2021

A review of security standards and frameworks for IoT-based smart environments

Nickson M. Karie
Edith Cowan University

Nor Masri Sahri
Edith Cowan University

Wencheng Yang
Edith Cowan University

Craig Valli
Edith Cowan University

Victor R. Kebande

10.1109/ACCESS.2021.3109886
Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A review of security standards and frameworks for IoT-based smart environments. *IEEE Access, 9,* 121975-121995. https://doi.org/10.1109/ACCESS.2021.3109886

Received August 13, 2021, accepted August 29, 2021, date of publication September 3, 2021, date of current version September 10, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3109886

A Review of Security Standards and Frameworks for IoT-Based Smart Environments

NICKSON M. KARIE[1,2], (Member, IEEE), NOR MASRI SAHRI[1,2], WENCHENG YANG[1,2], CRAIG VALLI[1,2], (Member, IEEE), AND VICTOR R. KEBANDE[3,4]

[1]Cyber Security Cooperative Research Centre Ltd., Joondalup, WA 6027, Australia
[2]School of Science, Security Research Institute, Edith Cowan University, Joondalup, WA 6027, Australia
[3]Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, 97187 Luleå, Sweden
[4]Department of Computer Science, Blekinge Institute of Technology, 37179 Karlskrona, Sweden

Corresponding author: Nickson M. Karie (n.karie@ecu.edu.au)

This work was supported by Cyber Security Research Centre Ltd., funded through the Australian Government's Cooperative Research Centres Programme.

ABSTRACT Assessing the security of IoT-based smart environments such as smart homes and smart cities is becoming fundamentally essential to implementing the correct control measures and effectively reducing security threats and risks brought about by deploying IoT-based smart technologies. The problem, however, is in finding security standards and assessment frameworks that best meets the security requirements as well as comprehensively assesses and exposes the security posture of IoT-based smart environments. To explore this gap, this paper presents a review of existing security standards and assessment frameworks which also includes several NIST special publications on security techniques highlighting their primary areas of focus to uncover those that can potentially address some of the security needs of IoT-based smart environments. Cumulatively a total of 80 ISO/IEC security standards, 32 ETSI standards and 37 different conventional security assessment frameworks which included 7 NIST special publications on security techniques were reviewed. To present an all-inclusive and up-to-date state-of-the-art research, the review process considered both published security standards and assessment frameworks as well as those under development. The findings show that most of the conventional security standards and assessment frameworks do not directly address the security needs of IoT-based smart environments but have the potential to be adapted into IoT-based smart environments. With this insight into the state-of-the-art research on security standards and assessment frameworks, this study helps advance the IoT field by opening new research directions as well as opportunities for developing new security standards and assessment frameworks that will address future IoT-based smart environments security concerns. This paper also discusses open problems and challenges related to IoT-based smart environments security issues. As a new contribution, a taxonomy of challenges for IoT-based smart environment security concerns drawn from the extensive literature examined during this study is proposed in this paper which also maps the identified challenges to potential proposed solutions.

INDEX TERMS Control measures, IoT-based smart environments, risks, security assessment frameworks, security standards, taxonomy, threats.

I. INTRODUCTION

The Internet of Things (IoT) is relatively a new and emerging technology that is gaining popularity among many stakeholders. According to [1] IoT technology has brought about revolutionary impacts in many areas of our lives. Besides, it has become a key enabler of innovation and success in a wide range of fields including IoT-based smart environments [2]. IoT has also paved the way for the emergence of other IoT-based smart technologies which allow individuals to connect and control smart devices and appliances remotely using computers, smartphones, or tablets through the internet. Interconnected devices in an IoT-enabled smart environment allow individuals to control different device functions remotely through the internet [1]. However, it is common in a smart environment to find both IoT, as well as other non-IoT devices and services, blend to enhance the quality of life of people [3]. Connecting one's devices and appliances to the Internet,

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

however, exposes them as well as the data sensed, collected, and exchanged by them to a wide range of security threats and risks. Besides, every connected device can become a potential entry or attack point for malicious intruders hence the need for assessing and hardening IoT-based smart environments security.

While IoT is still expected to impact many other upcoming areas of our lives [4]; there are inherent security and privacy concerns that need to be continuously addressed. However, due to the dynamic, and heterogeneous nature of IoT-based smart environments, addressing many of the security and privacy issues is always a challenge. Security assessment of IoT-based smart environments such as smart homes and smart cities, for example, can be hard in environments where the status, posture, or security landscape, as well as the extent of the network visibility is not known. What makes security assessment in IoT-enabled smart environments even more challenging is the fact that once deployed the type and nature of most interconnected IoT devices or appliances rarely offer ongoing professional support to individuals in either their design or operation phases [1]. The lack of ongoing professional support thus impacts the security and privacy needs of many IoT-based smart environments.

Confronted by the security challenges in IoT-based smart environments, the authors in this paper conducted a review of existing conventional security standards and assessment frameworks highlighting their primary areas of focus to uncover those that can potentially address some of the security needs of IoT-based smart environments. A total of 80 ISO/IEC security standards, 32 ETSI standards and 37 different security frameworks which included 7 NIST special publications on security techniques were reviewed. The findings of this study can help IoT practitioners, researchers and other stakeholders understand the state-of-the-art of the domain as well as help them identify new research directions and spark further discussions on the development of new security standards and assessment frameworks to address existing and future security problems in IoT-based smart environments.

As a contribution, this paper thus aims to fulfil the following objectives:

1) To review existing security standards and assessment frameworks which include NIST special publications on security techniques to uncover their primary areas of focus and exposed the state-of-the-art and background of the domain.
2) To identify and discuss open problems and challenges related to IoT-based smart environment security concerns.
3) To propose and discuss a taxonomy of challenges for IoT-based smart environment, drawn from the extensive literature examined during this study, that also maps potential solutions to the identified open challenges and other future IoT smart technologies security issues.

As for the remaining part of the paper, section II presents an overview and motivation for this study while the background and existing research work are presented in section III. Section IV explains the research methodology used in this study followed by section V which presents reviews on conventional security standards and assessment frameworks. Section VI presents open problems and challenges related to IoT-based smart environments. As a new contribution section VII proposes and discusses a taxonomy of challenges for IoT-based smart environment in tandem with proposed potential solutions to the identified challenges. Finally, the paper concludes in section VIII and makes mention of future research work.

II. OVERVIEW AND MOTIVATION

This review was motivated by the understanding that conventional security standards and assessment frameworks meant for use in non-IoT environments are very different and many may not directly address the needs of IoT-based smart environments. This paper thus investigates the potentials that conventional security standards and assessment frameworks have in addressing IoT-based smart environments security concerns by exposing their primary areas of focus as well as the state-of-the-art and background of the domain.

While the benefits and prospects of an expanded IoT-based smart environment are huge, so does the attack surface. Consequently, an increased number of IoT devices, ecosystems and integration has meant that many vulnerable endpoints are being witnessed daily, especially in smart homes, smart cities, global enterprises, and critical infrastructures. IoT-based smart environments are currently a trend that is daily expanding, however, this expansion comes with a lot of complexity, integration, and security issues in the different areas of application. Because of these foregoing, a review of existing conventional security standards and assessment frameworks is positioned to uncover key and perennial security issues in IoT-based smart environments.

Additionally, the authors note with concern that based on the literature that has been reviewed in this paper, there is still a deficiency of specialized security standards and assessment frameworks that are primarily inclined to IoT-based smart environments. For this reason, key discoveries and conclusions in this study are explicitly based on leveraging the content of existing conventional security standards and assessment frameworks that are deemed to have the potential to be used in IoT-based smart environments. This study also identifies and discuss open problems and challenges while at the same time proposing a taxonomy of challenges for IoT-based smart environment mapping the identified challenges to potential solutions that can help address existing and future IoT security issues.

Furthermore, based on the exploration and the review conducted in this paper, it is evident that many existing or proposed solutions have had a limited scope when exploring security standards and assessment frameworks, however, this study is explicitly not limited to security standards in general and consideration of assessment frameworks has also been included to enrich the study as well as allow for broad and in-depth findings. The combination of relevant literature in security standards and assessment frameworks in this study helps to avoid generalization and opens up this study to a wider scope. Figure 1 shows an overview of the overlapping key aspects that motivated this study which also forms the primary focus areas of this paper.

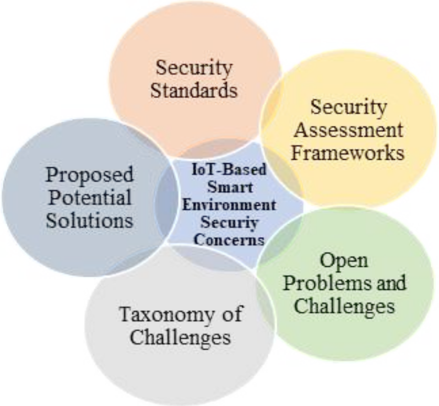
Security Standards
Security Assessment Frameworks
Proposed Potential Solutions
IoT-Based Smart Environment Securiy Concerns
Open Problems and Challenges
Taxonomy of Challenges

FIGURE 1. **Overview of the key aspects explored in this study.**

The authors also acknowledge that the key aspects explored in this study as shown in Figure 1 are not only applicable in this study but can also be used in different IoT application areas including those outside the scope of this paper. This paper explicitly focused on existing conventional security standards and assessment frameworks and their potentials to be adapted to IoT-based smart environments. However, as a key aspect, this paper also looked at different open problems and challenges while at the same time proposing a taxonomy of challenges mapped to potential solutions as highlighted in Figure 1.

III. BACKGROUND AND EXISTING RESEARCH WORK

Like many other fields, the IoT domain is growing very fast. However, with this growth comes many cybersecurity challenges. Previous research in the IoT domain has mostly focused on finding control measures to address deficiencies in different areas of IoT including security, privacy, vulnerabilities, and resiliency [5]–[8]. However, the need for security standards and assessment frameworks that specifically focuses on IoT-based smart environments is also as important as the research itself. As part of the background and existing research work, this section will focus on the security and privacy concerns for IoT-based smart environments as well as existing research on security standards or assessment frameworks. It is also important to note at this point that privacy is not a primary focus of this study and is not explored further beyond the background section.

A. SECURITY AND PRIVACY CONCERNS IN IoT-BASED SMART ENVIRONMENTS

In IoT-based smart environments, a lot of data and information get shared among various devices. Without a good security standard or security assessment mechanism in place, the data and information moving in and around these environments can become susceptible or vulnerable to a variety of security threats and risks [9]. Some of the concerns relating to data and information in IoT-based smart environments as discussed by [3], [5]–[12] are summarized in the subsections below.

1) SECURITY CONCERNS

- **Data and Information Leakage**: In any IoT smart environment, without proper security mechanisms that protect data and information from malware and other malicious intruders, personal information could easily be leaked resulting in security breaches [11].
- **Eavesdropping**: With information moving in and around IoT-based smart environments and over to the Internet, malicious attackers can take advantage of unsecured network communications and steal data as it is being transmitted between the connected IoT devices which can lead to other serious security breaches.
- **Hacking**: Most of the data and information collected by IoT devices within smart environments may be stored on internet-accessible systems like the ‘‘Cloud’’. Many cloud-based IoT devices and systems are known to have security vulnerabilities and can easily be victims of hacking and cyberattacks as data transmission like video data from cameras may not even be encrypted when sent over the internet.
- **Software Exploitation:**Because of the lack of standardization in many IoT-based smart environments, rogue software can easily find its way into IoT devices through firmware upgrade and trusted boot, device acquisition as well as apps and services. This can affect service delivery by altering device configurations. Besides, many IoT devices run on autonomously lightweight versions of the well-known operating system which hackers can search for software vulnerabilities and exploit them to gain privileged access to sensitive information [7].
- **IoT Device Security**: Because of the lack of specialized universal approved IoT security standards or security assessment frameworks, some devices may be manufactured with poor security baselines such as old and unpatched embedded operating systems and software, weak, guessable, or hard-coded passwords, insecure data transfer and storage, among others. This makes such IoT devices vulnerable to different security threats and attacks.
- **IoT Device Hijacking and Ransomware**: As a result of poor security, lack of specialized universal approved IoT security standards, assessment frameworks, and rising numbers in the use of IoT devices, many of these devices may soon become easy targets of ransomware attacks.
- **Technology Minded and Security Aware Users**: With the growing innovation of IoT technologies, many users are yet to understand how modern IoT devices are designed and function. This makes it easy for attackers

to use social engineering to trick IoT device users into providing sensitive data or information which can be used to gain access into smart environment networks, such as smart homes and smart cities, putting everyone's life at risk.

