Computers, Materials & Continua
DOI:10.32604/cmc.2021.016058
Article

Tech Science Press

Systematic Analysis of Safety and Security Risks in Smart Homes

Habib Ullah Khan[1,*], Mohammad Kamel Alomari[1], Sulaiman Khan[2], Shah Nazir[2], Asif Qumer Gill[3], Alanoud Ali Al-Maadid[4], Zaki Khalid Abu-Shawish[1] and Mostafa Kamal Hassan[1]

[1]Department of Accounting and Information Systems, College of Business and Economics, Qatar University, Doha, Qatar
[2]Department of Computer Science, University of Swabi, Swabi, Pakistan
[3]School of Software, University of Technology Sydney, Sydney, Australia
[4]Department of Finance & Economics, College of Business & Economics, Qatar University, Doha, Qatar
[*]Corresponding Author: Habib Ullah Khan. Email: habib.khan@qu.edu.qa
Received: 21 December 2020; Accepted: 11 February 2021

Abstract: The revolution in Internet of Things (IoT)-based devices and applications has provided smart applications for humans. These applications range from healthcare to traffic-flow management, to communication devices, to smart security devices, and many others. In particular, government and private organizations are showing significant interest in IoT-enabled applications for smart homes. Despite the perceived benefits and interest, human safety is also a key concern. This research is aimed at systematically analyzing the available literature on smart homes and identifying areas of concern or risk with a view to supporting the design of safe and secure smart homes. For this systematic review process, relevant work in the most highly regarded journals published in the period 2016–2020 (a section of 2020 is included) was analyzed. A final set of 99 relevant articles (journal articles, book sections, conference papers, and survey papers) was analyzed in this study. This analysis is focused on three research questions and relevant keywords. The systematic analysis results and key insights will help researchers and practitioners to make more informed decisions when dealing with the safety and security risks of smart homes, especially in emergency situations.

Keywords: Smart buildings; IoT; smart homes; systematic literature review; prototype model

1 Introduction

During the last decade, Internet of Things (IoT)-enabled smart applications have been increasingly integrated into our daily life and related activities, e.g., healthcare, home, manufacturing, and transportation [1]. These applications are connected through the Internet to enhance and facilitate the way we live, work, and play [2]. The IoT-enabled smart home is one of the important areas discussed in this paper [2]. A smart home has technologies that facilitate sensing and monitoring of people and home appliances. In short, smart homes are used to monitor and control home-facing operations and their continuous adaptation. In the last few years, concepts from smart

homes have been applied to other areas, such as smart healthcare systems [3], energy systems [4], security and emergency management systems [5], and comfort and entertainment systems [6].

A smart living environment's automatic transformation mechanism is controlled by the arguing system, which is considered the brain of the smart living architectures. The smart home arguing system (SHAS) is used to make accurate decisions ensuring the security, safety, and comfort of the inhabitants and their surroundings. Keeping this in mind, researchers have intensively explored and studied multiple artificial intelligence (AI)-based systems and their uses for ambient-assisted living (AAL) systems. However, no systematic mechanism has been proposed that investigates the decision support systems (DSS) incorporated in smart living environments. Chan et al. [7] and Calvaresi et al. [8] reviewed smart living environments. Others, including Zaidan et al. [9] and Brand et al. [10], studied smart homes from single application domain perspectives, such as IoT-based communication components, and privacy concerns of IoT components in living environments. Furthermore, Wilson et al. [11] reported on smart home residents and their uses of the underlying infrastructure from socio-technical perspectives. To the best of our knowledge, there is a lack of comprehensive systematic literature review of the current context of human safety and security in smart homes.

In this paper, a systematic literature review (SLR) is presented that examines the aforementioned domain of smart homes from the following perspectives:

- Determine the main goal of smart living systems;
- Deliver new understanding and new knowledge about human safety in a rapidly evolving smart built environment;
- Identify and characterize the key features and requirements of smart living to ensure safety and security during emergencies;
- Catalogue the tools and features that provide the abilities to monitor, collect, and process real-time human sensors, and build data for efficient and effective decision making.

The rest of this paper is organized as follows. In Section 2, the proposed SLR process adapted for literature search and analysis is described. SLR results are reported and discussed in Section 3. The limitations of the proposed research work are outlined in Section 4, followed by conclusions and directions of planned future work in Section 5.

2 Review Process

SLR is a well-known process used to identify and evaluate available research work relevant to a particular subject or event of interest. SLR aims to present a fair evaluation of a particular research topic using a rigorous, trustworthy, and auditable methodology [12]. SLR studies are reported in many fields, e.g., networking PMIPV6 domains [13] and healthcare Big Data analytics [14]. The main reasons for performing a SLR are the following:

- To explore and summarize the existing research work on a particular technology;
- To find the gaps in the available technology that will ultimately lead to future investigations.

In the proposed research work, the SLR process is conducted by following the guidelines suggested by Kitchenham et al. [15,16]. The proposed review process protocol is depicted in Fig. 1 and consists of three main phases: (1) planning the review process, (2) performing the review process, and (3) reporting the results of the review process. All these steps are illustrated in detail in Fig. 1.

