiveness and practicality of IoT security metrics, facilitating informed decision-making by IoT stakeholders; and
- it analyzes emerging trends and advancements in IoT security, offering insights into potential future directions for research and development in this area.

Following an introduction to the IoT and an emphasis on the significance of data security within it, the paper defines key terms and classifies existing security metrics. The paper assesses the aforementioned metrics, analyzes emerging trends, and provides implications and suggestions for future research.

Recent research has provided additional perspectives on IoT security and performance metric evaluation. Patel et al. (2023) conducted a systematic review on the selection methods for performance evaluation metrics in IoT applications, offering insights into criteria prioritization. Similarly, Harbi et al. (2021) presented a comprehensive survey on emerging IoT security trends, highlighting key challenges and countermeasures. In the industrial context, Dhirani et al. (2021) mapped out the cyber threat landscape and standards for IIoT systems, while Darabkh et al. (2022) and Al-Amiedy et al. (2023) focused on RPL protocol vulnerabilities and defense mechanisms. Moreover, several works have emphasized the role of IoT in domains, such as smart agriculture and vertical farming, integrating artificial intelligence and SDN to enhance performance and security (Banitalebi Dehkordi, 2024; Rathor et al., 2024; Wakili & Bakkali, 2024). These studies further enrich the landscape of IoT research and reinforce the necessity for robust and context-aware security metrics.

Despite the growing relevance of security in IoT ecosystems, the academic discourse remains fragmented in terms of how security metrics are defined, evaluated, and applied. Most studies emphasize individual dimensions, such as authentication or encryption, without offering a holistic view of how these metrics function together in real-world applications. Furthermore, while taxonomies of metrics exist, there is a lack of standardized frameworks for comparing their effectiveness or applicability across different IoT use cases. This study aimed to address that gap by analyzing how IoT security metrics have evolved in the literature, identifying areas of overemphasis and underrepresentation, and offering a conceptual taxonomy that highlights future opportunities for balanced and standardized metric development.

IOT METRICS

The utilization of IoT systems to efficiently assist diverse enterprise domains is on the rise, as well (Ahmed et al., 2019; Lampropoulos et al., 2019). A notable characteristic of contemporary IoT systems is the considerable potential heterogeneity of the employed technologies, which may have adverse effects on the system's interoperability, seamless integration, overall dependability, and security (Bures et al., 2021; Hassan & Madani, 2017; Marinissen et al., 2016).

Several concerns are associated with the assessment of IoT systems. Certain formulas that are allocated to the metrics are occasionally lacking in efficiency. Certain suggestions may be in opposition to others; to address this concern, certain scholars have suggested weighting factors of significance that are applied to each specific metric; performance metrics about security and privacy threats; and energy efficiency-related metrics (Moulla et al., 2023).

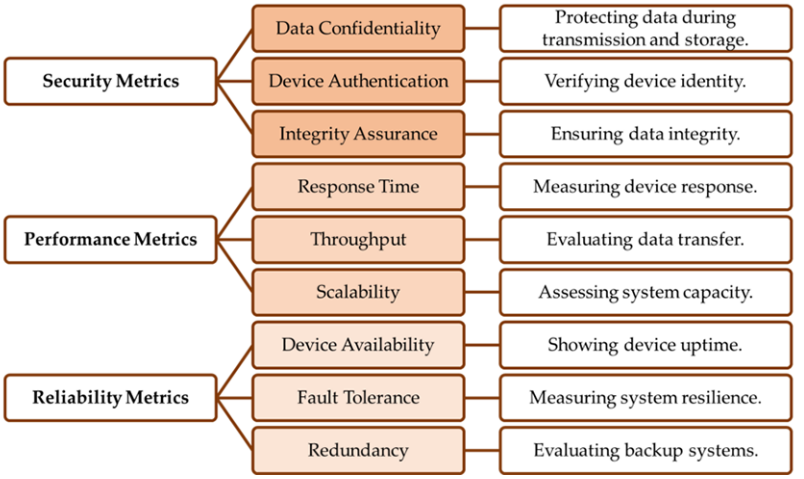
Functional domains, like security, performance, and dependability, can be used to categorize IoT metrics. Features, like intrusion detection systems, and network anomaly detection are examples of security metrics that identify and detect cyberattacks on IoT devices (Cvitić et al., 2021; Li et al., 2024). Performance metrics, which include response time, throughput, and resource usage, are used to evaluate the efficacy and efficiency of IoT devices (Cvitić et al., 2021; Seba et al., 2024). IoT device dependability and resilience, including fault identification and categorization and predictive maintenance, are the main topics of reliability metrics (Seba et al., 2024).

Before feeding data to models, these approaches frequently employ feature reduction techniques, like feature selection or extraction, which helps make detection effective for real-time requirements. Given the small number of features, feature extraction generally provides better detection performance than feature selection for IoT network intrusion detection in machine learning-based systems, according to a study comparing feature extraction and selection (Li et al., 2024).

Regarding performance, research highlights the role of sensors in the IoT ecosystem and the significance of reliable and accurate sensor data for the caliber and dependability of IoT systems. For IoT sensor fault prediction and classification, in the study by Seba et al. (2024), a hybrid convolutional neural network (CNN)-MLP classification model outperformed CNN and MLP in terms of accuracy, precision, recall, and F1-score. With a 98.21% accuracy rate, the study suggested a hybrid CNN-long short-term memory (LSTM) as a regression model that performed better for IoT sensor fault prediction than a gated recurrent unit, LSTM, bidirectional LSTM, CNN-gated recurrent unit, and CNN-bidirectional LSTM.

We can group IoT metrics according to functional domains, like security, performance, and dependability. We can further divide these groups based on particular characteristics, such as device availability and data confidentiality (Figure 1).

Figure 1. Key Internet of Things (IoT) Metrics



Security Metrics

Security metrics include the following:

- data confidentiality, which are metrics related to ensuring the confidentiality of data transmitted and stored by IoT devices;
- device authentication, which are metrics focusing on verifying the identity of devices to prevent unauthorized access; and
- integrity assurance, which are metrics ensuring the integrity of data to prevent tampering or unauthorized modifications.

Performance Metrics

Performance metrics include the following:

- response time, which are metrics measuring the time taken for IoT devices to respond to requests;
- throughput, which are metrics evaluating the amount of data transferred by IoT devices within a given timeframe; and
- scalability, which are metrics assessing the ability of IoT systems to handle increasing numbers of devices and data.

Reliability Metrics

Security metrics include the following:

- device availability, which are metrics indicating the percentage of time IoT devices are operational and accessible;
- fault tolerance, which are metrics measuring the system's ability to continue functioning in the presence of faults or failures; and
- redundancy, which are metrics evaluating the presence of backup systems to ensure continuous operation.

TAXONOMY OF SECURITY METRICS

Because the IoT is made up of electronic devices, it is made up of software that manages the operations of the electronic devices and hardware that is made up of electronic circuits, sensors, and occasionally actuators. As such, a thorough evaluation of each product's performance to confirm quality is not possible. Items describing the design, development, and support phases of the product lifecycle should be included in the process outline for security development. Static and/or dynamic security testing of IoT devices should be reflected in the aforementioned items to demonstrate IoT cyber-security performance (primarily in software) (Ito et al., 2021).

A high-level abstraction of security metrics can be obtained through a taxonomy, which offers an organized method for contrasting and analyzing different strategies. A more thorough grasp of security performance can be attained by classifying metrics, which makes it feasible to identify issues and common strategies across various security disciplines (Savola, 2007). A taxonomy can assist in identifying and categorizing security metrics in the context of the information and communication technology industry based on several variables, including vulnerabilities, defense mechanisms, and security incidents (Bhol et al., 2023).

Philippou et al. (2020) pointed out that defining standard security metrics is a difficult task. They offer a fresh approach to closing this gap, highlighting its potential for more accurate results even though it will take a lot of work to make the connections between metrics and corporate objectives. Studies, such as that of L. Wang et al. (2017), concentrated on network security metrics, while Longueira-Romero et al. (2020) filtered metrics for embedded systems. Contextualization differs depending on the domain. In a survey comparing security metrics in system security, Pendleton et al. (2016) found discrepancies between the intended metric properties and research findings. A range of techniques are used in the literature to evaluate and quantify the security of cloud services when choosing security metrics, as shown in Table 1.