- **Insufficient IoT Device Testing and Updates**: Most of the IoT devices are produced quickly to meet the increasing market demands and hence do not undergo proper testing or follow any acceptable security standards or assessment frameworks. Users mostly put their trust in the manufactures to test the IoT devices as well as provide security control measures. However, due to high demands, many manufacturers focus more on creating and releasing new products to the market without having proper testing or putting security control measures in place. Besides, old IoT devices may no longer be updated or take long to be updated resulting in security risks in IoT-based smart environments.
- **Lack of Active Device Monitoring**: Monitoring IoT devices can be challenging [10]. This is because most of the existing monitoring tools and practices especially those focusing on the cloud were traditionally designed to monitor time-series metric data with no focus on modern IoT devices or their processes. Lack of active IoT device monitoring tools makes it hard to have full network visibility in IoT-based smart environments. Besides, there exist a lack of such tools that can be used to directly monitor individual IoT devices deployed in IoT-based smart environments.
- **Shortage of Efficient and Robust Security Protocols**: The lack of efficient and robust security protocols including proper IoT security standards, assessment frameworks and safeguards could lead to security breaches in smart environments leading to personal data exfiltration [10], [13].
- **Impersonation:**With many IoT devices in smart environments lacking strong authentication or access control mechanisms, it becomes easy for intruders to impersonate a legitimate user and use the credentials or any other information that gives them access to existing IoT resources in an IoT-based smart environment [7]. Successful impersonation could further be used to escalate other serious security attacks.
- **Health and Safety of Users**: If a hacker gains access to an IoT-based smart environment such as smart homes, he or she may, for example, try to change medical prescriptions or order products that the homeowner does not need or is allergic to. As a result, the health of the homeowner and the entire family is at risk because they may not have time to verify the automation processes initiated by the hackers [14].
- **Denial of Service (DoS/DDoS)**: With the advancement in technology, hackers can try to cause a DoS/DDoS to existing hubs in IoT-based smart environment networks or the sensors themselves [7]. However, attackers can also access the network and send bulk messages to IoT devices such as Clear To Send (CTS) and Request To Send (RTS) [11] causing DoS attacks to legitimate IoT devices.
- **Other Security Threats:** With the rapid growth in the number and usage of IoT devices, other security threats may also exist in IoT-based smart environments such as home invasions, trespass, falsification [11] rogue and counterfeit IoT devices, botnet attacks, physical attacks, unintentional damage or loss, disasters and outages, failures or malfunctions, [3] dynamic systems, authentication, unsecured wireless network problems [5], side-channel attack, man-in-the-middle, identity theft, advanced persistent threat (APT) [13], jamming, function creep, buffer overflow, large-scale unauthorized data mining, surveillance, unauthorized access or deletion or modification of data, worms, viruses and malicious code [15], the openness of the networked systems, weak passwords, fixed firmware [16], resource constraints, headless nature of IoT devices, tamper-resistant packages, heterogeneous protocols, dynamic characteristics, longevity expectations [17] among many other security threats.

2) PRIVACY CONCERNS

Privacy in IoT-based smart environments according to [18] means that "*information about individuals must be protected and should not be exposed without explicit consent from the owners under any circumstances*". Because of the ease of connectivity of IoT devices to the internet, and the lack of proper security mechanisms or common security standards and assessment frameworks designed for IoT-based smart environments, the risk of exposure of personal data or information into the hands of malicious attackers can be high [10]. Some of the privacy concerns related to IoT-based smart environments include:

- **Data Storage and Usage**: with the introduction of cloud storage by third parties [19], [20] many IoT devices can easily store generated or collected data from smart environments in public cloud infrastructure. The problem, however, is that there is a lack of standardization on how to store and process IoT data from different sources that are mostly unstructured and can lead to a breach of privacy. This, therefore, calls for the development of universal security and privacy standards, best practices, methods, and tools that can consistently handle IoT data as well as ensure that distributed data is securely accessed and transported [21] with high levels of privacy either to the public or private clouds.
- **Tracking and Location Privacy**: Because of the ease and availability of internet connectivity to IoT devices, tracking users based on location is very common. Once a malicious attacker identifies a user, they can collect data that tracks the user behaviour [18] including location history which the attacker can use to stalk a user leading to a breach of privacy.

- **Context-Aware or Situational Privacy**: As a result of poor security mechanisms implemented in some IoT devices, detecting, spotting, and locating users' movement, activities, and gathering data based on actions can be possible [16] leading to a breach of privacy.
- **Sensed, Generated or Collected Data Privacy**: Some manufactures of IoT devices can design their firmware to collect data sensed or generated by the devices especially about the usage of services and other data about their customers. The data or information collected in this manner may not fully adhere to the privacy needs of the users, especially during transmission and may lead to a breach of user privacy.
- **User Privacy Information Mining**: Because of non-fully protected network communication in IoT networks, privacy mining as discussed by [22] can be used to mine private information from smart homes or smart cities leading to other serious security and privacy breaches.
- **Other privacy concerns** that have been identified in the literature include user profiling, utility monitoring and controlling [18], collection, use and disclosure of IoT data without the users' consent, de-identification of IoT data, dependency on vendors, interoperability, managing IoT devices, accountability, and transparency [23]. As mentioned earlier, this paper will not discuss privacy concerns further. The next section elaborates on some of the existing research work on security assessment frameworks.

B. EXISTING RESEARCH WORK

In literature, several security standards, assessment frameworks, and special publications on security techniques exist which can be used in different environments (e.g., network security, world wide web security, applications security, telecommunication among other areas). However, these security standards and assessment frameworks were primarily designed with specific application environments in mind hence different steps or processes for different environments are involved as highlighted later in section V. Researchers in the IoT domain have also proposed different approaches and techniques to address different IoT deficiencies and forms the basis of the existing research work in this section.

In [24], the authors proposed IoT-based integrated home security and monitoring system. The authors argued that home security remains a critical issue hence the need for a security and monitoring system for IoT-based smart home environments. Their proposed system, however, focused on detecting intruders, room temperature, humidity, rain, fire, as well as monitor the light condition. The security of the individual devices and the entire security landscape of the smart home after device deployment was not considered in their research which can leave the smart home vulnerable to a variety of security threats and risks.

An end-to-end security assessment framework based on Software Defined Network (SDN) to evaluate the security level for CloudIoT was developed by [25]. Their study was motivated by the existence of numerous choices of cloud-resource providers and IoT devices and not necessarily IoT-based smart environments. Their research stated that evaluating the security levels of both the cloud-resource providers and IoT devices is very important in promoting the adoption of CloudIoT and reduce business security risks [25]. The current paper, however, focuses on reviewing security standards and assessment frameworks to identify those that have the potential to address IoT-based smart environments security concerns.

Another study by [26] argued that security has become a vital factor for any IoT smart environment. For this reason, they proposed in their research an Identified Security Attributes (ISA) framework to evaluate the security features of the Internet of Health Things (IoHT) based devices in the healthcare environment. Their study was motivated by the understanding that fragile patient's data always moves from IoT devices to servers. During transmission, patient's data can fall into the hands of malicious attackers. For this reason, their study concluded that proper security is indispensable for IoHT based equipment due to their exposure to different security attacks [26].

Research by [27] stated that the rapid growth of IoT-based systems raises security concerns making a security assessment framework for IoT systems imperative. The authors then proposed an assessment framework to evaluate the security features of IoT-based equipment using hybrid multi-criteria decision making (MCDM) methodology and later carried out an empirical study on the assessment of IoT-based healthcare devices [27].

More research by [28] claimed that patient's data is very critical and so is its secure transmission in smart healthcare applications. In their research [28] proposed a framework to protect medical information from external threats which the authors claim has both scientific as well as economic significance as it consumes less possible resources of low-powered medical devices; thus, it could be used for real-time healthcare applications.

In another research, the authors in [29] state that ''*in inventory automation, real-time check on items, their information management, and status management, monitoring can be carried out using IoT*''. However, the data that flows among the devices in the network demands a security assessment framework that ensures authentication, authorization, integrity, and confidentiality. For this reason, the authors proposed ''a lightweight IoT-based security assessment framework for inventory automation using wireless sensor networks [29].

Research by [30] proposed a secure and compliant continuous assessment framework for evaluating the security and compliance levels of cloud services. The proposed framework facilitates cloud service to customers to select an optimal cloud service provider (CSP) who satisfies their desired security requirements. However, the framework also enables cloud service customers to evaluate the compliance of the selected CSP in the process of using cloud services [30].

Research by [31] designed and implemented a risk assessment framework for cloud service providers meant to provide assurance that will lead to higher confidence of cloud service consumers on one side and cost-effective and reliable productivity of cloud service providers and resources organized by individual infrastructure providers on the other side.

Denning *et al.* [32] proposed a framework for evaluating security risks associated with technologies used at home. On the same note, Kang *et al.* [33] proposed an enhanced security framework for smart devices in a smart home environment meant to provide integrity using self-signing and access control techniques for preventing security threats such as data modification, leakage, and code fabrication. Table 1 below provides a summary of the existing work discussed and their primary focus areas.

TABLE 1. Existing research work and their primary focus areas.

	Primary Focus Areas		
Proposed Frameworks	*Smart Home*	*Cloud IoT*	*IoT Health*
IoT-based Integrated Home Security and Monitoring System [24].	√		
End-to-end Security Assessment Framework based on Software Defined Network (SDN) [25].		√	
An Identified Security Attributes (ISA) Framework [26].			√
An Assessment Framework to Evaluate Security Features of IoT-based Equipment [27].	√		√
A Framework to Protect Medical Information [28]			√
A Lightweight IoT-based Security Framework for Inventory Automation Using Wireless Sensor Network [29].	√	√	√
A Secure and Compliant Continuous Assessment Framework for Evaluating the Security and Compliance Levels of Cloud Services [30].	√	√	
An Effective and Efficient Risk Assessment Framework for Cloud Service Providers [31]	√	√	
A Framework for Evaluating Security Risks Associated with Technologies used at Home [32]	√		
An Enhanced Security Framework for Smart Devices in a Smart Home Environment [33]	√		

Infer from the summarized research works in Table 1 that most of it does not directly focus on providing security assessment for IoT-based smart environments, but only specific application areas thus do not fully cater for all the primary security needs of IoT-based smart environments. Table 1 further justifies the need for developing new security standards and assessment frameworks for IoT-based smart environments. The next section discusses the research methodology used to conduct the review in this paper.

IV. METHODOLOGY

In conducting the review process, the authors in this paper adopted the guidelines and principles that shows systematic methods that uphold the theoretical validity of the study. These guidelines pinpoint the need for identifying the key study area, sampling, extracting useful data and interpreting the validity of these data and finally mapping the outcome as potential results. Based on the same notion, this study primarily focused on identifying the relevant articles on security standards and assessment frameworks including NIST special publication on security techniques, examining them to find whether they satisfy the suggested selection criteria and disseminating the findings while identifying the existing research gaps or challenges as is shown in Figure 2. The review methodology used in this study comprises of three primary phases as follows:

- **Phase I:** Study area identification, the definition of research questions, sampling and defining the key search strategy or criteria.
- **Phase II:** Applying the search strategy or criteria to known literature, conducting snow bowling search, database search, evaluating the search and defining the selection criteria.
- **Phase III:** Identifying the accepted literature, articles, papers, websites and web documents for review and reviewing based on the selected key study topic.

A. PHASE I: STUDY AREA IDENTIFICATION

Study area identification in the context of this paper was based on several research questions that also formed the basis of the whole study. Given that the objective is to review the current state of the art of security standards and assessment frameworks, this holds as the guiding principle that shows the key activities that could be leveraged for IoT-based smart environments. Based on this objective the key research questions for this study have been coined as follows:

- **RQ1:** What is the current state of the art of conventional security standards and assessment frameworks with regards to IoT-based smart environments security concerns?
- **RQ2:** Which of the existing conventional security standards and assessment frameworks can be adapted to help address some of the primary security requirements of IoT-based smart environments?
- **RQ3:** What are the open problems and challenges based on the existing exceptions in the security standards and assessment frameworks?

Basing our study on the above-mentioned research question, the next phase addresses the key search strategy.

B. PHASE II: SEARCH STRATEGY

The second phase is based on conducting an online search. The scope of this study has been inclined towards security standards and assessment frameworks which also include NIST special publications on security techniques.