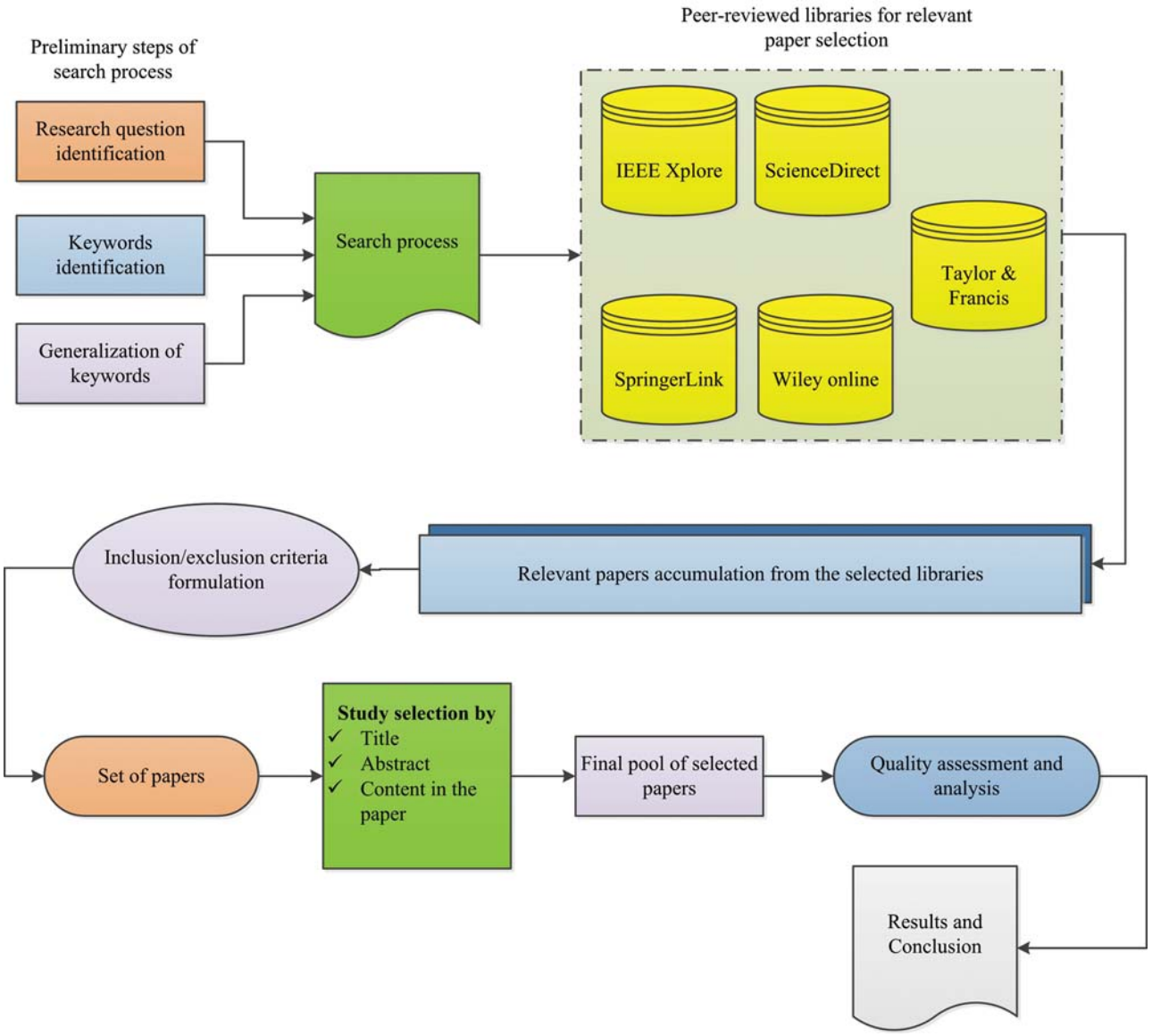

Figure 1: Research protocol of the proposed SLR work

2.1 Review Process Planning

The proposed systematic review process is performed using the guidelines provided by Kitchenham [16,17]. Based on these guidelines, researchers must explore the existing evidence on a topic of interest and determine the need for a review process. Furthermore, the study outlines the key pre-review activities: formulation of the research questions, identification of the keywords and query formulation, selection of the peer-reviewed online digital libraries for the accumulation of the relevant primary articles for the review process, and the inclusion/exclusion criteria. Accordingly, the present systematic review was performed due to recent increasing research interest in smart homes and living environments. It is noted that there is a lack of systematic literature

review study in the specific context of smart home safety and security risks, particularly during emergency situations.

2.1.1 Research Question Formulation

As discussed earlier, research question formulation is an essential activity in conducting a SLR. For defining the most relevant research questions, the Goal-Questions-Metrics approach of Van Solingen et al. [18] was followed, and, consequently, the three research questions given in Tab. 1 were formulated.

Table 1: Research questions

S. No.	Research question	Goal
RQ1	What are the state-of-the-art approaches proposed for development of smart buildings?	Summarizes the different state-of-the-art techniques suggested for development of smart buildings in smart cities.
RQ2	What hardware components are used for early alarm mechanisms in emergency situations?	Aims to uncover the hardware devices or applications reported in the literature for early alarm purposes in case of emergencies.
RQ3	What proactive approaches are developed to reduce the loss of life or injuries in smart buildings during emergency situations?	Based on the literature, aims to accumulate knowledge on various proactive approaches that have been developed to reduce the human loss of life or injuries in emergency situations by providing guidance, communications, and monitoring facilities.