Table 1. Research Methods for Evaluating Cloud and Network Security

No.	Research Method	Description	Source
1	Quantitative framework for security assurance	Evaluates cloud service security assurance using a quantitative framework. Provides a concise summary of compliance with security standards and vulnerabilities.	(Shukla et al., 2023)
2	Qualitative research method	Utilizes qualitative research to examine cloud security metrics. Compiles reliable data from research articles to offer in-depth understanding.	(Ahmadi, 2023)
3	Thematic analysis approach	Categorizes data related to cloud security metrics and measures. Identifies patterns using thematic analysis, methodically coding and categorizing data.	(Ahmadi, 2023)
4	Identification of security controls	Focuses on selecting information security controls using techniques, like AHP, ANP, VIKOR, and GRA. Aids in evaluating and enhancing security control assessment.	(Diéguez et al., 2023)
5	Network analysis metrics	Various metrics are used in network analysis to characterize networks locally, focusing on nodes or edges. Understanding network composition and behavior relies heavily on these metrics.	(Morrison et al., 2022)

These methods offer insights into the various techniques used to improve cloud security and give a thorough understanding of how security metrics are chosen and assessed in the literature. Table 2 lists the various methods for choosing security metrics that have been used in the literature.

Table 2. Approaches for Selecting Security Metrics in Literature

Approach	Description	Reference
Multivocal literature review (MLR)	Employs a snowballing method to investigate scholarly and gray literature, subsequently filtration them through a multistep procedure.	(Fernández-Alemán et al., 2013)
Automatic generation	A framework is employed to produce precise security metrics after an examination of the field's context and security objectives.	(Ani et al., 2018)
Classification and selection	Defines a domain-aligned classification of metrics and then selects those that adequately address all necessary security aspects.	(Morrison et al., 2018)

Note. MLR = multivocal literature review.

The suggested criteria include classification based on security objectives, measurement techniques (qualitative or quantitative), contextual relevance to IoT environments, granularity, scope, and practicality to effectively categorize security metrics within IoT. Metrics are categorized based on particular security objectives, like availability, confidentiality, and integrity, taking into account how well they apply to different kinds of devices, communication protocols, and deployment situations. Metrics range in scope and granularity, offering insights into everything from individual devices to entire ecosystems. Their actionability and practicality guarantee that they can be measured and applied in real-world IoT implementations feasibly.

EVALUATION OF IOT SECURITY METRICS

The objective of this section is to systematically evaluate the current state of IoT security metrics in academic literature by identifying which metrics are most studied, analyzing trends over time, and classifying them by core security objectives (confidentiality, integrity, availability, authentication, and nonrepudiation). This analysis provides insights into the relative emphasis of each metric, highlights underexplored areas, and informs future research priorities.

To achieve this, a structured literature search was conducted using the Scopus database for articles published between 2019 and April 2024. The following queries were used:

- TITLE (“Internet of Things” OR “IoT”) AND TITLE-ABS-KEY (“Security”) AND TITLE (“Confidentiality”)
- TITLE (“Internet of Things” OR “IoT”) AND TITLE-ABS-KEY (“Security”) AND TITLE (“Integrity”)
- TITLE (“Internet of Things” OR “IoT”) AND TITLE-ABS-KEY (“Security”) AND TITLE (“Availability”)
- TITLE (“Internet of Things” OR “IoT”) AND TITLE-ABS-KEY (“Security”) AND TITLE (“Authentication”)
- TITLE (“Internet of Things” OR “IoT”) AND TITLE-ABS-KEY (“Security”) AND TITLE (“Nonrepudiation”)

The search results were analyzed by document count per metric, citation performance, and publication trends. Metrics were also categorized by security dimension and evaluated. As shown in Figure 2, authentication is the most researched metric, significantly outpacing others, such as confidentiality and availability. This suggests a heavy research focus on verifying identity in IoT systems. Although essential, this focus risks overshadowing other equally important dimensions,

such as integrity, availability, and especially nonrepudiation, which remain underrepresented for research intensity.

Figure 2. Total Number of Documents of Each Metric

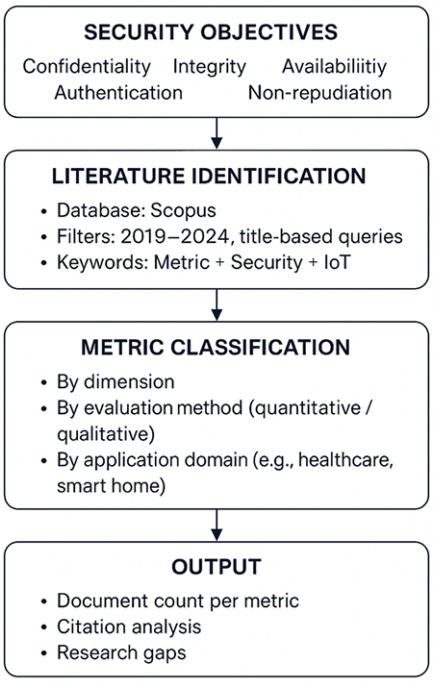


Table 3 summarizes the top 20 most cited papers and the security metrics they address. Notably, 80% of the highly cited articles relate to authentication, with fewer addressing integrity and availability. Nonrepudiation and confidentiality are seldom focal points in high-impact studies.

Table 3. Top 20 Papers Based on Citation

Study	Year	Source Title	Cited by	Security Metric
(El-Hajj et al., 2019)	2019	*Sensors*	292	Authentication
(Gope & Sikdar, 2019)	2019	*IEEE Internet of Things Journal*	254	Authentication
(Esfahani et al., 2019)	2019	*IEEE Internet of Things Journal*	213	Authentication
(Shen et al., 2020)	2020	*IEEE Journal on Selected Areas in Communications*	203	Authentication
(Jamil et al., 2020)	2020	*Sensors*	194	Integrity
(Wazid et al., 2020)	2020	*Journal of Network and Computer Applications*	178	Authentication
(Khalid et al., 2020)	2020	*Cluster Computing*	177	Authentication
(B. Chatterjee et al., 2019)	2019	*IEEE Internet of Things Journal*	176	Authentication

continued on following page

Table 3. Continued

Study	Year	Source Title	Cited by	Security Metric
(Hang & Kim, 2019)	2019	*Sensors*	174	Integrity
(U. Chatterjee et al., 2019)	2019	*IEEE Transactions on Dependable and Secure Computing*	172	Authentication
(Xiong et al., 2019)	2019	*IEEE Internet of Things Journal*	164	Availability
(Zhou et al., 2019)	2019	*Future Generation Computer Systems*	154	Authentication
(Fotouhi et al., 2020)	2020	*Computer Networks*	134	Authentication
(Hamidi, 2019)	2019	*Future Generation Computer Systems*	131	Authentication
(Zhao et al., 2020)	2020	*Information Processing and Management*	130	Integrity
(Wazid et al., 2019)	2019	*Journal of Systems Architecture*	129	Authentication
(Aghili et al., 2019)	2019	*Future Generation Computer Systems*	126	Authentication
(Zhang et al., 2019)	2019	*IEEE Wireless Communications*	118	Authentication
(Alzubi, 2021)	2021	*Computer Communications*	110	Authentication
(Vijayakumar et al., 2020)	2020	*IEEE Transactions on Industrial Informatics*	106	Authentication

Note. IEEE = Institute of Electrical and Electronics Engineers.

This data highlights both the strength and the imbalance in current research: While authentication mechanisms have advanced, there is a lack of standardization or comparative frameworks for evaluating metric effectiveness across real-world IoT systems.

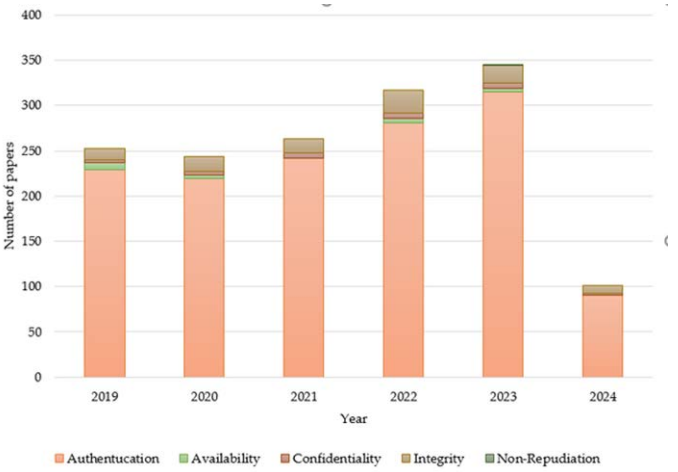
The analysis was limited to Scopus-indexed documents, which may have excluded relevant papers from other databases. Additionally, only title-based searches were used, which may not capture all relevant literature due to varying terminology. There was also no experimental or simulation-based validation in this study, which is acknowledged as a key area for future work. As shown in Figure 3, the conceptual framework for this study followed a four-step process encompassing security objectives, literature filtering, classification of metrics, and extraction of actionable insights.