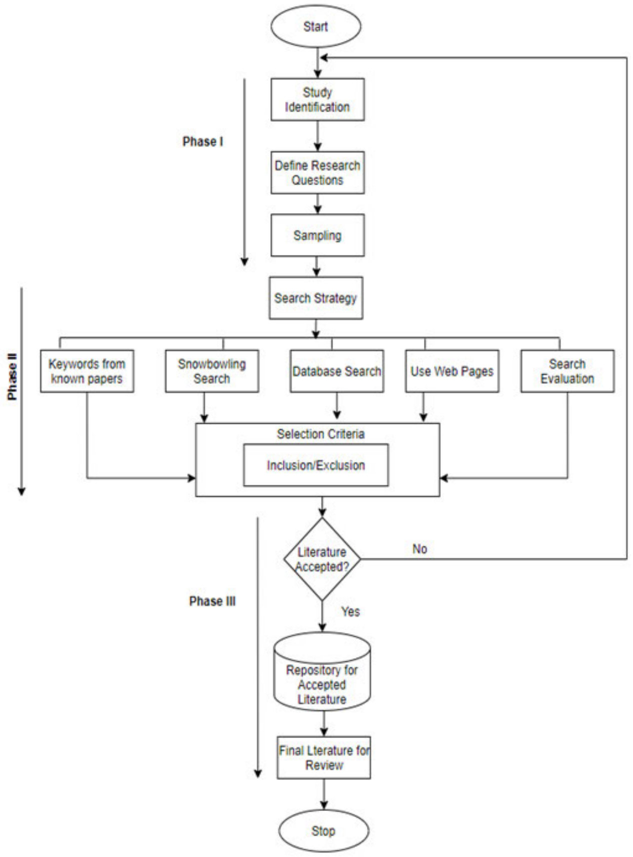

FIGURE 2. Research methodology.

As a result, the authors explored Google Scholar, ACM, Springer Link, IEEE Xplore, Web of Science, Web Search Engines and Scopus with the queries and search strings shown in Table 2.

TABLE 2. Queries and search strings used.

Search Query	Search Strings
RQ1	"Security Standard" OR "Security Assessment Framework" OR "Security Techniques"
RQ2	"Security Standard for IoT-based Smart Environments" OR "Security Assessment Framework for IoT-based Smart Environments"
RQ3	"Open Problems" AND "Security Challenges in IoT-based Smart Environments"

After conducting a keyword search based on the criteria mentioned in Table 2, the number of papers, online articles, web documents and other special publications obtained is summarized in Table 3.

C. PHASE III: IDENTIFYING AND REVIEWING THE LITERATURE

To filter the selected papers, online articles, and special publications the following approach was adopted:

TABLE 3. Total number of resources identified based on the search criteria.

Article Source	RQ1	RQ2	RQ3	Total
IEEE Xplore	38	50	28	116
Google Scholar	74	62	52	188
Search Engines	118	95	104	317
ScienceDirect	42	48	37	127
SpringerLink	8	15	10	33
Web of Science	20	12	18	50
Total	**300**	**282**	**249**	**831**

- The paper, article, websites, web document or other special publications are only included in the next phase when all the authors agree that they hold some relevance based on the study objectives.
- Doubted papers, articles, websites, web documents or any other special publications are jointly reviewed to show if they satisfy the selection criteria in part or fully as shown in Figure 2.
- Papers, articles, websites, web documents or any special publications considered not to be relevant by all the authors were deleted or removed from the selection criteria.
- All accepted papers, articles, websites, web documents and special publications were included in a repository ready to be reviewed.

During this phase, all the gathered literature, 831 in total was subjected to thorough readings by the authors with two objectives in mind: the first objective was to extract all the relevant data needed for our study while the second objective was to check for the correctness and relevance of the extracted data. The information considered from each literature was inclined towards the primary objectives of this study. After reviewing the titles, abstracts, and sections of all the 831 identified literature resources shown in Table 3, a total of 617 literature resources were deemed irrelevant and excluded from the selection criteria. Of the 214 that remained, 131 were categorized as doubtful. Consultation and discussions formed the basis of this process especially on any agreement and consensus to be made on any of the literature under contention or categorized as doubtful. After many considerations based on the content of each paper, article, websites, web documents and other literature resources, a total of 149 data items were extracted from the accepted literature that was deemed relevant by the authors which included, 80 ISO/IEC security standards, 32 ETSI standard and 37 different security assessment frameworks (including 7 NIST special publications on security techniques). The 149 identified data items formed the final repository for review and are summarized in Table 4.

The next section presents a review of all the selected security standards and assessment frameworks including the NIST special publications on security techniques. This section aims to uncover the primary focus area of each of the security standard and assessment frameworks identified and selected from the literature to find out which of them potentially addresses some of the security requirements or needs of IoT-based smart environments and if not, can be adapted to handle IoT-based smart environments security concerns.

V. REVIEW OF EXISTING SECURITY STANDARDS AND ASSESSMENT FRAMEWORKS

Existing security standards offer insight into recommended security controls, processes, procedures, baselines, and guidelines that are deemed ideal for networks and in some cases mandatory for compliance [34]. Most existing security assessment frameworks, on the other hand, offer security best practices, methods and guidelines that organizations can embrace to get the best results for implementing a successful program [34]. However, IoT-based smart environments networks raise new security concerns that are not directly addressed by most of the existing conventional security standards and assessment frameworks [3]. This section of the paper, therefore, reviews the existing security standards and assessment frameworks including some NIST special publications identified and selected from the reviewed literature highlighting their primary areas of focus to uncover those that can potentially be adapted to address the security needs of IoT-based smart environments.

A. EXISTING SECURITY STANDARDS AND ASSESSMENT FRAMEWORKS

Table 4 shows a summary of the different security standards and assessment frameworks identified, selected and discussed in this section including the owner and the primary focus area of each standard and framework. Note also that some of the standards and assessment frameworks discussed in this section are specialized by industry or geographic region. A more detailed description of each identified standard and assessment framework is given in the sub-section to follow.

1) NIST CYBERSECURITY FRAMEWORK

The NIST cybersecurity framework was created based on a set of industry standards and best practices to help organizations manage their critical infrastructure cybersecurity risks [35]. Because IoT is becoming a part of critical infrastructure, this framework has the potential to be used in IoT-based smart environments. The framework consists of a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, offering detailed guidance for developing individual organizational profiles. Specifically, the framework is broken down into five key functions (identify, protect, detect, respond, and recover) that manage the risks to data and information security [36].

- **Identify**: Helps organisations develop an understanding of how to manage cybersecurity risk to systems, people, assets, data, and capabilities [37] including asset management, business environment, and information technology governance through comprehensive risk assessment and management processes.

TABLE 4. Summary of existing security standards and assessment frameworks, methods, and guidelines.

Name of Framework	Owner	Primary Focus Areas
NIST Cybersecurity Framework [35]	National Institute of Standards and Technology (USA)	Integrates industry standards and best practices to help organizations manage and improve their critical infrastructure cybersecurity risks (threats, vulnerabilities, and impacts) [36].
NIST Risk Management Framework (RMF) [38]	National Institute of Standards and Technology (USA)	Manage information security and privacy risk for organizations and systems [38]
NIST Privacy Framework [40]	National Institute of Standards and Technology (USA)	Focus on improving privacy through enterprise risk management [40]
NIST SP 800-53 [39]	NIST (USA)	Focus on security and privacy controls for information systems and organizations [39]
NIST SP 800-30 [41]	NIST (USA)	Focus on providing guidance for conducting information systems risk assessments [41]
NIST SP 800-37 [42]	NIST (USA)	Focus on providing guidelines for applying the RMF [38] to information systems and organizations [42].
NIST SP 800-39 [43]	NIST (USA)	Focus on providing guidance for an integrated, organization-wide program for managing information security risk to organizational operations [43]
HIPAA [82].	Department of Health and Human Services (HHS) -USA	Focus on standards for electronic health records as well as the security and privacy of sensitive health information [82].
Family Education Rights and Privacy Act (FERPA) [47]	U.S. Department of Education	Focus on protecting student educational records [47].
PCI-DSS [48]	PCI Security Standards Council - USA	Focus on protecting consumer financial information when stored electronically [48].
Cybersecurity Maturity Model Certification (CMMC) [50]	Department of Defense (DoD)-USA	Focus on normalizing and standardizing cybersecurity preparedness across the federal government's defence industrial base (DIB) [50].
Cybersecurity Capability Maturity Model (C2M2) [52]	U.S. Department of Energy (DOE)	Focus on consistently measuring the maturity levels of cybersecurity capabilities in an organisation [52].
FFIEC Cybersecurity Assessment Tool [53]	Federal Financial Institutions Examination Council (FFIEC)	Focus on identifying organisations risks and determine their cybersecurity preparedness [53].
NERC 1300 Standard [55]	North American Electric Reliability Corporation	Focus on reducing risks to the reliability of the bulk electric systems from any compromise of critical cyber assets [55]
NERC-CIP Standards [56]	North American Electric Reliability Corporation	Focus on providing specific guidance on cybersecurity for the North American power systems [56].
ANSI/ISA 62443 [57]	International Society of Automation	Focus on processes, techniques and requirements for Industrial Automation and Control Systems (IACS) including Secure product development lifecycle requirements [57].
FISMA 2014 [75]	Cybersecurity and Infrastructure Security Agency	Focus on security requirements that government agencies can use to enhance their cybersecurity posture [75].

TABLE 4. ***(Continued.)*** **Summary of existing security standards and assessment frameworks, methods, and guidelines.**

General Data Protection Regulation (GDPR) [58]	European Parliament and Council of the European Union	Focus on data protection and privacy in the European Union and the European Economic Area [58].
SOC 2 [59]	American Institute of Certified Public Accountants (AICPA)	Focus on providing guidance on security, availability, integrity, and privacy of sensitive user information to organizations that collect and store personal customer information in cloud services [59].
Threat Assessment and Remediation Analysis (TARA) [60]	Jackson E. Wynn, The MITRE Corporation	Focus on identifying and assessing cyber vulnerabilities and selecting countermeasures effective at mitigating those vulnerabilities [60].
Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) [61]	Carnegie Mellon University (CMU) and U.S. Department of Defence.	Focus on identifying and managing information security risks [61].
IASME Governance [62].	IASME Consortium. UK	Focus on information assurance for small and medium-sized enterprises [62].
CIS v7 [65]	Center for Internet Security (CIS) - USA	Focus on enhancing the security standards of all organizations [65].
Control Objectives for Information and Related Technologies (COBIT) [66]	Information Systems Audit and Control Association (ISACA) -USA	Focus on IT security, governance, and management [66].
Committee of Sponsoring Organizations (COSO) [68]	COSO	Focus on identifying and managing enterprise cybersecurity risk, internal control, and fraud deterrence [68].
Technical Committee on Cyber Security (TC CYBER) [71]	TC CYBER	Focuses on improving privacy awareness for individuals or organizations as well as telecommunication standards across countries located within the European zones [71].
Health Information Trust Alliance (HITRUST) CSF [64]	HITRUST	Focus on security and privacy [64].
Consortium for IT Software Quality (CISQ) [73]	CISQ	Focus on risks and vulnerabilities in software applications [73].
Australian Signals Directorate (ASD) Essential 8 [69]	Australian Cyber Security Centre	Focus on helping organisations protect their systems against a range of adversaries [69].
10 steps to cybersecurity [70]	National Cyber Security Centre	A general focus on how organisations can protect themselves in cyberspace [70].
NZISM Protective Security Requirements (PSR) Framework [67]	New Zealand	Focus on minimum mandatory security standards for government departments and agencies [67].
New Zealand Privacy Act 2020 [72]	New Zealand	Focus on protecting individual privacy [72]
FedRAMP [74]	FedRAMP	Focus on security authorizations for Cloud Service Offerings. [74]
Security Content Automation Protocol (SCAP) [76]	OpenSCAP	Focus on automated configuration, vulnerability and patch checking, technical control compliance activities, and security measurement [76].
ETSI Standards [71] [83]	ETSI	Focus on different areas of telecommunication and cybersecurity including IoT-based Smart Environments (See Table 5 for details)

- **Protect**: Helps organisations develop and implement appropriate safeguards to ensure the delivery of critical services [37]. This phase also includes defining security controls for protecting data and information systems including access control, training and awareness, data security, information protection procedures, and maintaining protective technologies [31].
- **Detect**: Helps organisations develop and implement appropriate activities to identify the occurrence of a cybersecurity event [37] as well as offering guidelines for detecting anomalies in security, monitoring systems, and networks to uncover security incidences [36].
- **Response**: Helps organisations develop and implement appropriate activities to act regarding a detected cybersecurity incident [37]. This also includes recommendations for planning responses to security events, mitigation procedures, communication processes during a response, and activities for improving security resiliency [36].
- **Recovery**: Helps organisations develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident [37] as well as guidelines that a company can use to recover from attacks [36].

2) NIST RISK MANAGEMENT FRAMEWORK (RMF)

The Risk Management Framework (RMF) [38] provides a comprehensive, flexible, repeatable, and measurable 7-step process (prepare, categorize, select, implement, assess, authorize, and monitor) that any organization can use to manage information security and privacy risks.