2.1.2 Identification of Keywords and Query Formulation

After formulating the research questions, the next and most important activity of the SLR was to identify keywords and formulate a search query to systematically select the most relevant articles from the selected online digital libraries. Keywords and the search query are shown in Tab. 2.

Table 2: Keywords and query for search process

(“SMART BUILDINGS” OR “SMART HOME” OR “SMART HOMES” OR “SMART LIVING ENVIROMENTS”) AND (“SECURITY” OR “SAFETY” OR “RISKS” OR “THREATS”) AND (“EMERGENCY SERVICES” OR “EMERGENCY EVACUATION” OR “COMMUNICATION DEVICES” OR “AUTO CONTROL DEVICES” OR “IOT DEVICES”)

2.1.3 Online Digital Library Selection

The five well-known online digital libraries shown in Tab. 3 were selected to identify relevant research.

Table 3: Online digital libraries selected for article accumulation

S. No.	Digital library	Hyperlink	Access date
1.	Wiley online	https://onlinelibrary.wiley.com	July 28, 2020
2.	IEEE Xplore	https://ieeexplore.ieee.org/Xplore/home.jsp	July 26, 2020
3.	SpringerLink	https://link.springer.com/	July 27, 2020
4.	ScienceDirect	https://www.sciencedirect.com	July 27, 2020
5.	Taylor & Francis	https://www.tandfonline.com	July 28, 2020

The primary articles were selected and downloaded from these digital libraries based on the defined query. After downloading, these papers were further analyzed and explored to remove the redundant and irrelevant papers, if any. Irrelevant papers, i.e., those that did discuss smart buildings or smart homes, were removed. The finalized primary articles were then merged into a single set or directory. These are the papers that address at least one of the research questions. In summary, 99 research articles were selected as most relevant primary research articles for the purpose of the present SLR study.

2.1.4 Inclusion/Exclusion Criteria

Defining inclusion/exclusion criteria is the most challenging job in a SLR research process. As the main activity of the process, it ensures the selection of the most relevant primary articles for the final pool of papers for further quality assessment. Tab. 4 presents the inclusion/exclusion criteria of the primary studies relevant to the aforementioned proposed research questions.

Table 4: Inclusion/exclusion criteria

Inclusion criteria
1) Include only those papers that are reported in English language.
2) Include only primary studies.
3) Include papers published between 2016 and 2020.
4) Does the paper's title reflects enough knowledge about smart homes and smart living environments, and does the paper contain information for emergency exit and safety precautions?
5) Determine whether the abstract provides enough information about the smart buildings and safety measures during emergency situations.
6) Do the contents in the paper provide proper validation?
Exclusion criteria
1) Exclude papers written in languages other than English.
2) Exclude ambiguous papers.
3) Exclude research papers containing less than three pages.
4) Exclude papers that fail to satisfy the inclusion criteria.

The selected primary research articles were thoroughly checked and analyzed by all the authors to ensure research validity and avoid any possible omission. Significant attention is given to the last three questions, which are defined for the inclusion of a paper in this study. A voting mechanism was considered for this step. If more than half of the authors agreed to the inclusion of the paper, then the paper was added to the final set of the most relevant articles; otherwise, the paper was excluded. This voting mechanism is based on the paper's title, abstract, and contents presented in the research article itself. A summary of the overall inclusion process is shown in Tab. 5. A final pool of 99 relevant primary articles was selected for the assessment process.

Table 5: Selection of the primary studies for final pool

Digital library	Articles selected based on			
	Query	Title	Abstract	Content provided
IEEE	1035	546	216	51
ScienceDirect	1399	312	77	10
SpringerLink	2106	276	107	22
Wiley online	883	131	39	9
Taylor & Francis	172	91	37	7
Total	99			

2.2 Review Process

After performing the preliminary steps of selecting the online digital libraries, identifying research questions, selecting keywords, and determining inclusion/exclusion criteria, the next phase was to perform the review using the research protocol selected as shown in Fig. 1. This activity includes defining final pool selection, data synthesis, monitoring, and quality assessment processes. All of these steps are discussed in detail in the following subsections.

2.3 Final Pool of Relevant Articles

After sorting the selected digital libraries for the relevant primary articles and performing the inclusion/exclusion process, a final set of 99 relevant articles were selected for SLR. The final pool of papers includes workshop papers, conference proceedings, book sections, journal articles, and review/survey articles. Tab. 6 presents details of the selected finalized pool of research articles.

Table 6: Evolution of final set of relevant papers

Digital library	Journal articles	Conference papers	Book sections	Review papers
IEEE Xplore	[19–25]	[26–66]		[67–69]
ScienceDirect	[70–75]	[76–78]		
SpringerLink	[4,79–89]	[90–95]	[96–99]	[9–11,100,101]
Taylor & Francis	[102–106]			
Wiley online	[107–110]		[111–117]	

The mapping of paper sources is shown in Fig. 2, from which it is concluded that IEEE Xplore contains more papers when compared to other sources. This may reflect the interest of researchers to publish their research work in IEEE Xplore.