Figure 3. Conceptual Framework for Evaluating Internet of Things (IoT) Security Metrics

A quantitative analysis of the number of articles published annually for each IoT security metric, as illustrated in Figure 4, identifies several noteworthy trends and patterns. Of all the security

metrics, authentication has been studied the most, as evidenced by the large number of articles it has consistently received. The importance of authentication protocols and mechanisms in maintaining the security and integrity of IoT ecosystems is highlighted by this constant attention. Ferdowsi and Saad (2019) introduced a new watermarking algorithm for authenticating IoT signals, essential for cyberattack detection. It used deep learning to embed stochastic features in signals for IoT gateway authentication. In massive IoT scenarios, a game-theoretic framework predicted vulnerable devices, improving gateway decision-making. Gateway decisions were also helped by a deep reinforcement learning algorithm predicting unauthenticated device states. Simulations showed nearly 100% message transmission reliability with an attack detection delay under 1 second.

Figure 4. Analysis of the Number of Articles in Research Output (2019–2024)



As concerns about data integrity and privacy within IoT systems continue, integrity and confidentiality metrics also show a significant amount of research activity, with several articles that have remained relatively constant over time. Each type of security attack is linked to one or more architecture layers, so proper authentication, confidentiality, and validity must be implemented for better protection (Doss et al., 2022).

Availability metrics are less common in the literature, but they are still present when it comes to authentication, integrity, and confidentiality metrics. These metrics are still acknowledged as essential elements of IoT security, even though their numbers are not as high as those of authentication, integrity, and confidentiality. Nonrepudiation metrics, on the other hand, are represented in a very different way; they are the least visible in the research output and have the fewest articles. This points to a possible area for further investigation and examination of new methods to deal with nonrepudiation issues in IoT settings.

The top-cited papers' heavy emphasis on authentication highlights how crucial it is to IoT security theory and practice. To effectively address security challenges in IoT ecosystems, researchers and practitioners should keep giving priority to authentication mechanisms and protocols. The increasing acknowledgment of integrity and availability metrics in IoT security is demonstrated by the existence of highly cited papers addressing these topics. To maintain data integrity and guarantee the continuous availability of IoT services and resources, more research and development work is necessary. The most cited area of research in IoT security is authentication, as shown by Table 3, which breaks down the total number of citations received

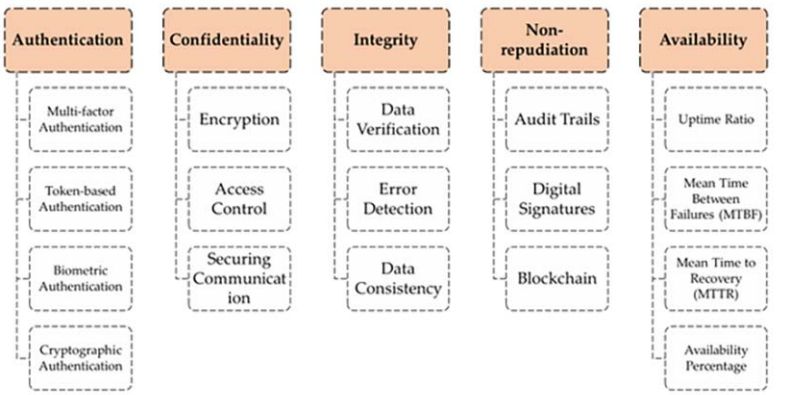
by the top 20 papers based on citation count and categorizes them according to their respective security metrics.

While authentication metrics have been the most extensively explored in the literature, this emphasis risks overlooking other critical aspects, such as confidentiality, availability, and nonrepudiation. These dimensions are equally vital for a secure IoT environment, especially given the increased heterogeneity and resource constraints of IoT devices. For example, ensuring availability and integrity in battery-powered or latency-sensitive systems can be as crucial as authentication in certain applications, such as healthcare or industrial automation. Future research should seek to balance this emphasis by exploring lightweight mechanisms to enhance the coverage of these underrepresented metrics.

DISCUSSION

As illustrated in Figure 5, IoT security investigation metrics in this survey include confidentiality, integrity, availability, authentication, and nonrepudiation. Each security metric has subcategories for encryption, access control, data verification, and multifactor authentication. Evaluation approaches are aligned with security metrics to assess IoT security measures comprehensively, ensuring ecosystem robustness and reliability.

Figure 5. Taxonomy of Internet of Things (IoT) Security Metrics and Evaluation Approaches



Note. MTBF = mean time between failures; MTTR = mean time to recovery.

Confidentiality Metrics

The parameter regulates and safeguards confidential information against unauthorized parties (Ram et al., 2021). Given that IoT applications predominantly utilize wireless data transmission, the security of the information is comparatively higher than that of a wired network. The utilization of cryptography can be regarded as a highly effective approach to safeguarding the privacy of information (Hodgson, 2019).

When discussing IoT security, confidentiality pertains to safeguarding sensitive information against unauthorized access, disclosure, or alteration while it is being exchanged among IoT devices (Minh, 2019; Tawalbeh et al., 2020). It is an essential security prerequisite that safeguards the confidentiality and integrity of information transmitted throughout the IoT network. The following metrics are employed to assess confidentiality in IoT security (Minh, 2019):

1. Access control: It assesses the efficacy of access control mechanisms in mitigating unauthorized access to confidential information. The study by Selvan and Singh (2022) proposed a risk-based access control model for fog-IoT to address security concerns. It used fog-IoT environment features to calculate risk factors from real-time data requests, considering device context, resource sensitivity, action severity, and risk history. An adaptive security agent detected abnormal device behavior. Compared to existing models, risk assessment accuracy improved for various scenarios.
2. Encryption strength: The robustness of encryption algorithms implemented to safeguard data was assessed while it was being transmitted. The IoT, or IoT, was a global network of physically connected objects that communicated with one another. With components, like smartphones, wireless sensor networks, and radio frequency identification, security was a big worry. Chanal and Kakkasageri (2021) suggested a hybrid algorithm that combines the advanced encryption standard, elliptic curve cryptography, and message digest algorithm (i.e., MD5) to address this. This method improved data confidentiality by preventing tampering and unauthorized access. Across a range of file sizes, their simulations showed better performance metrics when compared to conventional advanced encryption standard encryption.
3. Securing communication: It evaluates how well secure communication protocols work to reduce the dangers of replay, tampering, and eavesdropping attacks. An affordable Raspberry Pi 3 smart meter for IoT applications was introduced by Tenório et al. (2019). It exceeded standard security protocols in three stages: secure data acquisition, encryption, and transmission, ensuring data integrity even in untrusted cloud environments or remote adversary access. This solution was flexible, simple, efficient, and affordable, making it suitable for IoT applications.

Integrity Metrics

Integrity ensures the information is accurate, relevant, consistent, and reliable throughout all operational procedures involving data (Reilly et al., 2019), including data transfer, updating, retrieval, storage, and capture. Ensuring integrity in IoT security is of the utmost importance to preserve the trustworthiness and genuineness of data transmitted among IoT devices and to thwart unauthorized alterations that may compromise the functionality and security of the system (Abosata et al., 2021). These metrics aid in validating the consistency and dependability of data by providing a quantitative evaluation of its integrity. IoT systems can bolster the overall security and dependability of the system by verifying the authenticity and consistency of information over its entire lifecycle via data integrity measurement. Integrity metrics are an indispensable instrument for the surveillance and assessment of data integrity. They empower IoT systems to promptly identify and address any unauthorized modifications (Nazir et al., 2024).

Data integrity stands as a cornerstone in IoT's evolution, fueling decision-making in critical domains. However, the ubiquity of edge devices renders them vulnerable to cyber-attacks. Given the safety-critical nature and commercial value of IoT-generated data, threats, like data tampering and malicious infusion, loom large (Garagad et al., 2020). BalancePIC's solution balances user privacy, data integrity, and computational cost. It uses balanced truth discovery and biometric elliptic curve cryptography authentication for privacy. Processing data in zones reduces computational costs and protects against threats. Simulations show it maintains balance in these areas (T. Wang et al., 2020).

Availability Metrics

Availability, as it pertains to IoT security, denotes the capacity of IoT systems and devices to consistently function, be accessible, and react to authorized users and devices (Kumar et al., 2019; Rachit et al., 2021; Tawalbeh et al., 2020). Cybersecurity incidents disrupt the availability of data in IoT applications, thereby impeding access to IoT devices. By implementing equipment maintenance, up-to-date operating software, system redundancy, system backups, enhanced system resiliency, and proactive recovery strategies from unforeseen incidents, one can guarantee the accessibility of the

information. High availability, defined as the agreed-upon level of operational performance that minimizes system unavailability to the greatest extent possible, is critical in IoT applications (Abdul-Ghani et al., 2018). The reliability block diagram, fault tree, and continuous time Markov chain used by Nguyen et al. (2020) showed the overall architecture, system architectures, and operative states. They used this framework for a smart factory IoT infrastructure with cloud, fog, and edge computing. Analysis showed that cloud failures reduced availability, while edge computing helped recover. Cloud servers' virtualization and fog servers' operating systems were also vulnerable to cyberattacks.