- **Prepare**: Takes care of the essential activities to prepare an organization for managing security and privacy risks.
- **Categorize**: Helps an organisation to categorize the system and information processed, stored, and transmitted based on impact analysis.
- **Select**: Helps organisations select the set of NIST SP 800-53 [39] controls to protect the system based on risk assessment.
- **Implement**: Helps an organisation implement the controls and document how controls are deployed.
- **Assess**: Helps an organisation in assessment to determine if controls are in place, operating as intended, and producing the desired results.
- **Authorize**: This involves senior officials in an organisation making risk-based decisions to authorize the system (to operate).
- **Monitor**: Helps an organisation to continuously monitor control implementation and risks to the systems.

With the growing security and privacy concerns in IoT-based smart environments, this framework has the potential to be adapted for use in function-specific areas of IoT security and privacy risks management.

3) NIST PRIVACY FRAMEWORK

The NIST privacy framework was developed to help organizations identify and manage privacy risks as well as build innovative products and services while protecting individuals' privacy [40]. The core functions of the framework are as below:

- **Identify**: Help organisations develop an understanding of how to manage privacy risks for individuals arising from data processing.
- **Govern**: Help organisations develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.
- **Control**: Help organisations develop and implement appropriate activities to enable them or individuals to manage data with sufficient granularity to manage privacy risks.
- **Communicate**: Help organisations develop and implement appropriate activities to enable them as well as individuals to have a reliable understanding of how data are processed and associated privacy risks.
- **Protect**: Help organisations develop and implement appropriate data processing safeguards.

From this framework, the identify, control, and protect functions can help manage privacy issues in IoT-based smart environments.

4) NIST SP 800-53

This special publication on security matters provides security and privacy controls for information systems and organizations [39] to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of security threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks.

5) NIST SP 800-30

This special publication was developed to guide organisations in conducting information systems risk assessments [41].

6) NIST SP 800-37

The NIST SP 800-37 special publication describes and provides guidelines for applying the RMF to information systems and organizations [42].

7) NIST SP 800-39

This special publication was developed to guide an integrated, organization-wide program for managing information security risk to organizational operations (mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems [43].

8) NIST SP 800-12

NIST SP 800-12 [44] was primarily designed for federal and governmental agencies but can also be used by others focusing on control and computer security within an organization.

9) NIST SP 800-14

The NIST SP 800-14 [45] provides general descriptions of commonly used security principles to help organizations understand cybersecurity policies [36].

10) NIST SP 800-53R1

NIST SP 800-53R1 [46] was designed with a focus on protecting the confidentiality, integrity, and availability of the system and its information.

11) HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

HIPAA was developed to provide guidelines for enabling health plans, health care providers and health care clearinghouses to implement sufficient controls for securing employee or customer health information and protect sensitive patient health information from being disclosed without the patient's consent or knowledge [82]. With the growing number of wearable IoT medical devices, HIPAA can be adapted for use in IoT-based smart health systems.

12) FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA)

FERPA was developed to protect the privacy of student education records [47] and applies to all schools that receive funds under an applicable program of the U.S. Department of Education [47].

13) PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCI-DSS)

PCI DSS was designed to help protect the safety of card data [48] and defines a set of requirements intended to ensure that all organisations that process, store, or transmit credit card information maintain a secure environment [49] to reduce credit card fraud. With the increasing usage of near field communication, PCI-DSS can be enforced in IoT devices such as smartphones that are sometimes used for processing credit card information.

14) CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

Developed by the United States Department of Defence (DoD), CMMC is used to measure defence contractors' capabilities, readiness, and sophistication in cybersecurity [50]. The cybersecurity maturity model provides a framework or a pathway for organizations to periodically assess or measure the maturity of a security program and guidance on how to reach the next level [51].

15) CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)

Developed by the U.S. Department of Energy (DOE) C2M2 enables organizations to voluntarily measure the maturity levels of their cybersecurity capabilities consistently [52].

16) FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL (FFIEC) CYBERSECURITY ASSESSMENT TOOL

Like the CMMC and C2M2, the FFIEC Cybersecurity Assessment Tool (FFIEC-CAT) is meant to help organisations identify their cybersecurity risk level and determine the maturity of their cybersecurity programs. The assessment tool provides a repeatable and measurable process for financial institutions to measure their cybersecurity preparedness over time [53] as well as to measure risk levels across several categories, including delivery channels, connection types, external threats, and organizational characteristics [54].

17) NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION (NERC) 1300

Developed by NERC, this standard is meant to help organisations in reducing risks to the reliability of the bulk electric systems from any compromise of critical cyber assets [55].

18) NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION CRITICAL INFRASTRUCTURE PROTECTION (NERC-CIP)

The NERC-CIP standards were developed to provide specific guidance on cybersecurity for the North American power systems. A list of all the applicable standards is available at [56]. The increasing use of smart inverters and other IoT devices in electricity distribution companies can benefit from adapting both NERC 1300 and NERC-CIP standards

19) AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI)/INTERNATIONAL SOCIETY OF AUTOMATION (ISA) (ANSI/ISA 62443)

The ANSI together with the ISA developed ANSI/ISA 62443 which is part of the IEC 62443 international series of standards on industrial communication networks – information technology security for networks and systems. This standard defines processes, techniques and requirements for Industrial Automation and Control Systems (IACS) and includes secure product development lifecycle requirements meant to help in developing and maintaining secure products [57]. IoT device manufacturers can benefit from the use of ANSI/ISA 62443 in their product development lifecycle and help produce secure IoT products.

20) GENERAL DATA PROTECTION REGULATION (GDPR)

The GDPR was designed for the European Union and imposes data privacy and security obligations onto organizations anywhere, so long as they target or collect data related to people in the EU [58]. This may also be adapted to suit specific environments where IoT devices are used to collect and distribute data related to individuals.

21) SYSTEMS AND ORGANIZATIONS CONTROLS (SOC2)

Designed by the American Institute of CPAs (AICPA), SOC2 enable organizations that collect and store personal customer information using cloud services to maintain proper security as well as security requirements to which vendors and third parties must conform [36]. SOC2 reports are meant to protect the needs of users requiring detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems [59] which may also include IoT-based smart systems. Also, SOC2 provides Software-as-a-Service (SaaS) companies with guidelines and requirements for mitigating data breach risks and strengthening their cybersecurity postures [36].

22) THREAT ASSESSMENT AND REMEDIATION ANALYSIS (TARA)

TARA was developed as part of a MITRE portfolio of systems security engineering practices that contribute to the achievement of mission assurance for systems during the acquisition process [60]. TARA primarily focuses on identifying and assessing cyber vulnerabilities and selecting countermeasures effective at mitigating those vulnerabilities. The capabilities of TARA can easily be adapted for IoT-based smart environments to help in identifying and assessing cyber vulnerabilities.

23) OPERATIONALLY CRITICAL THREAT, ASSET, AND VULNERABILITY EVALUATION (OCTAVE)

OCTAVE was developed by the Software Engineering Institute at Carnegie Mellon University on behalf of the U.S Department of Defence to help in identifying and managing information security risks [61]. It is anchored on three basic aspects: build asset-based threat profiles, identify infrastructure vulnerabilities, and develop a security strategy and plans. OCTAVE defines a comprehensive evaluation method that helps an organization to identify the information assets that are important to the organization, the threats to those assets, and the vulnerabilities that may expose those assets to the threats. OCTAVE also helps organisations understand what information is at risk [61].

24) INFORMATION ASSURANCE FOR SMALL AND MEDIUM ENTERPRISES (IASME) GOVERNANCE

Developed by the IASME consortium, the IASME governance standard is used to accredit a business's cybersecurity posture [62]. The standard includes such areas as, risk assessment and management, monitoring, change management, training and managing people, backup, and incident response and business continuity. There were suggestions for the IASME consortium to deliver IoT certification to give confidence to consumers and businesses that IoT devices have attained a minimum accepted level of security [63].

25) HEALTH INFORMATION TRUST (HITRUST)

The HITRUST Alliance developed a framework that is a combination of the Department of Defense (DoD) Cybersecurity Maturity Model (CMMC) framework and the New York (NY) DOH Office of Health Insurance Programs. HITRUST-CSF primarily focuses on security and privacy issues in organisations [64].

26) CENTER FOR INTERNET SECURITY V7 (CIS V7)

Developed by the CIS, CIS v7 helps organisations to enhance their security standards [65] by listing actionable cybersecurity requirements for enhancing security standards in all organizations [36].

27) CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGIES (COBIT)

COBIT [66] was developed by the Information Systems Audit and Control Association (ISACA) and focuses on IT security, governance, and management in organizations that want to improve product quality and, at the same time, adhere to enhanced security best practices [36].

28) NZISM PROTECTIVE SECURITY REQUIREMENTS (PSR) FRAMEWORK

Developed by the New Zealand government the framework is part of the National Security Intelligence Service's Protective Security Requirements (PSR) and outlines the government's expectations for managing personnel, physical and information security including the baselines and minimum mandatory security standards for government departments and agencies [67].

29) COMMITTEE OF SPONSORING ORGANIZATIONS (COSO)

COSO of the Treadway commission is dedicated to developing frameworks and guidance on enterprise risk management, internal control, and fraud deterrence [68]. Among the frameworks developed under the COSO umbrella are:

- *Enterprise Risk Management - Integrated Framework*: This framework addresses the evolution of enterprise risk management and the need for organizations to improve their approach to managing risk as well as meet the demands of an evolving business environment [68].
- *Internal Control-Integrated Framework*: This framework helps organizations design and implement internal controls [68].

30) AUSTRALIAN SIGNALS DIRECTORATE (ASD) ESSENTIAL 8

Developed by ASD in collaboration with the Australia Cyber Security Centre (ACSC), the Essential 8 is meant to help organisations protect their systems against a range of adversaries [69].

31) 10 STEPS TO CYBERSECURITY

This is an initiative of the National Cyber Security Centre (NCSC) in the UK and provides 10 steps of general guidance on how organisations can protect themselves in cyberspace [70].

32) TECHNICAL COMMITTEE ON CYBER SECURITY (TC CYBER) FRAMEWORK

TC CYBER developed a framework [71] that recommends a set of requirements for improving privacy awareness for individuals or organizations as well as improving the telecommunication standards across countries located within the European zones [36]. TC CYBER initiatives are split across 9 key areas where standardization can help bring better security [71] which are understanding the cybersecurity ecosystem, protection of personal data and communication, consumer IoT security and privacy, cybersecurity for critical national infrastructures, network security, cybersecurity tools and guides, direct support to EU legislation, and quantum-safe cryptography.

33) NEW ZEALAND PRIVACY ACT 2020

Developed by the parliamentary counsel office in New Zealand the Privacy Act 2020 promote and protect individual privacy [72].

34) CONSORTIUM FOR IT SOFTWARE QUALITY (CISQ)

CISQ develops security standards meant for developers to maintain when developing software applications [73] as well as assess the risks and vulnerabilities present in completed software applications or those under development. Developers use the CISQ standards to measure the size and quality of their software programs [36].

35) FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM (FedRAMP)

FedRAMP developed a framework to provide a standardized approach to security authorizations for cloud service offerings [74]. The framework can enable government agencies to evaluate cyber threats and risks to different infrastructure platforms, cloud-based services, and software solutions [36].

36) FEDERAL INFORMATION SECURITY MODERNIZATION ACT (FISMA)

Developed by the Cybersecurity and Infrastructure Security Agency (CISA), FISMA [75] is aimed at helping federal agencies implement adequate measures to protect critical information systems from different types of attacks as well as help them develop and maintain highly effective cybersecurity programs [36].

37) SECURITY CONTENT AUTOMATION PROTOCOL (SCAP)

OpenSCAP developed the SCAP standard with a focus on automated configuration, vulnerability and patch checking, technical control compliance activities, and security measurement [76]. SCAP aims to standardize the processes through which security software programs communicate security issues, configuration information, and vulnerabilities [36].

38) ETSI STANDARDS

The European Telecommunications Standards Institute (ETSI) is a nonprofit organisation dedicated to producing telecommunications standards that can be used throughout Europe.[1] However, ETSI also develops standards for different areas of cybersecurity and the Internet of Things (IoT). Because of the vast number of standards developed by ETSI, in this section, we sample some of those that focus on addressing some components of cybersecurity and the Internet of Things (IoT). For a comprehensive list of all the ETSI standards, the reader is advised to consult [71] and [82]. To be in line with the objectives of this study, Table 5 summarizes sampled ETSI standards and their primary focus areas either touching on cybersecurity or the IoT-based smart environments like smart cities, smart grids, smart metering, smart body area networks and Smart Cards.

TABLE 5. Summary of ETSI standards.