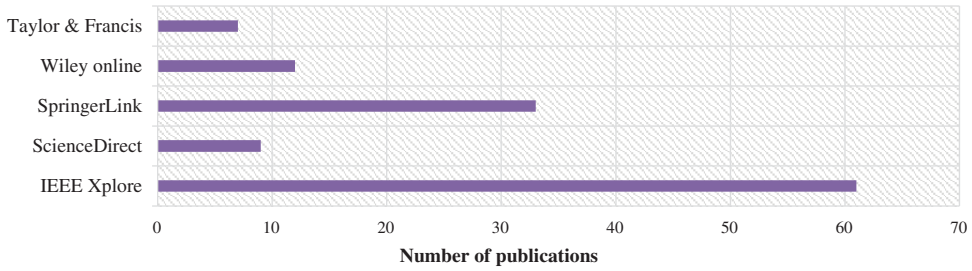

Figure 2: Contribution of each library in the final set of relevant papers

The final paper set was also sorted based on year and publication sources. It is observed that the number of publications increases with the passage of time, which may reflect the growing interest among the research community in the proposed area of research. Fig. 3 shows the sorting results.

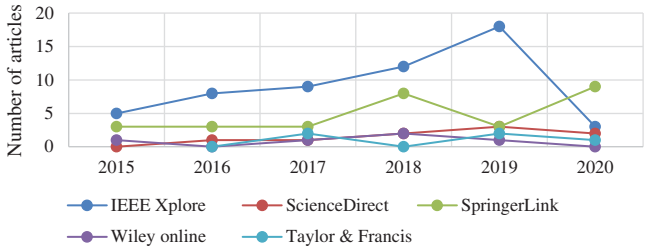

Figure 3: The Sorting Results

Furthermore, the final set of relevant papers was sorted based on digital library, reference list, type of paper, and publication year, as depicted in Fig. 4. In the figure, the outer shell represents the references to the primary articles, the medium shell the paper type, and the most-inner-shell date of publication.

2.4 Quality Assessment

The quality of the selected relevant articles was assessed using the criteria defined in the SLR protocol. The set of relevant articles was reviewed and assessed against each of the research questions and corresponding criteria (QC) listed in Tab. 7.

This assessment ensured the quality of each selected paper for SLR. Furthermore, weights were assigned to all research questions based on the following criteria:

- 0 if a paper has no information for the selected research question;
- 0.5 if a paper has a piece of partial but satisfactory information about a research question;
- 1 if a paper contains a full and complete description for the research question.

After performing the quality assessment, the most relevant articles were determined, as shown in Fig. 5.

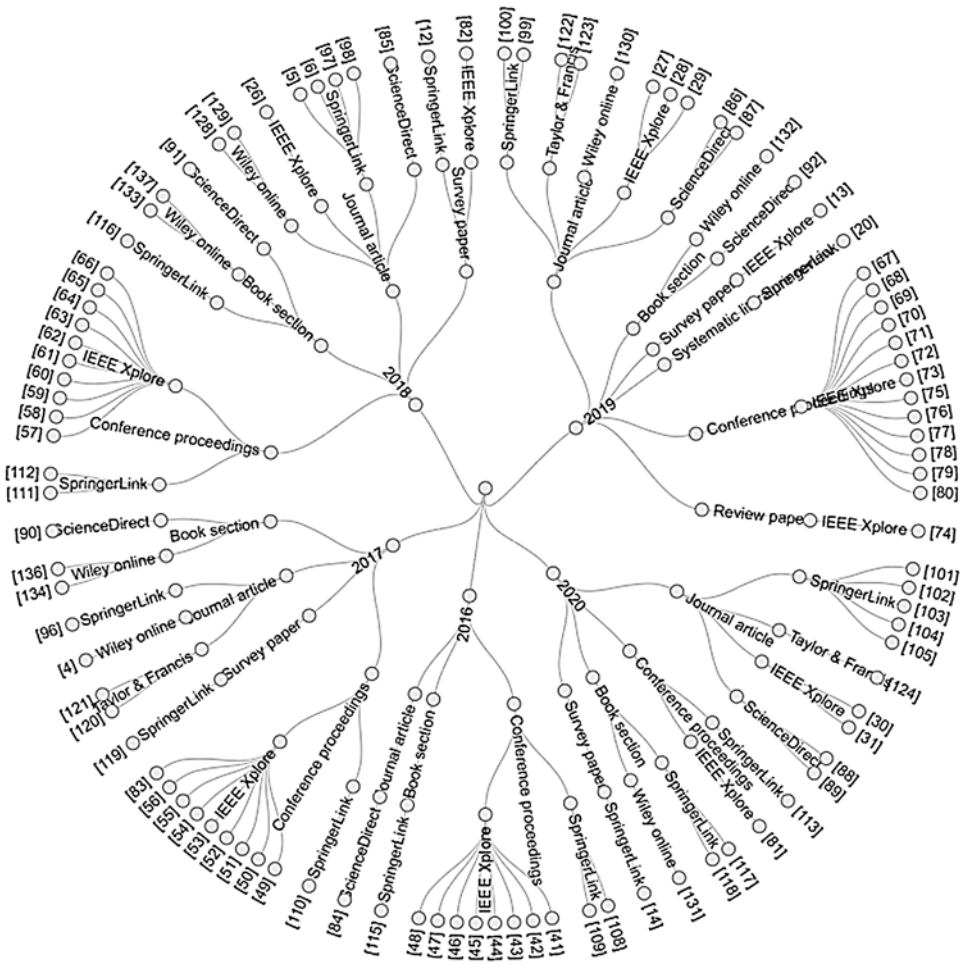

Figure 4: Evolution of the final selected papers

Table 7: Quality criteria for assessment process

Quality criterion	Criterion description
QC1	Whether the paper provides detailed information about architecture or design followed for development of smart buildings in smart cities.
QC2	Whether the paper provides in-depth knowledge and understanding about human safety in rapidly evolving smart environments.
QC4	Whether the paper provides a proactive approach to reducing loss of life and injuries in emergency situations by providing proper guidance, communication, and monitoring facilities.