A variety of metrics are frequently employed to assess availability (Mazhar et al., 2023):

1. the "uptime/downtime ratio" evaluates the proportion of total time observed during which a device or system is operational to the time it is non-operational, and an increased uptime ratio indicates enhanced availability;
2. mean time between failures (MTBF) provides an estimation of the system's availability and reliability by calculating the average time between system failures;
3. mean time to recovery (MTTR) indicates the system's responsiveness and recovery capabilities by quantifying the average time required to restore a system to its operational state following a failure; and
4. availability percentage quantifies the extent of availability about the overall time observed; to illustrate, a system that maintains an availability of 99.9% experiences an approximate annual downtime of 8.76 hours.

Authentication Metrics

The process of authentication verifies the legitimacy of a message, transmission, originator, or a person's permission to receive a specific kind of data (Cambou et al., 2018). In terms of IoT security, authentication is the process of confirming users' and devices' identities before allowing access to resources or services (Ito et al., 2021).

There are several methods of IoT authentication, including one-way, two-way, three-way, distributed, and centralized authentication (Agrawal & Ahlawat, 2020). Sun et al. (2019) addressed the challenge of maintaining gait recognition performance in WIoT devices. The proposed approach improved gait recognition and user authentication rates to 96.9% and 91.75%, respectively, by using speed-adaptive gait cycle segmentation and individualized matching threshold generation. Gait recognition improved by 25.8% and user authentication by 21.5% over existing methods. For IoT network security, Qaisi et al. (2022) proposed tag-embedding message authentication to improve authentication rates and tag confidentiality. The scheme reduced resource consumption but needed improvement against nearby eavesdroppers. In contrast, Mahbub et al. (2020) proposed three authentication levels to improve IoT network security. Performance was evaluated using an ANFIS-based authentication model, analyzed by successful authentication rate, and simulated with fuzzy logic in MATLAB. Simulations showed that successful authentication should be at least 70% for any two levels and 30% for any individual level. Although numerical results beyond these criteria are not provided, the study found that the proposed mechanism improves IoT network security.

Nonrepudiation Metrics

Nonrepudiation is the capacity to guarantee that a party to an IoT transaction cannot contest the transaction's validity (Das et al., 2018). Both the sender and the recipient of the data will be notified when the information has been delivered; the sender will receive proof of delivery, while the recipient will receive identification proof of the sender (Fang et al., 2020). The ability to confirm the identity of communicating peers and guarantee that devices or users with legitimate credentials are granted access to services and resources is among the metrics used in IoT security to measure nonrepudiation (Li et al., 2019). Divya et al. (2023) suggested a novel multiparty computation framework to improve

nonrepudiation, especially in IoT networks. The framework minimized computation overhead while guaranteeing strong security by introducing novel encryption and split key management techniques. Compared to existing schemes, simulation results showed a significant improvement with 48% less overhead, 54% less delay, and 58% faster processing.

Challenges Unique to IoT Environments

IoT environments present distinct challenges that complicate the implementation and evaluation of security metrics. Resource constraints, such as limited processing power, memory, and energy capacity, make it impractical to deploy computationally intensive encryption and authentication algorithms. For example, many low-power nodes in sensor networks cannot support traditional public key cryptography. Additionally, the increasing use of edge computing introduces security vulnerabilities at the network perimeter, which are not adequately addressed by cloud-based models.

Privacy concerns in smart home and healthcare settings add another layer of complexity, where sensitive data transmission requires both confidentiality and regulatory compliance. The dynamic and decentralized nature of IoT systems means that static security models are often inadequate. These challenges underscore the need for tailored metrics and lightweight, context-aware security solutions specific to IoT systems.

Practical and Managerial Implications

The findings of this review offer several implications for IoT system designers, managers, and policymakers. First, the imbalance in research attention, particularly the overemphasis on authentication, suggests that decision-makers may be relying on uneven security strategies. Managers should aim to integrate underutilized metrics, like nonrepudiation and availability, into IoT risk assessments to ensure comprehensive protection.

Second, the absence of standardized evaluation frameworks hinders consistent policy benchmarking. Regulatory agencies and corporate cybersecurity teams should advocate for and adopt flexible scoring or ranking methodologies to assess the maturity of IoT security deployments across industries. Lastly, the study highlights the urgent need for lightweight security solutions suitable for low-resource environments, a crucial insight for vendors targeting smart cities, agriculture, and healthcare sectors.

FUTURE TRENDS

It is challenging to guarantee the security of the heterogeneous IoT ecosystem in the absence of standard security protocols and a common taxonomy. To address vulnerabilities across hardware, software, and data, standardization is required at the manufacturing, communication, and data audit levels (U. Tariq et al., 2023). One major security issue that needs to be addressed is ensuring the availability, confidentiality, and integrity of IoT data. Another is securing the communication between IoT devices (AlSalem et al., 2023; U. Tariq et al., 2023). To stop illegal access and data misuse, more research is required on access control methods and anomaly detection strategies for IoT systems (U. Tariq et al., 2023). The IoT's integration with other technologies, such as software-defined networking, presents new security issues that require attention (Rachit et al., 2021; Taherdoost, 2023a).

Organizations implementing IoT solutions need to comply with strict compliance requirements due to the growing emphasis on data protection and privacy regulations (such as the CCPA and GDPR) (Aljeraisy et al., 2021; Sirur et al., 2018). To ensure compliance, security strategies must be continuously monitored and adjusted due to the dynamic nature of IoT technologies and the constantly changing regulatory landscape (Brass & Sowell, 2021; Schiller et al., 2022).

By 2025, there will be over 30 billion IoT devices. People were previously aware of the IoT project, but they disregarded it because it appeared difficult to execute and complicated. With the

advancement of technology, people are realizing that this is not unachievable, as the IoT is developing at an increasingly rapid pace (Tawalbeh et al., 2020).

Future research should focus on the development and empirical validation of standardized security metric frameworks that are scalable across diverse IoT environments. This includes introducing scoring systems or ranking methodologies to evaluate and compare metric effectiveness under varying operational constraints. Simulations, testbed environments, or real-world case studies would greatly strengthen the assessment of these metrics.

Moreover, there is a need to design lightweight, adaptive security protocols tailored for constrained devices, and to explore novel applications of blockchain, federated learning, and explainable artificial intelligence in securing distributed IoT networks. Emerging areas, such as energy-aware authentication and privacy-preserving data aggregation, represent promising research frontiers that remain underexplored.

Future research should address several key priorities. First, there is a need to develop and validate standardized frameworks for comparing security metrics under different IoT conditions, including edge computing, smart cities, and health monitoring systems. Second, the creation of lightweight security protocols that balance performance and power consumption remains an underdeveloped but critical area of study.

Third, future work should explore cross-metric interaction effects, for example, how enhancing integrity may impact availability or device latency. Finally, researchers should pursue case study-based validations and simulation modeling to test the practical utility and trade-offs of security metrics in real deployments.

LIMITATIONS OF THE STUDY

While this study provides a comprehensive analysis of IoT security metrics and emerging trends, it is not without limitations. First, the scope of the literature review was restricted to articles indexed in the Scopus database, which may have excluded relevant studies published in other databases or gray literature. Second, the classification and evaluation of metrics focused on five main security dimensions, confidentiality, integrity, availability, authentication, and nonrepudiation, which, while fundamental, may not encompass all nuanced security concerns in diverse IoT applications. Third, the fast-evolving nature of IoT technologies means that new metrics and security frameworks may emerge rapidly, potentially limiting the long-term applicability of the findings. Finally, the study did not empirically validate the practicality of each metric through case studies or simulations, which could be explored in future research.

Additionally, the current study does not include experimental validation, benchmark comparisons, or simulation-based testing of the reviewed metrics. As a result, while the theoretical foundation is robust, the practical performance and feasibility of these metrics in operational IoT environments remain untested. This limits the immediate applicability of the findings and underscores the importance of future work involving empirical studies or deployment-specific evaluations.

In addition to the scope and data limitations discussed earlier, the absence of practical validation means that the findings cannot be directly generalized to operational environments. While the literature analysis provides valuable mapping of trends, without benchmarking or real-world testing, the relative effectiveness of one metric versus another remains speculative. As such, conclusions should be viewed as directional rather than prescriptive, pending further empirical research.

CONCLUSION

This study presented a structured review and evaluation of IoT security metrics across five key dimensions: confidentiality, integrity, availability, authentication, and nonrepudiation. Through an analysis of recent literature indexed in Scopus (2019–2024), the work identifies authentication as

the most extensively researched metric, followed by integrity, while confidentiality, availability, and nonrepudiation remain underexplored. The findings reflect patterns already noted in the literature, reinforcing rather than challenging the prevailing focus on identity verification. Although this may limit the novelty of our conclusions, the study makes a useful contribution by consolidating, classifying, and visualizing metric usage trends. It also highlights substantial research gaps in real-world benchmarking and evaluation practices, especially in relation to resource-constrained environments. A major limitation of this study is the absence of empirical simulations or case studies to validate the discussed metrics. Consequently, this work should be seen as a foundation for future research rather than a definitive framework. It invites further studies that (1) empirically test the proposed metrics, (2) develop standardized evaluation frameworks, and (3) design balanced security strategies across all metric dimensions. Addressing these gaps will be essential to building resilient and scalable IoT security systems.