Name of Standard	Primary Focus Areas
1. ETSI GS OEU 019 V1.1.1 (2017-08)	
2. ETSI TR 103 506 V1.1.1 (2018-09)	Focus on Smart Cities
3. ETSI TR 103 455 V1.1.1 (2020-09)	
4. ETSI TS 103 410-4 V1.1.2 (2020-05)	
5. ETSI TR 103 290 V1.1.1 (2015-04)	
6. ETSI TS 103 735 V1.1.2 (2021-07)	
7. ETSI TR 103 546 V1.1.1 (2020-04)	Smart Grids
8. ETSI TR 103 411 V1.1.1 (2017-02)	
9. ETSI TS 103 267 V2.1.1 (2020-02)	
10. ETSI TS 103 425 V1.1.1 (2016-11)	
11. ETSI TS 104 001 V2.2.1 (2019-01)	Smart Metering
12. ETSI TR 102 691 V1.1.1 (2010-05)	
13. ETSI TR 103 751 V1.1.1 (2021-04)	
14. ETSI TR 103 711 V1.1.1 (2020-10)	Smart Body Area Networks
15. ETSI TR 103 395 V1.1.2 (2021-06)	
16. ETSI TR 103 394 V1.1.1 (2018-01)	
17. ETSI TS 103 326 V1.2.1 (2021-07)	
18. ETSI TS 103 465 V16.5.0 (2021-08)	
19. ETSI TR 103 380 V1.0.0 (2015-11)	Smart Cards
20. ETSI TS 102 922-1 V7.3.0 (2021-02)	
21. ETSI TS 102 705 V16.0.0 (2021-02)	
22. ETSI TS 102 695-3 V13.0.0 (2019-04)	
23. ETSI GS ISI 008 V1.1.1 (2018-06)	
24. ETSI TS 103 816-5 V1.1.1 (2021-07)	Other Areas of Cybersecurity
25. ETSI TR 103 787-1 V1.1.1 (2021-05)	
26. ETSI TS 103 643 V1.1.1 (2020-01)	
27. ETSI TR 103 370 V1.1.1 (2019-01)	
28. ETSI GS NGP 005 V1.1.1 (2017-04)	
29. ETSI GS LTN 003 V1.1.1 (2014-09)	Other Areas of Internet of Things (IoT)
30. ETSI GR IP6 008 V1.1.1 (2017-06)	
31. ETSI GS CIM 016 V1.1.1 (2021-04)	
32. ETSI TR 118 551 V2.0.0 (2020-11)	

The next section presents a summary of the ISO/IEC 27000 Series of standards on information technology security techniques identified to support this study and shown in Table 6.

B. INTERNATIONAL STANDARDS ORGANISATION (ISO) 27000 SERIES

Developed jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) the ISO/IEC 27000-series of standards shown in Table 6 is a collection of published standards as well as others under development (as at the time of this study) related to information technology, security techniques, privacy, incidence response and risk management that can be used across a wide range of types and sizes of business organisations.

The summary presented in Table 6 shows different standards in the ISO/IEC 27000 family in tandem with their primary focus areas [77]. Note that of all the 80 ISO/IEC 27000 series of standards identified in this study only 8 which is 10% of all the standards have a direct focus on IoT security and privacy with 5 published and *3* under development at the time of this study.

As is evident from Table 6, the ISO/IEC 27000-series of standards are broad in scope and cover a variety of areas including privacy, confidentiality, integrity, availability, technical information technology and other cybersecurity areas. However, a good number of the standards also cover information technology and security techniques. All the 80 ISO/IEC 27000-series standards listed in Table 6 apply to organizations of all sizes especially in assessing and mitigating cyber security and information risks. It is also important to note at this point that the ISO/IEC 27000-series of standards are continuously updated to be in line with the dynamic nature of cybersecurity as well as the ever-changing security threats, vulnerabilities and other impacts of cyber security incidents. For a compressive discussion of the individual standards listed in Table 6, the reader can consult [77]. Discussing and evaluating individual standards is outside the scope of this study, however, future research may consider individual discussions and evaluations of specific standards identified.

Table 6 at this point again justifies the need to develop new standards and assessment frameworks focusing on IoT-based smart environments as only 10% of the listed standards have a direct focus on IoT security and privacy. This is because most of the security standards and assessment frameworks identified in this paper were not designed to directly address the security needs of IoT-based smart environments. This is arguable because of the dynamic nature of digital technology. For this reason, new security standards and assessment frameworks will need to be developed to specifically address the security needs of IoT-based smart environments. The next section briefly explains open problems and challenges related to IoT-based smart environments security issues.

VI. OPEN PROBLEMS AND CHALLENGES FOR IoT-BASED SMART ENVIRONMENTS

This section provides a brief description of open problems and challenges related to IoT-based smart environments security concerns. However, the problems and challenges can also be considered as potential areas for future research directions. Some of the open problems and challenges identified are briefly discussed below.

[1] https://www.etsi.org/standards

TABLE 6. Summary of existing security standards.

Name of Standard	Primary Focus Areas
1. ISO/IEC 27000: 2018	Information Security Management Systems - Overview and Vocabulary
2. ISO/IEC 27001:2013	Information Security Management Systems-Requirements.
3. ISO/IEC 27002: 2013	Code of Practice for Information Security Controls
4. ISO/IEC 27003:2017	Information Security Management Systems - Guidance
5. ISO/IEC 27004:2016	Information Security Management - Monitoring, Measurement, Analysis and Evaluation
6. ISO/IEC 27005:2018	Information Security Risk Management
7. ISO/IEC CD 27005.2	Guidance on Managing Information Security Risks and Opportunities [Under Development]
8. ISO/IEC 27006:2015	Requirements for Bodies Providing Audit and Certification of Information Security Management Systems
9. ISO/IEC 27007:2020	Guidelines for Information Security Management Systems Auditing
10. ISO/IEC TS 27008:2019	Guidelines for the Assessment of Information Security Controls
11. ISO/IEC 27009:2020	Cybersecurity and Privacy Protection - Sector-Specific Application of ISO/IEC 27001 - Requirements
12. ISO/IEC 27010:2015	Information Security Management for Inter-Sector and Inter-organizational Communications
13. ISO/IEC 27011:2016	Code of Practice for Information Security Controls Based on ISO/IEC 27002 For Telecommunications Organizations
14. ISO/IEC 27013:2015	Guidance on the Integrated Implementation of ISO/IEC 27001 And ISO/IEC 20000-1
15. ISO/IEC DIS 27013	Guidance on the Integrated Implementation of ISO/IEC 27001 and ISO/IEC 20000-1 [Under Development]
16. ISO/IEC 27014:2020	Governance of Information Security
17. ISO/IEC TR 27016 :2014	Information Security Management - Organizational Economics
18. ISO/IEC 27017:2015	Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services
19. ISO/IEC 27018:2019	Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors.
20. ISO/IEC 27019:2017	Information Security Controls for the Energy Utility Industry
21. ISO/IEC 27021:2017	Competence Requirements for Information Security Management Systems Professionals
22. ISO/IEC TS 27022:2021	Guidance on Information Security Management System Processes
23. ISO/IEC 27031:2011	Guidelines for Information and Communication Technology Readiness for Business Continuity
24. ISO/IEC WD 27031	Information and Communication Technology Readiness for Business Continuity [Under Development]
25. ISO/IEC 27032:2012	Guidelines for Cybersecurity
26. ISO/IEC CD 27032	Guidelines for Internet Security [Under Development]
27. ISO/IEC 27033-1:2015	Network Security - Part 1: Overview and Concepts
28. ISO/IEC 27033-2:2012	Network Security - Part 2: Guidelines for the Design and Implementation of Network Security
29. ISO/IEC 27033-3:2010	Network Security - Part 3: Reference Networking Scenarios - Threats, Design Techniques and Control Issues
30. ISO/IEC 27033-4:2014	Network Security - Part 4: Securing Communications between Networks Using Security Gateways
31. ISO/IEC 27033-5:2013	Network Security - Part 5: Securing communications across Networks Using Virtual Private Networks (VPNs)
32. ISO/IEC 27033-6:2016	Network Security - Part 6: Securing Wireless IP Network Access
33. ISO/IEC WD 27033-7.2	Network Security - Part 7: Guidelines for Network Virtualization Security [Under Development]
34. ISO/IEC 27034-1:2011	Application Security - Part 1: Overview and Concepts
35. ISO/IEC 27034-2:2015	Application Security - Part 2: Organization Normative Framework
36. ISO/IEC 27034-3:2018	Application Security - Part 3: Application Security Management Process
37. ISO/IEC 27034-4	Application security — Part 4: Validation and Verification (No Longer Available)
38. ISO/IEC 27034-5:2017	Application Security - Part 5: Protocols and Application Security Controls Data Structure
39. ISO/IEC 27034-5-1:2018	Application Security - Part 5-1: Protocols and Application Security Controls Data Structure, XML Schemas
40. ISO/IEC 27034-6:2016	Application Security - Part 6: Case Studies
41. ISO/IEC 27034-7:2018	Application Security - Part 7: Assurance Prediction Framework
42. ISO/IEC 27035-1:2016	Information Security Incident Management - Part 1: Principles of Incident Management
43. ISO/IEC CD 27035-1	Information Security Incident Management - Part 1: Principles and Process [Under Development]
44. ISO/IEC 27035-2:2016	Information Security Incident Management - Part 2: Guidelines to Plan and Prepare for Incident Response
45. ISO/IEC CD 27035-2	Information Security Incident Management - Part 2: Guidelines to Plan and Prepare for Incident Management [Under Development]
46. ISO/IEC 27035-3:2020	Information Security Incident Management - Part 3: Guidelines for ICT Incident Response Operations
47. ISO/IEC WD 27035-4	Information Security Incident Management - Part 4: Coordination [Under Development]
48. ISO/IEC 27036-1:2014	Information Security for Supplier Relationships - Part 1: Overview and Concepts
49. ISO/IEC 27036-2:2014	Information Security for Supplier Relationships - Part 2: Requirements
50. ISO/IEC 27036-3:2013	Information Security for Supplier Relationships - Part 3: Guidelines for Information and Communication Technology Supply Chain Security
51. ISO/IEC 27036-4:2016	Information Security for Supplier Relationships - Part 4: Guidelines for Security of Cloud Services
52. ISO/IEC 27037:2012	Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence
53. ISO/IEC 27038:2014	Specification for Digital Redaction
54. ISO/IEC 27039:2015	Selection, Deployment and Operations of Intrusion Detection and Prevention Systems (IDPS)

A. LACK OF STANDARDIZATION

The lack of standardized approaches that can scale beyond conventional network requirements into IoT-based smart environments presents a major challenge in developing and implementing IoT security control measures. Researchers and other stakeholders should consider developing new

TABLE 6. ***(Continued.)* Summary of existing security standards.**

55.	ISO/IEC 27040:2015	Storage Security
56.	ISO/IEC WD 27040.2	Storage Security [Under Development]
57.	ISO/IEC 27041:2015	Guidance On Assuring Suitability and Adequacy of Incident Investigative Method
58.	ISO/IEC 27042:2015	Guidelines for the Analysis and Interpretation of Digital Evidence
59.	ISO/IEC 27043:2015	Incident Investigation Principles and Processes
60.	ISO/IEC WD 27045.6	Big Data Security and Privacy - Processes [Under Development]
61.	ISO/IEC WD 27046.4	Big Data Security and Privacy - Implementation Guidelines [Under Development]
62.	ISO/IEC 27050-1:2019	Electronic SAFIoTy - Part 1: Overview and Concepts
63.	ISO/IEC 27050-2:2018	Electronic SAFIoTy - Part 2: Guidance for Governance and Management of Electronic SAFIoTy
64.	ISO/IEC 27050-3:2020	Electronic SAFIoTy - Part 3: Code of Practice for Electronic SAFIoTy
65.	ISO/IEC 27050-4:2021	Electronic SAFIoTy - Part 4: Technical Readiness
66.	ISO/IEC DIS 27070	Requirements for Establishing Virtualized Roots of Trust [Under Development]
67.	ISO/IEC WD 27071.4	Security Recommendations for Establishing Trusted Connections Between Devices and Services [Under Development]
68.	ISO/IEC CD 27099.3	Public Key Infrastructure - Practices and Policy Framework [Under Development]
69.	ISO/IEC 27102:2019	Information Security Management - Guidelines for Cyber-Insurance
70.	ISO/IEC TS27100:2020	Cybersecurity - Overview and Concepts
71.	ISO/IEC TS27110:2021	Cybersecurity Framework Development Guidelines
72.	ISO/IEC CD 27402	Cybersecurity - IoT Security and Privacy - Device Baseline Requirements [Under Development]
73.	ISO/IEC WD 27403.4	Cybersecurity – IoT Security and Privacy – Guidelines for IoT-Domotics [Under Development]
74.	ISO/IEC CD 27400.3	Cybersecurity – IoT Security and Privacy – Guidelines [Under Development]
75.	ISO/IEC TS27570:2021	Privacy Protection - Privacy Guidelines for Smart Cities
76.	ISO/IEC CD 27553	Security Requirements for Authentication Using Biometrics on Mobile Devices [Under Development]
77.	ISO/IEC WD 27557.2	Organizational Privacy Risk Management [Under Development]
78.	ISO/IEC 27701:2019	Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management - Requirements and Guidelines
79.	ISO 27789:2013	Health Informatics - Audit Trails for Electronic Health Records
80.	ISO 27799:2016	Health Informatics - Information Security Management in Health Using ISO/IEC 27002

security standards and assessment frameworks to address both current and future IoT security concerns.