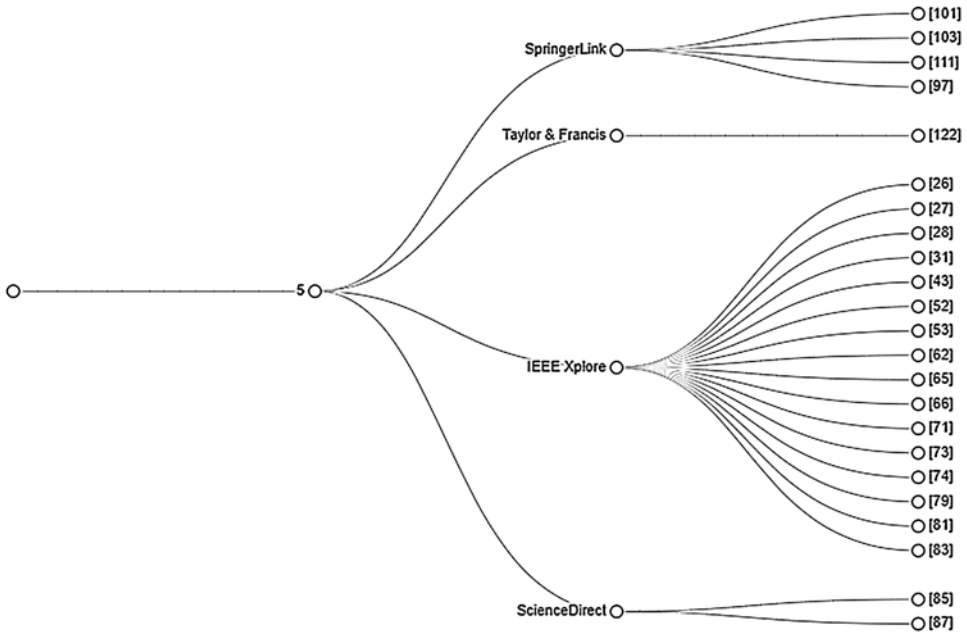

Figure 5: Most relevant research articles

3 Results and Discussions

Each subsection below provides details of each related research question formulated for the present SLR research work.

3.1 RQ1-What are State-of-the-Art Approaches Proposed for Development of Smart Buildings?

Responses to this question were used to synthesize the literature from 2016 to 2020 in which the approaches for developing smart building architectures were discussed. Tab. 8 outlines the different approaches proposed for smart building architectures.

3.2 RQ2-What Hardware Components are Used for Early Alarm Mechanism in Emergency Situations?

Smart homes or smart living environments are developed to facilitate living with high standards and resiliency in normal and emergency situations. Tab. 9 lists multiple hardware devices or applications that are proposed for early alarm purposes during emergency situations.

3.3 RQ3-What Proactive Approaches are Developed to Reduce Loss of Life or Injuries in Smart Buildings During Emergency Situations?

Smart living environments have been developed to ensure human healthcare and security, but concerns or emergency situations exist that must be addressed, such as short circuits, other fire issues, and earthquakes, that may adversely impact smart living environments. The present SLR study uncovered a number of approaches, which are listed in Tab. 10.

Table 8: List of approaches proposed for smart building architectures

S. No.	Smart building architectures	Description
1.	Smart home, smart office	This book chapter [115] introduces a case study for the smart home or smart office living environments.
2.	High-performance building design	This chapter [116] introduces multiple efforts for simulations and emissions that help realize the mitigation goals. It also explains the effects of varying climate conditions and procedures for climate resiliency planning.
3.	Hierarchical combinatorial reliability model	This research article [109] presents a hierarchical and combinatorial mechanism used to model and evaluate smart living system reliability. In particular, the proposed system encapsulates a multi-variant decision-diagram-based mechanism to address standby sparing, phased-mission, and functional dependence behaviors in the physical layer. The combinatorial strategies are developed using the total probability theorem.
4.	Smart home architecture	These research articles [11] outline the challenges faced by researchers in the available designs and architectures of smart living environments. Based on the challenges, it presents an optimal solution for smart homes.
5.	Smart home using embedded technology	These research articles [81,102] = propose a smart home architecture using embedded technology to ensure safety and basic needs of relevant objects.
6.	Ambient-assisted living (AAL) smart environments	This research article [104] proposes a new mechanism named "ambient assisted living" smart environments for the South Korean people. As it is believed that South Korea is anticipated to be a super-aged society by the end of 2025, persistent steps and efforts are being made to reduce the burden of maintaining and promoting a productive and healthy lifestyle for elderly people.
7.	Conjugated smart home environment	This paper [106] presents a conjugated single-chip-based controlling unit for controlling the daily tasks (morning wake-up calls, cooking timings), intrusion detection, and event control. This also ensures the security and safety of residents in smart environments.
8.	Efficient energy-management-based smart home interface	This research work [83] aims to develop an IoT-based smart home security system for real-time health monitoring technologies in a telemedicine architecture.