FUNDING STATEMENT

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. Funding for this research was covered by the authors of the article.

COMPETING INTERESTS

The authors of this publication declare that there are no competing interests.

PROCESS DATES

08, 2025
This manuscript was initially received for consideration for the journal on 02/03/2025, revisions were received for the manuscript following the double-anonymized peer review on 06/07/2025, the manuscript was formally accepted on 07/17/2025, and the manuscript was finalized for publication on 08/21/2025.

CORRESPONDING AUTHOR

Correspondence should be addressed to Hamed Taherdoost [hamed.taherdoost@gmail.com], Nachaat Mohamed [eng.cne1@gmail.com], and Yousef Farhaoui [y.farhaoui@fste.umi.ac.ma].

REFERENCES

Abdul-Ghani, H. A., Konstantas, D., & Mahyoub, M. (2018). A comprehensive IoT attacks survey based on a building-blocked reference model. *International Journal of Advanced Computer Science and Applications*, *9*(3). Advance online publication. DOI: 10.14569/IJACSA.2018.090349

Abosata, N., Al-Rubaye, S., Inalhan, G., & Emmanouilidis, C. (2021). Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications. *Sensors (Basel)*, *21*(11), 3654. DOI: 10.3390/s21113654 PMID: 34073975

Aghili, S. F., Mala, H., Shojafar, M., & Peris-Lopez, P. (2019). LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT. *Future Generation Computer Systems*, *96*, 410–424. DOI: 10.1016/j.future.2019.02.020

Agrawal, S., & Ahlawat, P. (2020). A survey on the authentication techniques in internet of things. *2020 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, 1–5. DOI: 10.1109/SCEECS48394.2020.86

Ahmadi, S. (2023). Cloud security metrics and measurement. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 2*(1), 93–107. DOI: 10.60087/jklst.vol2.n1.p107

Ahmed, B. S., Bures, M., Frajtak, K., & Cerny, T. (2019). Aspects of quality in internet of things (IoT) solutions: A systematic mapping study. *IEEE Access : Practical Innovations, Open Solutions*, *7*, 13758–13780. DOI: 10.1109/ACCESS.2019.2893493

Akbar, M. A., Alsanad, A., Mahmood, S., & Alothaim, A. (2021). A multicriteria decision making taxonomy of IoT security challenging factors. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 128841–128861. DOI: 10.1109/ACCESS.2021.3104527

Al-Amiedy, T. A., Anbar, M., Belaton, B., Bahashwan, A. A., Hasbullah, I. H., Aladaileh, M. A., & Mukhaini, G. A. (2023). A systematic literature review on attacks defense mechanisms in RPL-based 6LoWPAN of internet of things. *Internet of Things : Engineering Cyber Physical Human Systems*, *22*, 100741. DOI: 10.1016/j.iot.2023.100741

Aljeraisy, A., Barati, M., Rana, O., & Perera, C. (2021). Privacy laws and privacy by design schemes for the internet of things: A developer's perspective. *ACM Computing Surveys*, *54*(5), 1–38. DOI: 10.1145/3450965

AlSalem, T. S., Almaiah, M. A., & Lutfi, A. (2023). Cybersecurity risk analysis in the IoT: A systematic review. *Electronics (Basel)*, *12*(18), 3958. DOI: 10.3390/electronics12183958

Alzubi, J. A. (2021). Blockchain-based Lamport Merkle digital signature: Authentication tool in IoT healthcare. *Computer Communications*, *170*, 200–208. DOI: 10.1016/j.comcom.2021.02.002

Anand, P., Singh, Y., Selwal, A., Alazab, M., Tanwar, S., & Kumar, N. (2020). IoT vulnerability assessment for sustainable computing: Threats, current solutions, and open challenges. *IEEE Access : Practical Innovations, Open Solutions*, *8*, 168825–168853. DOI: 10.1109/ACCESS.2020.3022842

Ani, U. P. D., He, H., & Tiwari, A. (2018). A framework for operational security metrics development for industrial control environment. *Journal of Cyber Security Technology*, *2*(3–4), 201–237. DOI: 10.1080/23742917.2018.1554986

Axon, L., Fletcher, K., Scott, A. S., Stolz, M., Hannigan, R., Kaafarani, A. E., Goldsmith, M., & Creese, S. (2022). Emerging cybersecurity capability gaps in the industrial internet of things: Overview and research agenda. *Digital Threats : Research and Practice*, *3*(4), 1–27. DOI: 10.1145/3503920

Banitalebi Dehkordi, A. (2024). The impact of software-defined networks on reducing latency and enhancing data security in blockchain-based IoT architectures. *Journal of Soft Computing and Information Technology*, *13*(3), 12–30.

Belkeziz, R., & Jarir, Z. (2020). An overview of the IoT coordination challenge. *International Journal of Service Science, Management, Engineering, and Technology*, *11*(1), 99–115. DOI: 10.4018/IJSSMET.2020010107

Bhol, S. G., Mohanty, J., & Pattnaik, P. K. (2023). Taxonomy of cyber security metrics to measure strength of cyber security. *Materials Today: Proceedings*, *80*, 2274–2279. DOI: 10.1016/j.matpr.2021.06.228

Brass, I., & Sowell, J. H. (2021). Adaptive governance for the internet of things: Coping with emerging security risks. *Regulation & Governance*, *15*(4), 1092–1110. DOI: 10.1111/rego.12343

Bures, M., Klima, M., Rechtberger, V., Ahmed, B. S., Hindy, H., & Bellekens, X. (2021). Review of specific features and challenges in the current internet of things systems impacting their security and reliability. In Rocha, Á., Adeli, H., Dzemyda, G., Moreira, F., & Ramalho Correia, A. M. (Eds.), *Advances in intelligent systems and computing* (pp. 546–556). Springer., DOI: 10.1007/978-3-030-72660-7_52

Cambou, B., Flikkema, P. G., Palmer, J., Telesca, D., & Philabaum, C. (2018). Can ternary computing improve information assurance? *Cryptography*, *2*(1), 6. DOI: 10.3390/cryptography2010006

Chanal, P. M., & Kakkasageri, M. S. (2021). Preserving data confidentiality in internet of things. *SN Computer Science*, *2*(1), 53. Advance online publication. DOI: 10.1007/s42979-020-00429-z

Chatterjee, B., Das, D., Maity, S., & Sen, S. (2019). RF-PUF: Enhancing IoT security through authentication of wireless nodes using in-situ machine learning. *IEEE Internet of Things Journal*, *6*(1), 388–398. DOI: 10.1109/JIOT.2018.2849324

Chatterjee, U., Govindan, V., Sadhukhan, R., Mukhopadhyay, D., Chakraborty, R. S., Mahata, D., & Prabhu, M. M. (2019). Building PUF based authentication and key exchange protocol for IoT without explicit CRPS in verifier database. *IEEE Transactions on Dependable and Secure Computing*, *16*(3), 424–437. DOI: 10.1109/TDSC.2018.2832201

Clim, A., Toma, A., Zota, R. D., & Constantinescu, R. (2022). The need for cybersecurity in industrial revolution and smart cities. *Sensors (Basel)*, *23*(1), 120. DOI: 10.3390/s23010120 PMID: 36616718

Cvitić, I., Peraković, D., Periša, M., & Gupta, B. (2021). Ensemble machine learning approach for classification of IoT devices in smart home. *International Journal of Machine Learning and Cybernetics*, *12*(11), 3179–3202. DOI: 10.1007/s13042-020-01241-0

Darabkh, K. A., Al-Akhras, M., Zomot, J. N., & Atiquzzaman, M. (2022). RPL routing protocol over IoT: A comprehensive survey, recent advances, insights, bibliometric analysis, recommendations, and future directions. *Journal of Network and Computer Applications*, *207*, 103476. DOI: 10.1016/j.jnca.2022.103476

Das, A. K., Zeadally, S., & He, D. (2018). Taxonomy and analysis of security protocols for internet of things. *Future Generation Computer Systems*, *89*, 110–125. DOI: 10.1016/j.future.2018.06.027

Dhirani, L. L., Armstrong, E., & Newe, T. (2021). Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap. *Sensors (Basel)*, *21*(11), 3901. DOI: 10.3390/s21113901 PMID: 34198727

Diéguez, M., Cares, C., Cachero, C., & Hochstetter, J. (2023). MASISCo—Methodological approach for the selection of information security controls. *Applied Sciences (Basel, Switzerland)*, *13*(2), 1094. DOI: 10.3390/app13021094