B. TECHNOLOGY EVOLUTION

Technology evolution makes IoT devices function smoothly as standalone systems or part of existing solutions to improve the life and quality of IoT devices users. However, many manufactures of IoT devices do not incorporate security designs and make use of different protocols and technologies that create complex configurations in IoT-based smart environments. Standards and assessment frameworks needed to be developed to streamline the way different IoT technologies are designed, manufactured, and implemented.

C. SECURITY AND PRIVACY

Security and privacy are inherent challenges to many IoT application domains. The hacking of IoT devices is causing serious security and privacy challenges that have the potential to drag into the unforeseeable future of IoT. With new IoT devices being manufactured daily and added into existing networks, their connectivity to the internet provides malicious actors with an entry point to smart environments where they can carry out their malicious activities, especially since many of the IoT devices suffer from known security loopholes. Poor security and privacy can expose people's lives as well as their health to malicious individuals through hack attacks.

D. CONNECTIVITY

With new IoT devices entering the market daily, connectivity issues are becoming a challenge as well. New communication models, protocols and technologies need to be developed to support the tens, hundreds and thousands of new devices being connected to the internet daily.

E. LAW ENFORCEMENT AND REGULATIONS

Being relatively a new technology, the Internet of things presents legal issues in different jurisdictions with regards to applicable laws and regulations. For a detailed account [78] and [79] present in their research, some of the legal and ethical issues associated with IoT smart environments.

F. OTHER IoT CHALLENGES

Other challenges found in the literature include compatibility, interoperability, scalability, intelligent analysis and actions, reliability, management of IoT network and its resources, data confidentiality and visualization [80]. As a new contribution, the next section presents the proposed taxonomy that classifies the different challenges related to IoT smart environments and their proposed potential solutions.

VII. TAXONOMY OF CHALLENGES FOR IoT-BASED SMART ENVIRONMENT AND PROPOSED POTENTIAL SOLUTIONS

In this section, we present a taxonomy of challenges for IoT-based smart environments in tandem with proposed potential solutions. Figure 3 shows a high-level overview of the different IoT-based smart environment challenges discussed in this section.

A. SCOPE OF THE PROPOSED TAXONOMY

Fundamentally, the taxonomy in this section has been drawn from the examined literature in this paper. The taxonomy was

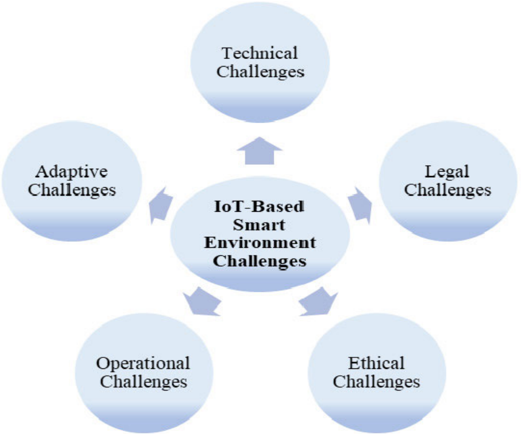

FIGURE 3. IoT-based smart environment challenges.

necessitated by the existence of key security and privacy challenges in IoT-based smart environments. Logically, while the key considerations could be inclined on the security of data, devices and key technologies being utilized, our study was inclined to the relevant considerations (methods/techniques) in IoT-based smart environments that are centred on handling security and privacy as well as how the data that is generated in these environments are managed securely. These insights have been considered while combing through the existing security standards and assessment frameworks. Furthermore, they formed a foundation that has enabled effective and systematic exploration of security standards and assessment frameworks which in the long run have also been used to define the scope of the taxonomy as well as a baseline for identifying open problems and challenges that are relative to IoT-based smart environment.

With many known challenges in IoT-based smart environments, attempts have been made to address specific challenges by different stakeholders. The contribution in this paper is, however, an exceptional effort in the direction of a taxonomy of challenges for IoT-based smart environments based on the examined literature in this paper. The scope of the taxonomy is, thus, restricted to the literature reviewed by the authors in this study. It is also important to note that, the various challenges identified and discussed in this paper are not, in whatever way an exhaustive list, however, the taxonomy was created taking into consideration the major challenges associated with IoT-based smart environments as shown in Figure 3. The next section explains the proposed taxonomy in this study.

B. PROPOSED TAXONOMY OF CHALLENGES FOR IoT-BASED SMART ENVIRONMENT

The proposed taxonomy is an extended version of the different categories of challenges shown in Figure 3. Table 7 shows the details of the different challenges drawn from the reviewed literature in this paper. The taxonomy consists of five different categories of challenges arranged from top to bottom with the first one being the technical challenges. This is followed by the legal challenges, ethical challenges, operational challenges, and finally the adaptive challenges.

The sub-sections to follow briefly explains the various categories of the IoT-based smart environment challenges shown in Table 7. However, it is also important to note at this point that, the various sub-categories of the challenges shown in the second column of Table 7 focus more on specific challenges associated with each category. To simplify the understanding as well as present specific finer details of the proposed taxonomy, the authors organized the taxonomy into categories and sub-categories as shown in Table 7. Besides, when developing specialized IoT security tools that focus on addressing the individual but specific IoT challenges, the sub-categories can be useful. Also, note that most of the sub-categories of the challenges shown in Table 7 were only selected as common examples to facilitate this study and do not in any way represent an exhaustive list. To improve on the list of the specific sub-categories of the challenges to each named category, more research still needs to be done.

1) TECHNICAL CHALLENGES

In this paper, we view technical challenges as those that can be addressed using existing knowledge, expertise, and resources. They are easy to identify, define and their solution are based on known experts' knowledge and skills. Implementing the solutions to any of the identified technical challenges often falls to someone with the knowledge, expertise, and authority to do so. Examples of technical challenges faced by IoT-based smart environments identified for this study are shown in column two of Table 7.

2) LEGAL CHALLENGES

Legal challenges are related to legal specifics and may include both civil and criminal aspects. Several legal challenges affect IoT-based smart environments. Stakeholders note with concern, for example, how service providers use, store and secure users' personal information. Users and manufacturers of IoT devices, therefore, need to be aware of the legal challenges highlighted in Table 7, their complications and also understand that there are no concrete answers to them yet.

3) ETHICAL CHALLENGES

Many ethical challenges may arise from deploying IoT devices and services. Ethical challenges present people with tough choices of what is good or bad, what is acceptable or not acceptable among other choices. Usually, ethical challenges are hard to resolve in a manner that is consistent with accepted ethical guidelines. This is because they present difficult situations, especially when one must choose between two or more options yet neither of their choices resolves the situation ethically. Table 7 lists some of the examples of ethical challenges identified for this study.

TABLE 7. Taxonomy of challenge for IoT-based smart environment and their proposed potential solutions.

Categories of IoT-based Smart Environments Challenges	Sub-Categories	Proposed Potential Solutions
1. Technical Challenges	• Dynamic Technology • Hardware Miniaturization • Software Upgrades or Patches • Architecture • Compatibility and Longevity • Bandwidth • Energy Efficiency • Continuity/Low Power and Constrained Resources • Implementation Cost • Vulnerability of IoT Devices • Fragmentation • Active Device Monitoring • Insufficient IoT Device Testing and Updates • Hacking • Fixed firmware • Failures or Malfunctions	See Section C: i, ii, iii, iv, v, vi, vii, viii, ix, x, and xi
2. Legal Challenges	• Security • Privacy • Accountability • Impersonation • User profiling • Law Enforcement Regulations • IoT Globalization • Prosecution of Intruders • Regulation and Compliance • Determining Liability of IoT Devices • Actual Owners of IoT Devices • Discrimination • Surveillance • Consent • Identity Theft • Legal Ownership of Data • Government Access to IoT Data • Deleting Personal Data • Home invasions and Trespass • Tracking and Location Privacy • Context-Aware or Situational Privacy • Sensed, Generated or Collected Data Privacy • User Privacy Information Mining • Unauthorized access or Deletion or Modification of Data	See Section C: ii, iii, iv, v, vi, vii, viii, ix, and xi
3. Ethical Challenges	• Privacy • Eavesdropping • User Identification • Data and Information Access • Data and Information Integrity • Attacks on Devices • Collection, Use and Disclosure of IoT data • De-identification of IoT data • Discrimination and Equality on the use of IoT Services • Responsibility • Transparency • Falsification • Evading Detection • Trust • Malicious Use of IoT Devices and Services • IoT Device Hijacking, malware, and Ransomware	See Section C: iii, v, vi, vii, viii, ix, and xi
4. Operational Challenges	• Standardization (Ambiguous Security Standards) • IoT Device Security • Attack Prediction and Prevention • Efficient and Robust Security Protocols • Denial of Service (DoS/DDoS) • Management and Governance • Weak passwords • Technology Minded and Security aware Users • Software Exploitation • Vagueness • Business Models, Policies and Procedures • Connectivity/Network Performance Monitoring • Scalability • Self-Organization • Data Collection, Storage, Processing and Usage • Availability • Reliability • Transparency • Interoperability • Operations Sustainability • Control • Insufficient Testing and Updating • Coexistence in a Crowded Environment • Big Data Issues • Data and Information Leakage • Data Synchronization Between IoT Devices • Cyber Risks • Resource Consumption • Resource constraints • Cloud computing	See Section C: i, ii, iii, iv, v, vi, vii, viii, ix, x, and xi
5. Adaptive Challenges	• User Expectations • Education and Training • Dependency on Vendors • Cultural Shift • Health and Safety of Users • Deploying IoT Devices and Services • Rolling out New or Upgraded IoT Devices or Services • Taking Responsibility for Device or Service Failures • Predicting and Preventing Attacks • Disasters and Outages • Dynamic Characteristics	See Section C: iii, v, vi, vii, viii, ix, x, and xi

TABLE 7. ***(Continued.)*** **Taxonomy of challenge for IoT-based smart environment and their proposed potential solutions.**

4) OPERATIONAL CHALLENGES

With the growing number of IoT devices and their deployment in different smart environments, operational challenges are bound to occur. In an environment where IoT devices and services are deployed, operational challenges are those that could create waste, drain resources, impact operational performance, render a business less profitable and hinder growth. Different categories of operational challenges have been identified as examples to support this study and are shown in Table 7.

5) ADAPTIVE CHALLENGES

Unlike technical challenges, adaptive challenges as shown in Table 7 are difficult to identify. These type of challenges presents people with situations that have no known solutions [81]. In some cases, there may be too many solutions for a single adaptive challenge with no clear choice as well. Adaptive challenges are by nature, adaptive. This implies that they are complex, ambiguous unpredictable, volatile, fluid and change with circumstances [81]. Resolving adaptive challenges sometimes require people to learn new ways of doing things, change their attitudes, values and norms and adopt experimental mindsets [81].

Based on the general description of the challenges identified in this study and the small space in column three of Table 7, the proposed potential solutions for each category are listed separately in the next section and numbers i to xi. Note also that some of the proposed solutions apply to more than one category of the challenges as captured in column three of Table 7.

C. PROPOSED POTENTIAL SOLUTIONS TO THE IDENTIFIED CHALLENGES

IoT devices are becoming important components in deploying different types of services in smart environments. To overcome the different challenges described in this paper, this section presents proposed potential solutions that can help protect IoT-based smart environments and ensure services continuity and stability in future deployments. The proposed solutions include:

i. Developing security assessment frameworks for IoT-based smart environments to secure the IoT network.
ii. Developing IoT device-specific monitoring tools.
iii. Implementing secure authentications for all IoT devices.
iv. Encrypting IoT data moving in and out of IoT-based networks (Encrypted communication).
v. Testing all IoT hardware before, during and after deployment (Testing IoT hardware).
vi. Use public key infrastructure security methods for IoT devices and smart environments.
vii. Developing and deploying only secure and trusted IoT applications.
viii. Implementing identity management.
ix. Trust establishment for secure data transmission and object authentication.
x. Hardening the security of the IoT networks including the use of strong login credentials.
xi. Regulating and certifying IoT devices before use to avoid launching IoT devices in a rush.