Table 9: List of hardware components used for early alarm purposes

S. No.	Early alarm device	Description
1.	Energy meter sensor	This book chapter [117] introduces the energy meter sensor-based application for a personal assistant and baby monitoring.
2.	X10, Insteon, ZigBee, and Universal Plug-and-Play	Zigbee has attracted significant attention due to pervasive access of embedded devices over the Internet and increasing penetration of wireless protocols in smart living environments. Aburukba et al. [26] suggested ZigBee for monitoring the well-being of aged or disabled persons in smart cities.
3.	TRI 2.0, consumer engagement, and perceived risk and trust	This research work [105] contributes new ideas for consumer preparedness in smart home technology adoption. This combines three significant frameworks: consumer engagement, technology readiness index (TRI) 2.0, and perceived risk and trust. This mechanism aims to learn about human intentions for adopting smart home living environments and living styles.
4.	Infrared rays, IPCAM's	This paper [106] presents a single-chip controlling unit for controlling daily tasks (morning wake-up calls, cooking timings) for intrusion detection and event control.
5.	IEEE 802.11-series components and heterogeneous sensors	This study [84] characterizes IEEE 802.11-enabled wireless networks under jamming attacks and proposes a safe and secure model for smart homes.
6.	LoRaWAN	LoRaWAN is considered a long-range secure communication technology. This research work [87] proposes use of LoRaWAN for security and communication purposes in smart homes.
7.	Robot-based integrated smart home	This is a robot-integrated smart home [71] developed to provide healthcare facilities for aged persons at a smart home. This is a layered architecture designed to perform guidance tasks, healthcare tasks, and other tasks for elderly people.
8.	Fire detection system	This research work [43] proposes an IoT-based fire-detection system in smart buildings. The system was designed using MQ-135 (CO2), MQ-7 (CO), MQ-2 (smog), and DHT-11 (temperature) sensors that were integrated with an Arduino board for accurately sourcing information in fire events.

Table 10: List of proactive approaches to counter emergency situations

S. No.	Proactive approach	Description
1.	Wireless sensor network	This book chapter [113] addresses common healthcare issues and suggests a wireless-sensor-based network architecture to monitor the air quality for carbon dioxide in complex indoor smart living environments. The research articles [29,35] proposed a wireless sensor network for elderly healthcare purposes in smart living environments.
2.	Smart bed	This paper [108] discusses the test bed using real-time datasets, which is aimed at observing system efficiency through different parameters, e.g., time consumption, response times for attack detection, and storage requirements of the proposed approach.
3.	Remote health monitoring of triage and priority system	This research work [83] develops an IoT-based smart living security mechanism for telemedicine systems intended to support real-time health monitoring.
4.	Observing and restricting wireless jamming attacks	This study [84] characterizes IEEE 802.11-enabled wireless network efficiency by proposing a safe and secure model for smart homes related to jamming attacks.
5.	Smart dust surveillance	This chapter [98] introduces multiple smart dust mesh perspectives based on the Internet of Everything and Everywhere (IoEE). It has numerous applications in the field of military and security, such as people and product monitoring, eHealth monitoring, and environment surveillance.
6.	Nexus services	In this research work [89], researchers propose a nexus model for smart cities that focuses on collaboration and teamwork services.
7.	RiSH	This is a robot-integrated smart home [71] developed to provide healthcare support for aged persons. This is a layered architecture aimed at supporting different guidance and healthcare functions for elderly people.
8.	Heterogeneous mechanism	This study [72] proposes a heterogeneous approach for evidence identification in IoT networks. A case study is performed to validate the proposed solution.
9.	Business model in European standard	Furszyfer Del Rio et al. [74] proposed a business model for European smart homes. They critically reviewed the available literature with a view to identifying and addressing common problems of security, emergency situations, and healthcare in their new business model.
10.	Acoustic surveillance system	This research work [19] explores machine learning and its application to acoustic surveillance of abnormal situations. The proposed system's main objective is to help an authorized person take appropriate actions to prevent life/property loss before or during an emergency.

4 Limitations

The limitations of the proposed research work are the following.

- Only five digital libraries were selected for SLR. However, these libraries provide broader coverage for peer-reviewed and high-quality research articles.
- A specific range of years (2016–2020 (a portion of 2020 was included in the review process) was selected for SLR. This was done to ensure the inclusion of recent trends and studies relevant to the current context of smart homes. This is also important to set the further research options based on the recent work reported in the present study.
- Google Scholar is another informal source of literature and was thus omitted from the present SLR since the focus was on the systematic selection of only peer-reviewed articles.
- Papers that contain the word "smart home" in their title were excluded, but their contents were not meaningful or relevant to the research questions posed. In other words, papers only containing definitions were omitted from the present study.

5 Conclusions and Future Work

During the past decade, IoT devices have provided state-of-the-art and smart applications for humans. These applications range from smart urban management to smart transportation management devices, smart healthcare devices, smart electrical and home devices, and many others. One of the most inspiring applications is smart homes that aim to support contemporary human living needs. Among the major concerns and challenges of researchers are the security and safety of smart homes. Embedding security in IoT-based applications has been identified as an opportunity to realize the vision of smart and energy-efficient homes and buildings. To address this problem, a SLR was performed to investigate the available literature published in the period 2016–2020 (a portion of 2020 was included in the systematic mapping). This was achieved using the SLR guidelines provided by Kitchenham [16,17].