Divya, K. S., Roopashree, H. R., & Yogeesh, A. C. (2023). Framework of multiparty computation for higher non-repudiation in internet-of-things (IoT). *International Journal of Computer Networks and Applications*, *10*(1), 84–94. DOI: 10.22247/ijcna/2023/218513

Doss, A. N., Shah, D., Smaisim, G. F., Olha, M., & Jaiswal, S. (2022). A comprehensive analysis of internet of things (IOT) in enhancing data security for better system integrity—A critical analysis on the security attacks and relevant countermeasures. *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 165–167). DOI: 10.1109/ICACITE53722.2022.9823817

El-Hajj, M., Fadlallah, A., Chamoun, M., & Serhrouchni, A. (2019). A survey of internet of things (IoT) authentication schemes. *Sensors (Basel)*, *19*(5), 1141. DOI: 10.3390/s19051141 PMID: 30845760

Esfahani, A., Mantas, G., Matischek, R., Saghezchi, F. B., Rodriguez, J., Bicaku, A., Maksuti, S., Tauber, M. G., Schmittner, C., & Bastos, J. (2017). A lightweight authentication mechanism for M2M communications in industrial IoT environment. *IEEE Internet of Things Journal*, *6*(1), 288–296. DOI: 10.1109/JIOT.2017.2737630

Estrada, R. A. (2022). *The internet of things (IoT): Privacy and security challenges and discovering IoT risks through exploratory research*. Utica University.

Fang, W., Chen, W., Zhang, W., Pei, J., Gao, W., & Wang, G. (2020). Digital signature scheme for information non-repudiation in blockchain: A state of the art review. *EURASIP Journal on Wireless Communications and Networking, 2020*(1). DOI: 10.1186/s13638-020-01665-w

Ferdowsi, A., & Saad, W. (2019). Deep learning for signal authentication and security in massive internet-of-things systems. *IEEE Transactions on Communications*, *67*(2), 1371–1387. DOI: 10.1109/TCOMM.2018.2878025

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, *46*(3), 541–562. DOI: 10.1016/j.jbi.2012.12.003 PMID: 23305810

Fotouhi, M., Bayat, M., Das, A. K., Far, H. A. N., Pournaghi, S. M., & Doostari, M. A. (2020). A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. *Computer Networks*, *177*, 107333. DOI: 10.1016/j.comnet.2020.107333

Garagad, V. G., Iyer, N. C., & Wali, H. G. (2020). Data integrity: A security threat for internet of things and cyber-physical systems. *2021 International Conference on Computational Performance Evaluation (ComPE)* (pp. 244–249). DOI: 10.1109/ComPE49325.2020.9200170

George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: Assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal*, *2*(1), 51–75. DOI: 10.5281/zenodo.10639463

Gope, P., & Sikdar, B. (2019). Lightweight and privacy-preserving two-factor authentication scheme for IoT devices. *IEEE Internet of Things Journal*, *6*(1), 580–589. DOI: 10.1109/JIOT.2018.2846299

Goyal, S., Sharma, N., Bhushan, B., Shankar, A., & Sagayam, M. (2021). IoT enabled technology in secured healthcare: Applications, challenges and future directions. In Hassanien, A. E., Khamparia, A., Gupta, D., Shankar, K., & Slowik, A. (Eds.), *Cognitive internet of medical things for smart healthcare: Services and applications* (pp. 25–48)., DOI: 10.1007/978-3-030-55833-8_2

Guerbouj, S. S. E., Gharsellaoui, H., & Bouamama, S. (2019). A comprehensive survey on privacy and security issues in cloud computing, internet of things and cloud of things. [IJSSMET]. *International Journal of Service Science, Management, Engineering, and Technology*, *10*(3), 32–44. https://ideas.repec.org/a/igg/jssmet/v10y2019i3p32-44.html. DOI: 10.4018/IJSSMET.2019070103

Gupta, A., Srivastava, A., Anand, R., & Tomažič, T. (2020). Business application analytics and the internet of things: The connecting link. In *New age analytics* (pp. 249–273). Apple Academic Press., DOI: 10.1201/9781003007210-10

Hamidi, H. (2019). An approach to develop the smart health using internet of things and authentication based on biometric technology. *Future Generation Computer Systems*, *91*, 434–449. DOI: 10.1016/j.future.2018.09.024

Hang, L., & Kim, D.-H. (2019). Design and implementation of an integrated IoT blockchain platform for sensing data integrity. *Sensors (Basel)*, *19*(10), 2228. DOI: 10.3390/s19102228 PMID: 31091799

Harbi, Y., Aliouat, Z., Refoufi, A., & Harous, S. (2021). Recent security trends in internet of things: A comprehensive survey. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 113292–113314. DOI: 10.1109/ACCESS.2021.3103725

Hassan, Q. F., & Madani, S. A. (2017). *Internet of things: Challenges, advances, and applications*. Chapman and Hall/CRC., DOI: 10.1201/9781315155005

Hodgson, R. (2019). Solving the security challenges of IoT with public key cryptography. *Network Security*, *2019*(1), 17–19. DOI: 10.1016/S1353-4858(19)30011-X

Ito, K., Morisaki, S., & Goto, A. (2021). IoT security-quality-metrics method and its conformity with emerging guidelines. *IoT*, *2*(4), 761–785. DOI: 10.3390/iot2040038

Jamil, F., Ahmad, S., Iqbal, N., & Kim, D.-H. (2020). Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals. *Sensors (Basel)*, *20*(8), 2195. DOI: 10.3390/s20082195 PMID: 32294989

Khalid, U., Asim, M., Baker, T., Hung, P. C. K., Tariq, M. A., & Rafferty, L. (2020). A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Cluster Computing*, *23*(3), 2067–2087. DOI: 10.1007/s10586-020-03058-6

Khanam, S., Ahmedy, I. B., Idris, M. Y. I., Jaward, M. H., & Sabri, A. Q. B. M. (2020). A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things. *IEEE Access : Practical Innovations, Open Solutions*, *8*, 219709–219743. DOI: 10.1109/ACCESS.2020.3037359

Kinnunen, S.-K., Ylä-Kujala, A., Marttonen-Arola, S., Kärri, T., & Baglee, D. (2018). Internet of things in asset management: Insights from industrial professionals and academia. *International Journal of Service Science, Management, Engineering, and Technology*, *9*(2), 104–119. DOI: 10.4018/IJSSMET.2018040105

Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of things is a revolutionary approach for future technology enhancement: A review. *Journal of Big Data*, *6*(1), 111. Advance online publication. DOI: 10.1186/s40537-019-0268-2

Lampropoulos, G., Siakas, K., & Anastasiadis, T. (2019). Internet of things in the context of industry 4.0: An overview. I. *International Journal of Entrepreneurial Knowledge*, *7*(1), 4–19. DOI: 10.37335/ijek.v7i1.84

Lata, M., & Kumar, V. (2021). Standards and regulatory compliances for IoT security. *International Journal of Service Science, Management, Engineering, and Technology*, *12*(5), 133–147. DOI: 10.4018/IJSSMET.2021090109

Li, J., Liao, X., & Puech, N. (2019). Security and privacy in IoT communication. *Annales des Télécommunications*, *74*(7–8), 373–374. DOI: 10.1007/s12243-019-00718-6

Li, J., Othman, M. S., Chen, H., & Yusuf, L. M. (2024). Optimizing IoT intrusion detection system: Feature selection versus feature extraction in machine learning. *Journal of Big Data*, *11*(1), 36. Advance online publication. DOI: 10.1186/s40537-024-00892-y

Longueira-Romero, Á., Iglesias, R., Gonzalez, D., & Garitano, I. (2020). How to quantify the security level of embedded systems? A taxonomy of security metrics. *2020 IEEE 18th International Conference on Industrial Informatics (INDIN)* (pp. 153–158). DOI: 10.48550/arxiv.2112.05475

Mahbub, T. N., Salim Reza, S. M., Hossain, D. A., Raju, M. H., Murshedul Arifeen, M., & Ayob, A. (2020). ANFIS based authentication performance evaluation for enhancing security in internet of things. *Proceedings of the International Conference on Computing Advancements*, 23, 1–4. DOI: 10.1145/3377049.3377089

Malarvizhi, C. A., Manzoor, S. R., & Haque, R. (2024). Revisiting the extended IoT use behavior model among senior NCD patients for smart healthcare in Malaysia. *International Journal of Service Science, Management, Engineering, and Technology*, *15*(1), 1–25. DOI: 10.4018/IJSSMET.349911

Malhotra, P., Singh, Y., Anand, P., Bangotra, D. K., Singh, P. K., & Hong, W.-C. (2021). Internet of things: Evolution, concerns and security challenges. *Sensors (Basel)*, *21*(5), 1809. DOI: 10.3390/s21051809 PMID: 33807724

Marinissen, E. J., Zorian, Y., Konijnenburg, M., Huang, C.-T., Hsieh, P.-H., Cockburn, P., Delvaux, J., Rozic, V., Yang, N. B., Singelee, D., Verbauwhede, I., Mayor, C., Van Rijsinge, R., & Reyes, C. (2016). IoT: Source of test challenges. *Proceedings - 2016 21th IEEE European Test Symposium (ETS)*. IEEE. DOI: 10.1109/ETS.2016.7519331

Masoodi, F., & Pandow, B. A. (2021). Internet of things: Financial perspective and its associated security concerns. *International Journal of Electronic Finance*, *10*(3), 145–158. DOI: 10.1504/IJEF.2021.115644

Mazhar, T., Talpur, D. B., Shloul, T. A., Ghadi, Y. Y., Haq, I., Ullah, I., Ouahada, K., & Hamam, H. (2023). Analysis of IoT security challenges and its solutions using artificial intelligence. *Brain Sciences*, *13*(4), 683. DOI: 10.3390/brainsci13040683 PMID: 37190648

McRae, L., Ellis, K., & Kent, M. (2018). *Internet of things (IoT): education and technology. The relationship between education and technology for students with disabilities* [Report]. Curtin University.