Note that every IoT device introduced into any network can be vulnerable to a variety of cyberattacks. The proposed solution identified above can help prevent potential future attacks in IoT-based smart environments. However, other IoT security solutions that can also be beneficial include the use of:

- IoT security analytics,
- End-to-end credentials
- IoT API security methods,
- Endpoint detection and response (EDR) tools
- Dedicated network visibility tools and finally
- Keeping up to date with the latest IoT security threats and breaches

VIII. CONCLUSION AND FUTURE WORK

Knowing that the security standards and assessment frameworks that can be deployed in IoT-based smart environments are quite different from those that can be used in non-IoT domains, the need for effective security standards and assessment frameworks for IoT-based smart environments is now inevitable. This is backed up by the fact that IoT-based smart environment security is dependent on a wide range of security checks which many existing security standards and assessment frameworks discussed in this study may not directly address. Besides, the security of IoT-based smart environments is determined by the installations and configurations made largely by sometimes untrained individuals. A combination of all these challenges makes the security of IoT-based smart environments much more difficult to develop, implement, enforce, and maintain. To address these challenges, this paper reviewed 80 ISO/IEC security standards, 32 ETSI standards and 37 different conventional security frameworks which included 7 NIST special publications on security techniques. The review process revealed the lack of security standards and assessment frameworks that directly addressed the security requirements and needs of IoT-based smart environments.

As a new contribution, this paper proposed a taxonomy that classifies the different challenges related to IoT-based smart environments into a few well defined and easily understood categories drawn from the literature examined by the authors in this study. The taxonomy also included proposed potential solutions to the identified challenges. Such a taxonomy can help researchers and other stakeholders identify and formulate future research directions related to the security and privacy issues of IoT-based smart environments. As part of the future work, the authors plan to developed and test an IoT-based smart environment security assessment framework in a simulated smart environment and assess its effectiveness and efficiency based on some of the challenges identified in this study. In addition, it is the authors view that in future research we will explore how the current taxonomy would translate and fit in other environments given the changing and dynamic nature of the IoT-based ecosystems. However, more research still needs to be done to improve on the work conducted in this study as well as spark further discussions into the development of new security standards and assessment frameworks for IoT-based smart environments.

REFERENCES

[1] H. Lin and N. W. Bergmann, "IoT privacy and security challenges for smart home environments," *Information*, vol. 7, no. 3, p. 44, 2016.

[2] N. M. Karie, N. M. Sahri, and P. Haskell-Dowland, "IoT threat detection advances, challenges and future directions," in *Proc. IEEE Workshop Emerg. Technol. Secur. IoT (ETSecIoT)*, Sydney, NSW, Australia, Apr. 2020, pp. 22–29.

[3] L. Cédric, D. Eleni, T. Guillaume, D. Guillaume, and A. Mouhannad. (Dec. 2015). *Security and Resilience of Smart Home Environments. Good Practices and Recommendations*. Accessed: Mar. 30, 2021. [Online]. Available: https://www.enisa.europa.eu/publications/security-resilience-good-practices/at_download/fullReport

[4] V. R. Kebande, N. M. Karie, and H. S. Venter, "Adding digital forensic readiness as a security component to the IoT domain," *Int. J. Adv. Sci., Eng. Inf. Technol.*, vol. 8, no. 1, pp. 1–11, 2018.

[5] W. M. S. Stout and V. E. Urias, "Challenges to securing the Internet of Things," in *Proc. IEEE Int. Carnahan Conf. Secur. Technol. (ICCST)*, Orlando, FL, USA, Oct. 2016, pp. 1–8, doi: 10.1109/CCST.2016.7815675.

[6] Z. A. Solangi, Y. A. Solangi, S. Chandio, M. B. S. A. Aziz, M. S. B. Hamzah, and A. Shah, "The future of data privacy and security concerns in Internet of Things," in *Proc. IEEE Int. Conf. Innov. Res. Develop. (ICIRD)*, Bangkok, Thailand, May 2018, pp. 1–4, doi: 10.1109/ICIRD.2018.8376320.

[7] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, and G. Baldini, "Security and privacy issues for an IoT based smart home," in *Proc. 40th Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO)*, Opatija, Croatia, May 2017, pp. 1292–1297, doi: 10.23919/MIPRO.2017.7973622.

[8] W. Ali, G. Dustgeer, M. Awais, and M. A. Shah, "IoT based smart home: Security challenges, security requirements and solutions," in *Proc. 23rd Int. Conf. Autom. Comput. (ICAC)*, Huddersfield, U.K., Sep. 2017, pp. 1–6, doi: 10.23919/IConAC.2017.8082057.

[9] V. R. Kebande, J. Bugeja, and J. A. Persson, "Internet of threats introspection in dynamic intelligent virtual sensing," in *Proc. 1st Workshop Cyber-Phys. Social Syst. (CPSS)*, Bilbao, Spain, 2020, pp. 1–8.

[10] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: Challenges and solutions," *Appl. Sci.*, vol. 10, no. 12, p. 4102, Jun. 2020.

[11] M. A. Razzaq, S. H. Gill, M. A. Qureshi, and S. Ullah, "Security issues in the Internet of Things (IoT): A comprehensive study," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 6, p. 383, 2017.

[12] V. R. Kebande and I. Ray, "A generic digital forensic investigation framework for Internet of Things (IoT)," in *Proc. IEEE 4th Int. Conf. Future Internet Things Cloud (FiCloud)*, Vienna, Austria, Aug. 2016, pp. 356–362.

[13] A. Jurcut, T. Niculcea, P. Ranaweera, and N.-A. Le-Khac, "Security considerations for Internet of Things: A survey," *Social Netw. Comput. Sci.*, vol. 1, no. 4, pp. 1–19, Jul. 2020.

[14] H. M. T. Gadiyar, G. S. Thyagaraju, and T. P. Bhavya, "Privacy and security issues in IoT based smart home applications," *Int. J. Eng. Res. Technol.*, vol. 6, no. 15, pp. 1–3, 2018.

[15] D. J. MacInnis, V. M. Patrick, and C. W. Park, "Looking through the crystal ball," in *Review of Marketing Research*, vol. 2. Bingley, U.K.: Emerald Group Publishing, 2006, pp. 43–80.

[16] S. Nagarkar and V. Prasad, "Evaluating privacy and security threats in IoT-based smart home environment," *Int. J. Appl. Eng. Res.*, vol. 14, no. 7, pp. 1–4, 2019.

[17] J. Bugeja, A. Jacobsson, and P. Davidsson, "On privacy and security challenges in smart connected homes," in *Proc. IEEE Eur. Intell. Secur. Informat. Conf. (EISIC)*, Uppsala, Sweden, Aug. 2016, pp. 172–175.

[18] M. Seliem, K. Elgazzar, and K. Khalil, "Towards privacy preserving IoT environments: A survey," *Wireless Commun. Mobile Comput.*, vol. 2018, p. 15, Nov. 2018, doi: 10.1155/2018/1032761.

[19] F. Hall, L. Maglaras, T. Aivaliotis, L. Xagoraris, and I. Kantzavelou, "Smart homes: Security challenges and privacy concerns," 2020, *arXiv:2010.15394*. [Online]. Available: http://arxiv.org/abs/2010.15394

[20] A. Cook, M. Robinson, M. A. Ferrag, L. A. Maglaras, Y. He, K. Jones, and H. Janicke, "Internet of cloud: Security and privacy issues," in *Cloud Computing for Optimization: Foundations, Applications, and Challenges*. Cham, Switzerland: Springer, 2018, pp. 271–301.

[21] E. Chris. (Oct. 18, 2018). *Internet of Things Challenges in Storage and Data*. Accessed: Mar. 31, 2021. [Online]. Available: https://www.computerweekly.com/news/252450705/Internet-of-things-challenges-in-storage-and-data

[22] M.-C. Lee, J.-C. Lin, and O. Owe, "Privacy mining from IoT-based smart homes," in *Proc. Int. Conf. Broadband Wireless Comput., Commun. Appl. (BWCCA)*, 2018, pp. 304–315, doi: 10.1007/978-3-030-02613-4_27.

[23] OVIC. (Feb. 2020). *The Internet of Things and Privacy*. Accessed: Mar. 31, 2021. [Online]. Available: https://ovic.vic.gov.au/wp-content/uploads/2020/02/Internet-of-Things-and-privacy-issues-paper-2.pdf

[24] Taryudi, D. B. Adriano, and W. A. C. Budi, "IoT-based integrated home security and monitoring system," *J. Phys., Conf. Ser.*, vol. 1140, no. 1, Dec. 2018, Art. no. 012006.

[25] Z. Han, X. Li, K. Huang, and Z. Feng, "A software defined network-based security assessment framework for CloudIoT," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1424–1434, Jun. 2018, doi: 10.1109/JIOT.2018.2801944.

[26] L. Wang, Y. Ali, S. Nazir, and M. Niazi, "ISA evaluation framework for security of internet of health things system using AHP-TOPSIS methods," *IEEE Access*, vol. 8, pp. 152316–152332, 2020, doi: 10.1109/ACCESS.2020.3017221.

[27] A. Hinduja and M. Pandey, "An ANP-GRA-based evaluation model for security features of IoT systems," in *Intelligent Communication, Control and Devices* (Advances in Intelligent Systems and Computing), vol. 989, S. Choudhury, R. Mishra, R. Mishra, and A. Kumar, Eds. Singapore: Springer, 2020, doi: 10.1007/978-981-13-8618-3_26.

[28] S. Pirbhulal, N. Pombo, V. Felizardo, N. Garcia, A. H. Sodhro, and S. C. Mukhopadhyay, "Towards machine learning enabled security framework for IoT-based healthcare," in *Proc. 13th Int. Conf. Sens. Technol. (ICST)*, Sydney, NSW, Australia, Dec. 2019, pp. 1–6, doi: 10.1109/ICST46873.2019.9047745.

[29] I. Batra, S. Verma, Kavita, and M. Alazab, "A lightweight IoT-based security framework for inventory automation using wireless sensor network," *Int. J. Commun. Syst.*, vol. 33, no. 4, p. e4228, Mar. 2020.

[30] X. Li, X. Jin, Q. Wang, M. Cao, and X. Chen, "SCCAF: A secure and compliant continuous assessment framework in cloud-based IoT context," *Wireless Commun. Mobile Comput.*, vol. 2018, Oct. 2018, Art. no. 3078272, doi: 10.1155/2018/3078272.

[31] K. Djemame, D. Armstrong, M. Kiran, and M. Jiang, "A risk assessment framework and software toolkit for cloud service ecosystems," in *Proc. Int. Conf. Cloud Comput., GRIDs, Virtualization*, 2011, pp. 119–126.

[32] T. Denning, T. Kohno, and H. M. Levy, "Computer security and the modern home," *Commun. ACM*, vol. 56, no. 1, pp. 94–103, Jan. 2013, doi: 10.1145/2398356.2398377.

[33] W. M. Kang, S. Y. Moon, and J. H. Park, "An enhanced security framework for home appliances in smart home," *Hum.-Centric Comput. Inf. Sci.*, vol. 7, no. 1, Dec. 2017, Art. no. 6, doi: 10.1186/s13673-017-0087-4.