Five different peer-reviewed online digital libraries were used for sourcing primary research articles. A total of 99 relevant articles (journal articles, book sections, conference proceedings, and survey papers) were identified for analysis and assessment purposes. This systematic synthesis and analysis of the existing research work will serve as a knowledgebase for researchers and designers interested in designing safe and secure smart homes of the future. Furthermore, the results from this SLR will inform the community about recent research trends in smart homes, which are important for formulating future research options.

Acknowledgement: This publication was supported by Qatar University Internal Grant No. IRCC-2020-009. The findings achieved herein are solely the responsibility of the authors.

Funding Statement: The author(s) received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Naoui, M. E. Elhdhili and L. A. Saidane, "Lightweight and secure password based smart home authentication protocol: LSP-SHAP," *Journal of Network and Systems Management*, vol. 27, no. 4, pp. 1020–1042, 2019.

[2] G. Lindsay, B. Woods and J. Corman, *Smart Homes and the Internet of Things*, Washington, D.C., United States: Atlantic Council, 2016.

[3] N. Falcionelli, P. Sernani, A. Brugués, D. N. Mekuria, D. Calvaresi *et al.,* "Indexing the event calculus: Towards practical human-readable personal health systems," *Artificial Intelligence in Medicine*, vol. 96, no. 4, pp. 154–166, 2019.

[4] J. Yu, N. Lee, C. S. Pyo and Y. S. Lee, "WISE: Web of object architecture on IoT environment for smart home and building energy management," *Journal of Supercomputing*, vol. 74, no. 9, pp. 4403–4418, 2018.

[5] M. Schneps-Schneppe, A. Maximenko, D. Namiot and D. Malov, "Wired smart home: Energy metering, security, and emergency issues," in *2012 IV Int. Congress on Ultra Modern Telecommunications and Control Systems*, St. Petersburg, Russia, pp. 405–410, 2012. https://doi.org/10.1109/ICUMT.2012.6459700.

[6] J. R. Velasco, I. Marsá-Maestre, A. Navarro, M. A. López-Carmona and A. J. de Vicente *et al.,* "Location-aware services and interfaces in smart homes using multiagent systems," *PSC*, vol. 5, pp. 104–110, 2005.

[7] M. Chan, D. Estève, C. Escriba and E. Campo, "A review of smart homes—Present state and future challenges," *Computer Methods and Programs in Biomedicine*, vol. 91, pp. 55–81, 2008.

[8] D. Calvaresi, D. Cesarini, P. Sernani, M. Marinoni, A. F. Dragoni *et al.,* "Exploring the ambient assisted living domain: A systematic review," *Journal of Ambient Intelligence and Humanized Computing*, vol. 8, no. 2, pp. 239–257, 2017.

[9] A. A. Zaidan, B. B. Zaidan, M. Y. Qahtan, O. S. Albahri, A. S. Albahri *et al.,* "A survey on communication components for IoT-based technologies in smart homes," *Telecommunication Systems*, vol. 69, no. 1, pp. 1–25, 2018.

[10] D. Brand, F. D. DiGennaro Reed, M. D. Morley, T. G. Erath and M. D. Novak, "A survey Assessing privacy concerns of smart-home services provided to individuals with disabilities," *Behavior Analysis in Practice*, vol. 13, no. 1, pp. 11–21, 2020.

[11] C. Wilson, T. Hargreaves and R. Hauxwell-Baldwin, "Smart homes and their users: A systematic analysis and key challenges," *Personal and Ubiquitous Computing*, vol. 19, no. 2, pp. 463–476, 2015.

[12] B. Kitchenham, "Procedures for performing systematic reviews," Keele, UK: Keele University, vol. 33, pp. 1–26, 2004.

[13] A. Hussain, S. Nazir, S. Khan and A. Ullah, "Analysis of PMIPv6 extensions for identifying and assessing the efforts made for solving the issues in the PMIPv6 domain: A systematic review," *Computer Networks*, vol. 179, pp. 107366, 2020.

[14] S. Nazir, S. Khan, H. U. Khan, S. Ali, I. García-Magariño *et al.,* "A comprehensive analysis of healthcare big data management, analytics and scientific programming," *IEEE Access*, vol. 8, pp. 95714–95733, 2020.

[15] S. Keele, "Guidelines for performing systematic literature reviews in software engineering," *Technical Report*, Ver. 2.3 EBSE Technical Report, 2007.

[16] B. Kitchenham, R. Pretorius, D. Budgen, O. P. Brereton, M. Turner *et al.,* "Systematic literature reviews in software engineering—A tertiary study," *Information and Software Technology*, vol. 52, no. 8, pp. 792–805, 2010.

[17] B. Kitchenham and S. Charters, "Guidelines for performing systematic literaturereviews in software engineering," in *Evidence-Based Software Engineering*, Boca Raton, Florida: Chapman & Hall/CRC, 2007.

[18] R. Van Solingen, V. Basili, G. Caldiera and H. D. Rombach, "Goal question metric (GQM) approach," *Encyclopedia of Software Engineering*, vol. SE-14, pp. 758, 2002.

[19] S. Ntalampiras, I. Potamitis and N. Fakotakis, "Probabilistic novelty detection for acoustic surveillance under real-world conditions," *IEEE Transactions on Multimedia*, vol. 13, no. 4, pp. 713–719, 2011.

[20] S. Chiou and Z. Liao, "A real-time, automated and privacy-preserving mobile emergency-medical-service network for informing the closest rescuer to rapidly support mobile-emergency-call victims," *IEEE Access*, vol. 6, pp. 35787–35800, 2018.