Minh, T. N. (2019). Confidentiality and integrity for IoT/mobile networks. In Mitra, P. (Ed.), *Recent trends in communication networks*. IntechOpen., DOI: 10.5772/intechopen.88011

Minoli, D., Sohraby, K., & Kouns, J. (2017). *IoT security (IoTSec) considerations, requirements, and architectures. 2017 14th IEEE Annual Consumer Communications & Networking Conference*. CCNC., DOI: 10.1109/CCNC.2017.7983271

Montenegro-Marin, C. E., Gaona-García, P. A., Prieto, J. D., & Nieto Acevedo, Y. V. (2017). Analysis of security mechanisms based on clusters IoT environments. *International Journal of Interactive Multimedia and Artificial Intelligence*, *4*(3), 55. DOI: 10.9781/ijimai.2017.438

Morrison, D., Bedinger, M., Beevers, L., & McClymont, K. (2022). Exploring the raison d'etre behind metric selection in network analysis: A systematic review. *Applied Network Science*, *7*(1), 50. Advance online publication. DOI: 10.1007/s41109-022-00476-w PMID: 35854964

Morrison, P., Moye, D., Pandita, R., & Williams, L. (2018). Mapping the field of software life cycle security metrics. *Information and Software Technology*, *102*, 146–159. DOI: 10.1016/j.infsof.2018.05.011

Moulla, D. K. M., Mnkandla, E., & Abran, A. (2023). Systematic literature review of IoT metrics. *Applied Computer Science*, *19*(1), 64–81. DOI: 10.35784/acs-2023-05

Nazir, A., He, J., Zhu, N., Anwar, M. S., & Pathan, M. S. (2024). Enhancing IoT security: A collaborative framework integrating federated learning, dense neural networks, and blockchain. *Cluster Computing*, *27*(6), 8367–8392. DOI: 10.1007/s10586-024-04436-0

Nguyen, T. A., Min, D., & Choi, E. (2020). A hierarchical modeling and analysis framework for availability and security quantification of IoT infrastructures. *Electronics (Basel)*, *9*(1), 155. DOI: 10.3390/electronics9010155

Patel, K., Mistry, C., Gupta, R., Tanwar, S., & Kumar, N. (2023). A systematic review on performance evaluation metric selection method for IoT-based applications. *Microprocessors and Microsystems*, *101*, 104894. DOI: 10.1016/j.micpro.2023.104894

Pendleton, M., Garcia-Lebron, R., Cho, J.-H., & Xu, S. (2016). A survey on systems security metrics. *ACM Computing Surveys*, *49*(4), 1–35. DOI: 10.1145/3005714

Philippou, E., Frey, S., & Rashid, A. (2020). Contextualising and aligning security metrics and business objectives: A GQM-based methodology. *Computers & Security*, *88*, 101634. DOI: 10.1016/j.cose.2019.101634

Porambage, P., Ylianttila, M., Schmitt, C., Kumar, P., Gurtov, A., & Vasilakos, A. V. (2016). The quest for privacy in the internet of things. *IEEE Cloud Computing*, *3*(2), 36–45. DOI: 10.1109/MCC.2016.28

Qaisi, M., Althunibat, S., & Qaraqe, M. (2022). Phase-assisted dynamic tag-embedding message authentication for IoT networks. *IEEE Internet of Things Journal*, *9*(20), 20620–20629. DOI: 10.1109/JIOT.2022.3177157

Rachit, B., Bhatt, S., & Ragiri, P. R. (2021). Security trends in internet of things: A survey. *SN Applied Sciences*, *3*(1), 121. DOI: 10.1007/s42452-021-04156-9

Ram, R. S., Kumar, M. V., Ramamoorthy, S., Balaji, B. S., & Kumar, T. R. (2021). An efficient hybrid computing environment to develop a confidential and authenticated IoT service model. *Wireless Personal Communications*, *117*(4), 2903–2927. DOI: 10.1007/s11277-020-07056-0

Rana, B., Singh, Y., & Singh, P. K. (2021). A systematic survey on internet of things: Energy efficiency and interoperability perspective. *Transactions on Emerging Telecommunications Technologies*, *32*(8), e4166. Advance online publication. DOI: 10.1002/ett.4166

Rathor, A. S., Choudhury, S., Sharma, A., Nautiyal, P., & Shah, G. (2024). Empowering vertical farming through IoT and AI-driven technologies: A comprehensive review. *Heliyon*, *10*(15), e34998. DOI: 10.1016/j.heliyon.2024.e34998 PMID: 39157372

Reilly, E., Maloney, M., Siegel, M., & Falco, G. (2019). An IoT integrity-first communication protocol via an ethereum blockchain light client. *2019 IEEE/ACM 1st International Workshop on Software Engineering Research & Practices for the Internet of Things (SERP4IoT)* (pp. 53–56). DOI: 10.1109/SERP4IoT.2019.00016

Sagay, A., & Jahankhani, H. (2020). Consumer awareness on security and privacy threat of medical devices. In Jahankhani, H., Kendzierskyj, S., Chelvachandran, N., & Ibarra, J. (Eds.), *Cyber defence in the age of AI, smart societies and augmented humanity* (pp. 95–116). Springer., DOI: 10.1007/978-3-030-35746-7_6

Savola, R. (2007). Towards a security metrics taxonomy for the information and communication technology industry. *International Conference on Software Engineering Advances (ICSEA 2007)* (p. 60). DOI: 10.1109/ICSEA.2007.79

Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., & Stiller, B. (2022). Landscape of IoT security. *Computer Science Review*, *44*, 100467. DOI: 10.1016/j.cosrev.2022.100467

Seba, A. M., Gemeda, K. A., & Ramulu, P. J. (2024). Prediction and classification of IoT sensor faults using hybrid deep learning model. *Discover Applied Sciences*, *6*(1), 9. DOI: 10.1007/s42452-024-05633-7

Selvan, S., & Singh, M. M. (2022). Adaptive contextual risk-based model to tackle confidentiality-based attacks in fog-IoT paradigm. *Computers*, *11*(2), 16. DOI: 10.3390/computers11020016

Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data protection and privacy of the internet of healthcare things (IoHTs). *Applied Sciences (Basel, Switzerland)*, *12*(4), 1927. DOI: 10.3390/app12041927

Shen, M., Liu, H., Zhu, L., Xu, K., Yu, H., Du, X., & Guizani, M. (2020). Blockchain-assisted secure device authentication for cross-domain industrial IoT. *IEEE Journal on Selected Areas in Communications*, *38*(5), 942–954. DOI: 10.1109/JSAC.2020.2980916

Shukla, A., Katt, B., & Yamin, M. M. (2023). A quantitative framework for security assurance evaluation and selection of cloud services: A case study. *International Journal of Information Security*, *22*(6), 1621–1650. DOI: 10.1007/s10207-023-00709-8

Sirur, S., Nurse, J. R., & Webb, H. (2018). Are we there yet? Understanding the challenges faced in complying with the general data protection regulation (GDPR). *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security* (pp. 88–95). DOI: 10.1145/3267357.3267368

Stellios, I., Kotzanikolaou, P., Psarakis, M., & Alcaraz, C. (2021). Risk assessment for IoT-enabled cyber-physical systems. In Tsihrintzis, G., & Virvou, M. (Eds.), *Advances in core computer science-based technologies* (*Vol. 14*, pp. 157–173). Springer., DOI: 10.1007/978-3-030-41196-1_8

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues. *IEEE Communications Surveys and Tutorials*, *22*(2), 1191–1221. DOI: 10.1109/COMST.2019.2962586