[34] H. Dawson. (Jun. 27, 2019). *The Most Influential Security Frameworks of All Time*. Accessed: Mar. 31, 2021. [Online]. Available: https://www.infosecurity-magazine.com/opinions/most-influential-frameworks-1-1-1/

[35] NIST-A. (Feb. 12, 2014). *Cybersecurity Framework*. Accessed: Mar. 31, 2021. [Online]. Available: https://www.nist.gov/cyberframework

[36] G. Mutune. *Top Cybersecurity Frameworks*. Accessed: Apr. 13, 2021. [Online]. Available: https://cyberexperts.com/cybersecurity-frameworks/#2_NIST_Cybersecurity_Framework3

[37] NIST-B. (Apr. 16, 2018). *Framework for Improving Critical Infrastructure Cybersecurity*. Accessed: Apr. 13, 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[38] NIST-C. *NIST Risk Management Framework-RMF*. Accessed: Apr. 13, 2021. [Online]. Available: https://csrc.nist.gov/Projects/risk-management/about-rmf

[39] W. L. Ross and W. Copan. (Dec. 10, 2020). Security and privacy controls for information systems and organizations. NIST. Accessed: Apr. 13, 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[40] N. Lefkovitz and K. Boeckl. (Jun. 2020). *NIST Privacy Framework: An Overview*. Accessed: Apr. 13, 2021. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=930470

[41] R. M. Blank and P. D. Gallagher. (Sep. 2012). *Guide for Conducting Risk Assessments*. Accessed: Apr. 13, 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[42] W. L. Ross and W. Copan. (Dec. 2018). *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. Accessed: Apr. 13, 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

[43] G. Locke and P. D. Gallagher. (Mar. 2011). *Managing Information Security Risk—Organization, Mission, and Information System View*. Accessed: Apr. 13, 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

[44] M. Nieles, K. Dempsey, and V. Y. Pillitteri, "An introduction to information security," U.S. Dept. Commerce, USA, Tech. Rep. NIST SP 800-12, Jan. 2017. Accessed: Apr. 15, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Publications/sp/800-12/rev-1/draft/documents/sp800_12_r1_draft.pdf

[45] M. Swanson and B. Guttman, "Generally accepted principles and practices for securing information technology systems," U.S. Dept. Commerce, USA, Tech. Rep. NIST SP 800-14, Sep. 1996. Accessed: Apr. 15, 2021. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=890092

[46] R. Ross, S. Katzke, A. Johnson, M. Swanson, G. Stoneburner, and G. Rogers. (Dec. 2006). *Recommended Security Controls for Federal Information Systems*. Accessed: Apr. 15, 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-53r1.pdf

[47] U.S. Department of Education. *Family Educational Rights and Privacy Act (FERPA)*. Accessed: Apr. 13, 2021. [Online]. Available: https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

[48] PCI-Security Standards Council. *Maintaining Payment Security*. Accessed: Apr. 13, 2021. [Online]. Available: https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

[49] Digital Guardian. *What is PCI Compliance?* Accessed: Apr. 13, 2021. [Online]. Available: https://digitalguardian.com/blog/what-pci-compliance

[50] OUSD(A&S) and United States DoD. *Cybersecurity Maturity Model Certification*. Accessed: Apr. 13, 2021. [Online]. Available: https://www.acq.osd.mil/cmmc/

[51] J. Christopher. (Nov. 1, 2018). The cybersecurity maturity model: A means to measure and improve your cybersecurity program. Forbes Technology Council. Accessed: Apr. 13, 2021. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2018/11/01/the-cybersecurity-maturity-model-a-means-to-measure-and-improve-your-cybersecurity-program/

[52] U.S. Department of Energy and Office of Cybersecurity, Energy Security, and Emergency Response. *Cybersecurity Capability Maturity Model (C2M2) Program*. Accessed: Apr. 13, 2021. [Online]. Available: https://www.energy.gov/ceser/energy-security/cybersecurity-capability-maturity-model-c2m2-program

[53] Federal Financial Institutions Examination Council (FFIEC). *Cybersecurity Assessment Tool*. Accessed: Apr. 13, 2021. [Online]. Available: https://www.ffiec.gov/cyberassessmenttool.htm

[54] Digital Guardian. (Aug. 12, 2020). *The FFIEC Cybersecurity Assessment Tool: A Framework for Measuring Cybersecurity Risk and Preparedness in the Financial Industry*. Accessed: Apr. 13, 2021. [Online]. Available: https://digitalguardian.com/blog/ffiec-cybersecurity-assessment-tool-framework-measuring-cybersecurity-risk-and-preparedness

[55] *Cyber Security*, Standard 1300, NERC, Sep. 2004. Accessed: Apr. 14, 2021. [Online]. Available: https://www.nerc.com/pa/Stand/Cyber%20Security%20Permanent/Draft_Version_1_Cyber_Security_Standard_1300_091504.pdf

[56] NERC. *CIP Standards*. Accessed: Apr. 13, 2021. [Online]. Available: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[57] *Security for Industrial Automation and Control Systems—Part 4–1: Secure Product Development Lifecycle Requirements*, Standard ANSI/ISA-62443-4-1-2018, International Society of Automation, 2018. Accessed: Apr. 14, 2021. [Online]. Available: https://www.isa.org/products/ansi-isa-62443-4-1-2018-security-for-industrial-au

[58] European Union. *What is GDPR, the EU's New Data Protection Law*. Accessed: Apr. 13, 2021. [Online]. Available: https://gdpr.eu/what-is-gdpr/

[59] AICPA. *SOC 2—SOC for Service Organizations: Trust Services Criteria*. Accessed: Apr. 13, 2021. [Online]. Available: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html

[60] J. E. Wynn. (Oct. 1, 2014). *Threat Assessment and Remediation Analysis (TARA)*. Accessed: Apr. 14, 2021. [Online]. Available: https://www.mitre.org/sites/default/files/publications/pr-2359-threat-assessment-and-remediation-analysis.pdf

[61] C. J. Alberts, S. G. Behrens, R. D. Pethia, and W. R. Wilson, "Operationally critical threat, asset, and vulnerability evaluation (OCTAVE) framework, version 1.0," Carnegie Mellon Univ., Softw. Eng. Inst., Pittsburgh, PA, USA, CMU/SEI Rep. CMU/SEI-99-TR-017 and ESC-TR-99-017, 2018.

[62] IASME Consortium. (2021). *IASME Governance Audited*. Accessed: Apr. 14, 2021. [Online]. Available: https://www.iasme.co.uk/iasme-governance/iasme-governance-audited/

[63] Realwire and Crossword Cybersecurity Plc. (Nov. 25, 2020). *IASME Consortium to Deliver IoT Certification Using Crossword Cybersecurity's Rizikon Assurance Platform*. Accessed: Apr. 14, 2021. [Online]. Available: https://www.realwire.com/releases/IASME-Consortium-to-deliver-IoT-Certification-using-Crossword-Cybersecurity

[64] Hitrust Alliance. *HITRUST CSF—One Framework, One Assessment, Globally*. Accessed: Apr. 14, 2021. [Online]. Available: https://hitrustalliance.net/product-tool/hitrust-csf/

[65] Center for Internet Security. *CIS Controls*. Accessed: Apr. 14, 2021. [Online]. Available: https://www.cisecurity.org/controls/

[66] ISACA. *COBIT*. Accessed: Apr. 14, 2021. [Online]. Available: https://www.isaca.org/resources/cobit

[67] Protectivesecurity and New Zealand Government. *Protective Security Requirements*. Accessed: Apr. 14, 2021. [Online]. Available: https://www.protectivesecurity.govt.nz/

[68] COSO. *Committee of Sponsoring Organizations of the Treadway Commission*. Accessed: Apr. 14, 2021. [Online]. Available: https://www.coso.org/Pages/default.aspx

[69] ACSC and Australian Signals Directorate. (Jun. 2020). *Essential Eight Maturity Model*. Accessed: Apr. 14, 2021. [Online]. Available: https://www.cyber.gov.au/sites/default/files/2020-06/PROTECT%20-%20Essential%20Eight%20Maturity%20Model%20%28June%202020%29.pdf

[70] National Cyber Security Centre. *10 Steps to Cyber Security*. Accessed: Apr. 14, 2021. [Online]. Available: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security

[71] ETSI Technical Committee. *TC CYBER Roadmap*. Accessed: Apr. 14, 2021. [Online]. Available: https://www.etsi.org/cyber-security/tc-cyber-roadmap

[72] Parliamentary Counsel Office. (Jun. 30, 2020). *Privacy Act 2020—New Zealand Legislation*. Accessed: Apr. 14, 2021. [Online]. Available: https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html

[73] Consortium for Information & Software Quality. *The Coding Rules to Deliver Resilient and Scalable Software*. Accessed: Apr. 14, 2021. [Online]. Available: https://www.it-cisq.org/coding-rules/index.htm

[74] Federal Risk and Authorization Management Program. Accessed: Apr. 14, 2021. *Securing Cloud Services for the Federal Government*. [Online]. Available: https://www.fedramp.gov/

[75] Cybersecurity and Infrastructure Security Agency. *Federal Information Security Modernization Act*. Accessed: Apr. 15, 2021. [Online]. Available: https://www.cisa.gov/federal-information-security-modernization-act

[76] OpenSCAP. *SCAP Standards*. Accessed: Apr. 15, 2021. [Online]. Available: https://www.open-scap.org/features/standards/

[77] ISO/IEC. *Standards in the ISO/IEC 27000 Family*. Accessed: Apr. 15, 2021. [Online]. Available: https://www.iso.org/search.html?q=27000

[78] A. AboBakr and M. A. Azer, "IoT ethics challenges and legal issues," in *Proc. IEEE 12th Int. Conf. Comput. Eng. Syst. (ICCES)*, Dec. 2017, pp. 233–237.

[79] N. Fabiano, "Internet of Things and the legal issues related to the data protection law according to the new European general data protection regulation," *Athens J. Law*, vol. 3, no. 3, pp. 201–214, Jun. 2017.

[80] A. Khanna and S. Kaur, "Internet of Things (IoT), applications and challenges: A comprehensive review," *Wireless Pers. Commun.*, vol. 114, no. 2, pp. 1687–1762, Sep. 2020, doi: 10.1007/s11277-020-07446-4.

[81] N. G. Joey. (Dec. 11, 2016). Adaptive challenge and the leadership challenge. Focus Adventure. Accessed: May 11, 2021. [Online]. Available: http://www.focusadventure.com/adaptive-challenge-and-the-leadership-challenge/

[82] U.S. Department of Health & Human Services. (1996). *Health Information Privacy*. Accessed: Apr. 13, 2021. [Online]. Available: https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html

[83] ETSI. *ETSI Standards*. Accessed: Aug. 11, 2021. [Online]. Available: https://www.etsi.org/standards#Pre-defined%20Collections

NICKSON M. KARIE (Member, IEEE) received the Ph.D. degree in computer science from the University of Pretoria, South Africa, in 2016, majoring in cybersecurity and digital forensics. He is currently a Cybersecurity CRC Research Fellow with the Security Research Institute, Edith Cowan University, Perth, WA, Australia. He has more than ten years of experience in academic teaching, research, and consultancy in different countries, including India, Kenya, South Africa, Swaziland, and Australia. His research interests include cybersecurity and digital forensics, intrusion detection and prevention, information and computer security architecture, network security and forensics, mobile device forensics, and cloud and the IoT security. He is also actively engaged as an editor, author, and reviewer in several high impact international conferences and journals.

NOR MASRI SAHRI received the Ph.D. degree in cyber security from Kyushu University, Kyushu, Japan, in 2016. He is a currently Postdoctoral Fellow Researcher with the Cyber Security CRC at Edith Cowan University, Perth, WA, Australia. Previously, he is also working as a Senior Network Engineer at Heitech Padu Berhad, Malaysia, managing various network communication projects. His current work is focused on the cybersecurity of critical infrastructure and the IoT. His research interests include threat detection and authentication protocols, SDN, and the Internet of Things. He has more than ten years of experience in cybersecurity research and education in both Malaysia and Australia. He is also actively engaged as a high impact journal reviewer.

WENCHENG YANG received the Ph.D. degree from the School of Engineering and Information Technology, University of New South Wales, Canberra, Australia, in 2015. He is a Cyber Security CRC Postdoctoral Fellow with Edith Cowan University (ECU), Australia. He has authored several papers published in high-ranking journals and conferences, e.g., IEEE Transactions on Information Forensics and Security and *Pattern Recognition*. His research interests include biometric security and biometric recognition.

CRAIG VALLI (Member, IEEE) received the Diploma degree in teaching from Western Australian CAE, Perth, Australia, in 1985, and the Bachelor of Education, Master of Management (Information Systems), and the Doctor of Information Technology degrees from Edith Cowan University, Perth, in 1990, 2000, and 2003, respectively. He has over 30 years of experience in the ICT industry and consults with industry and government on cybersecurity and digital forensics issues. He is currently the Director of the Security Research Institute, Edith Cowan University, and a Professor of digital forensics. He has over 100 peer-reviewed academic publications in cybersecurity and digital forensics. His main research and consultancy are focused on securing networks and critical infrastructures, detection of network borne threats, and forensic analysis of cybersecurity incidents. He is a fellow of the Australian Computer Society, and the Director of the Australian Computer Society Centre of Expertise in Security at ECU. He is also the Research Director of the Australian Cyber Security Research Institute, the Vice President of the High-Tech Crime Investigators Association (Australian Chapter), and a member of the INTERPOL Cyber Crime Experts Group.

VICTOR R. KEBANDE received the Ph.D. degree in computer science (information and computer security architectures and digital forensics) from the University of Pretoria, Hatfield, South Africa. He was a Researcher with the Information and Computer Security Architectures (ICSA) and the DIgiFORS Research Groups, University of Pretoria, and he was a Postdoctoral Researcher with the Internet of Things and People (IOTAP) Center, Department of Computer Science, Malmö University, Malmö, Sweden. He was also a Postdoctoral Researcher of cyber and information security in information systems research subject with the Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Luleå, Sweden. He is currently an Assistant Professor of IT Security with the Department of Computer Science (DIDA), Blekinge Institute of Technology (BTH), Karlskrona, Sweden. His research interests include cyber, information security and digital forensics in the IoT, the IoT security, digital forensics-incident response, cyber-physical system protection, critical infrastructure protection, cloud computing security, computer systems, distributed system security, threat hunting and modeling and cyber-security risk assessment, blockchain technologies, and privacy-preserving techniques. He also serves as an Editorial Board Member for *Forensic Science International: Reports* journal.