Sun, F., Mao, C., Fan, X., & Li, Y. (2019). Accelerometer-based speed-adaptive gait authentication method for wearable IoT devices. *IEEE Internet of Things Journal*, *6*(1), 820–830. DOI: 10.1109/JIOT.2018.2860592

Taherdoost, H. (2023a). Blockchain-based internet of medical things. *Applied Sciences (Basel, Switzerland)*, *13*(3), 1287. DOI: 10.3390/app13031287

Taherdoost, H. (2023b). Security and internet of things: Benefits, challenges, and future perspectives. *Electronics (Basel)*, *12*(8), 1901. DOI: 10.3390/electronics12081901

Tariq, M. U. (2024). Enhancing cybersecurity protocols in modern healthcare systems: Strategies and best practices. In Garcia, M., & de Almeida, R. (Eds.), *Transformative approaches to patient literacy and healthcare innovation* (pp. 223–241). IGI Global Scientific Publishing., DOI: 10.4018/979-8-3693-3661-8.ch011

Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review. *Sensors (Basel)*, *23*(8), 4117. DOI: 10.3390/s23084117 PMID: 37112457

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT privacy and security: Challenges and solutions. *Applied Sciences (Basel, Switzerland)*, *10*(12), 4102. DOI: 10.3390/app10124102

Tenorio, V., Souza, L., Albuquerque, M., Marinho, R., Silva, M., & Brito, A. (2019). Low-cost, practical data confidentiality support for IoT data sources. *2019 IX Brazilian Symposium on Computing Systems Engineering (SBESC)* (pp. 1–). DOI: 10.1109/SBESC49506.2019.9046097

Tewari, A., & Gupta, B. B. (2020). Security, privacy and trust of different layers in internet-of-things (IoTs) framework. *Future Generation Computer Systems*, *108*, 909–920. DOI: 10.1016/j.future.2018.04.027

Vetrivel, S., Maheswari, R., & Saravanan, T. (2024). Industrial IOT: Security Threats and Counter Measures. In Prasad, A., Singh, T. P., & Dwivedi Sharma, S. (Eds.), *Communication technologies and security challenges in IoT* (pp. 403–425). Springer., DOI: 10.1007/978-981-97-0052-3_20

Vijayakumar, P., Obaidat, M. S., Azees, M., Islam, S. K. H., & Kumar, N. (2020). Efficient and secure anonymous authentication with location privacy for IoT-based WBANs. *IEEE Transactions on Industrial Informatics*, *16*(4), 2603–2611. DOI: 10.1109/TII.2019.2925071

Wakili, A., & Bakkali, S. (2024). AOF: An adaptive algorithm for enhancing RPL objective function in smart agricultural IoT networks. *International Journal of Intelligent Networks*. DOI: 10.1016/j.ijin.2024.09.001

Wang, L., Jajodia, S., & Singhal, A. (2017). *Network security metrics*. Springer. DOI: 10.1007/978-3-319-66505-4

Wang, T., Bhuiyan, M. Z. A., Wang, G., Qi, L., Wu, J., & Hayajneh, T. (2020). Preserving balance between privacy and data integrity in edge-assisted internet of things. *IEEE Internet of Things Journal*, *7*(4), 2679–2689. DOI: 10.1109/JIOT.2019.2951687

Wazid, M., Das, A. K., Bhat, K. V., & Vasilakos, A. V. (2020). LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment. *Journal of Network and Computer Applications*, *150*, 102496. DOI: 10.1016/j.jnca.2019.102496

Wazid, M., Das, A. K., Hussain, R., Succi, G., & Rodrigues, J. J. P. C. (2019). Authentication in cloud-driven IoT-based big data environment: Survey and outlook. *Journal of Systems Architecture*, *97*, 185–196. DOI: 10.1016/j.sysarc.2018.12.005

Wolf, M., & Serpanos, D. (2020). *Safe and secure cyber-physical systems and internet-of-things systems*. Springer., DOI: 10.1007/978-3-030-25808-5

Xiong, J., Ren, J., Chen, L., Yao, Z., Lin, M., Wu, D., & Niu, B. (2019). Enhancing privacy and availability for data clustering in intelligent electrical service of IoT. *IEEE Internet of Things Journal*, *6*(2), 1530–1540. DOI: 10.1109/JIOT.2018.2842773

Zhang, J., Rajendran, S., Sun, Z., Woods, R., & Hanzo, L. (2019). Physical layer security for the internet of things: Authentication and key generation. *IEEE Wireless Communications*, *26*(5), 92–98. DOI: 10.1109/MWC.2019.1800455

Zhao, Q., Chen, S., Liu, Z., Baker, T., & Zhang, Y. (2020). Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems. *Information Processing & Management*, *57*(6), 102355. DOI: 10.1016/j.ipm.2020.102355 PMID: 32834400

Zhou, L., Li, X., Yeh, K. H., Su, C., & Chiu, W. (2019). Lightweight IoT-based authentication scheme in cloud computing circumstance. *Future Generation Computer Systems*, *91*, 244–251. DOI: 10.1016/j.future.2018.08.038

Dr. Hamed Taherdoost is an award-winning leader in research and development, known for his contributions across both industry and academia. He is the founder of Hamta Business Corporation, Associate Professor and Chair of RSAC at University Canada West, & Director of R&D at Q Minded | Quark Minded Technology Inc. He has over 20 years of experience in both industry and academic sectors. He has worked at international companies from Cyprus, the UK, Malta, Iran, Malaysia, and Canada and has been highly involved in development of several projects in different industries, healthcare, transportation, residential, oil and gas and IT. Additionally, he has served as a trusted technical and technology consultant for multiple companies, providing advisory and mentorship. In academia, Dr. Taherdoost has held teaching positions in Southeast Asia, the Middle East, and North America since 2009. He began his academic career as a lecturer at AU & PNU and later served as an adjunct professor and faculty fellow at Westcliff University, USA. His research tenure at IAU lasted over eight years, during which he supervised numerous students. Dr. Taherdoost has organized and chaired many workshops and conferences and has frequently been invited as a keynote speaker. He is an active member of the editorial, reviewer, and advisory boards for several prestigious journals published by Taylor & Francis, Springer, Emerald, Elsevier, MDPI, EAI, IGI Publishing, and Inderscience. He has also participated as an organising, scientific and technical committee member in over 270 conferences held across Europe, America, Australia, Asia, and Africa. He published over 250 scientific articles published in top-tier journals and conference proceedings. His work has been widely recognized, evidenced by an h-index of 42, i10-index of 95, over 15,700 citations on Google Scholar, more than 3.1 million reads, and 8,000 citations on ResearchGate, and 234,000 downloads on SSRN as of May 2024. He has also contributed 30 book chapters, 14 edited books as well as 13 authored books in the field of technology and research methodology. Dr. Taherdoost's leadership and innovation have earned him numerous accolades, including THE BIZZ Business Excellence Award, PeerJ Award, and recognition at the Asia Corporate Excellence & Sustainability Awards. He was a finalist for the Innovation in Teaching of Research Methodology Excellence Awards and Southeast Asian Startup Awards by Global Startup Awards. Additionally, his research achievements also include winning several best paper awards, outstanding reviewer awards and best presentation awards like MLIS Best Presentation Award of 2021 & 2022, the Outstanding Editorial Board Member award from Bilingual Publishing Co., Best Paper of the Year of Computers MDPI, and Best Interview Award of Encyclopedia. His rankings include being listed among 10 top SSRN Business Authors (2022, 2023 & 2024) and featured in the Stanford-Elsevier list of the world's top 2% of Scientists in 2021, 2022 and 2023. He is the Editor of International Journal of Information Technology Project Management, IGI (IF: 0.8), EAI Endorsed Transactions on Scalable Information Systems, EAI (Q2), International Journal of Electronic Government Research, IGI (IF: 1.2), Information Resources Management Journal, IGI (IF:1.4), Journal of Blockchain MDPI, and and International Journal of Data Mining, Modelling and Management (IF: 0.5 & CS: 0.9) by InderScience. He is Associate Editor of Frontiers in Research Metrics and Analytics (Scopus). He's been a guest editor of special issues in Results in Engineering, Elsevier (IF: 5 & CS:4.5), Electronics MDPI (IF: 1.9 & CS: 4.7), Computers MDPI (IF:2.8 & CS: 4.7), Discover Computing by Springer and Academic Editor of PLOS ONE. He is a Certified Cyber Security Professional and Certified Graduate Technologist. He is a GUS Fellow - GUS Institute | Global University Systems, senior member of IEEE, IAEEEE, IASED, IEDRC & HKSRA, Fellow Member of ISAC, Working Group Member of International Federation for Information Processing - IFIP TC 11 - Human Aspects of Information Security and Assurance and Information Security Management and member of CSIAC, ACT-IAC, and AASHE. Currently, he is involved in several multidisciplinary research projects, including studying innovation in information technology, blockchain and cybersecurity, and technology acceptance.