[21] S. Khatoon, S. M. M. Rahman, M. Alrubaian and A. Alamri, "Privacy-preserved, provable secure, mutually authenticated key agreement protocol for healthcare in a smart city environment," *IEEE Access*, vol. 7, pp. 47962–47971, 2019.
[22] S. A. Shah, D. Z. Seker, M. M. Rathore, S. Hameed, S. B. Yahia *et al.,* "Towards disaster resilient smart cities: Can internet of things and big data analytics be the game changers?," *IEEE Access*, vol. 7, pp. 91885–91903, 2019.
[23] D. Shin, K. Yun, J. Kim, P. V. Astillo, J. Kim *et al.,* "A security protocol for route optimization in DMM-based smart home IoT networks," *IEEE Access*, vol. 7, pp. 142531–142550, 2019.
[24] X. Luo, L. Yin, C. Li, C. Wang, F. Fang *et al.,* "A lightweight privacy-preserving communication protocol for heterogeneous IoT environment," *IEEE Access*, vol. 8, pp. 67192–67204, 2020.
[25] M. Wazid, A. K. Das, V. Odelu, N. Kumar and W. Susilo, "Secure remote user authenticated key establishment protocol for smart home environment," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 2, pp. 391–406, 2020.
[26] R. Aburukba, A. R. Al-Ali, N. Kandil and D. AbuDamis, "Configurable ZigBee-based control system for people with multiple disabilities in smart homes," in *2016 Int. Conf. on Industrial Informatics and Computer Systems*, Sharjah, United Arab Emirates, pp. 1–5, 2016. https://doi.org/10.1109/ICCSII.2016.7462435.
[27] E. Bajramovic, K. Waedt, A. Ciriello and D. Gupta, "Forensic readiness of smart buildings: Preconditions for subsequent cybersecurity tests," in *2016 IEEE Int. Smart Cities Conf.*, Trento, Italy, pp. 1–6, 2016. https://doi.org/10.1109/ISC2.2016.7580754.
[28] S. Escolar, D. Villa, F. J. Villanueva, R. Cantarero and J. C. López, "An adaptive emergency protocol for people evacuation in high-rise buildings," in *2016 IEEE Symp. on Computers and Communication*, Messina, Italy, pp. 364–371, 2016. https://doi.org/10.1109/ISCC.2016.7543767.
[29] R. S. Ransing and M. Rajput, "Smart home for elderly care, based on Wireless Sensor Network," in *2015 Int. Conf. on Nascent Technologies in the Engineering Field*, Navi Mumbai, India, pp. 1–5, 2015. https://doi.org/10.1109/ICNTE.2015.7029932.
[30] P. Gupta and J. Chhabra, "IoT based smart home design using power and security management," in *2016 Int. Conf. on Innovation and Challenges in Cyber Security*, Greater Noida, India, pp. 6–10, 2016. https://doi.org/10.1109/ICICCS.2016.7542317.
[31] X. Hong, C. Yang and C. Rong, "Smart home security monitor system," in *2016 15th Int. Symp. on Parallel and Distributed Computing*, Fuzhou, pp. 247–251, 2016. https://doi.org/10.1109/ISPDC.2016.42.
[32] J. Nicklas, M. Mamrot, P. Winzer, D. Lichte, S. Marchlewitz *et al.,* "Use case based approach for an integrated consideration of safety and security aspects for smart home applications," in *2016 11th System of Systems Engineering Conf.*, Kongsberg, Norway, pp. 1–6, 2016. https://doi.org/10.1109/SYSOSE.2016.7542908.
[33] S. Al Salami, J. Baek, K. Salah and E. Damiani, "Lightweight encryption for smart home," in *2016 11th Int. Conf. on Availability, Reliability and Security*, Salzburg, Austria, pp. 382–388, 2016. https://doi.org/10.1109/ARES.2016.40.
[34] S. Dharur, C. Hota and K. Swaminathan, "Energy efficient IoT framework for smart buildings," in *2017 Int. Conf. on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, Palladam, India, pp. 793–800, 2017. https://doi.org/10.1109/I-SMAC.2017.8058288.
[35] R. Fischer, K. Lamshöft, J. Dittmann and C. Vielhauer, "Advanced issues in wireless communication security: Towards a security-demonstrator for smart-home environments," in *2017 Int. Carnahan Conf. on Security Technology*, Madrid, Spain, pp. 1–6, 2017. https://doi.org/10.1109/CCST.2017.8167864.
[36] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri *et al.,* "Security and privacy issues for an IoT based smart home," in *2017 40th Int. Convention on Information and Communication Technology, Electronics and Microelectronics*, Opatija, pp. 1292–1297, 2017. https://doi.org/10.23919/MIPRO.2017.7973622.
[37] J. E. Hachem, T. A. Khalil, V. Chiprianov, A. Babar and P. Aniorte, "A model driven method to design and analyze secure architectures of systems-of-systems," in *2017 22nd Int. Conf. on Engineering of Complex Computer Systems*, Fukuoka, pp. 166–169, 2017. https://doi.org/10.1109/ICECCS.2017.31.

[38] M. Hajjem, H. Bouziri, E. Talbi and K. Mellouli, "Intelligent indoor evacuation guidance system based on ant colony algorithm," in *2017 IEEE/ACS 14th Int. Conf. on Computer Systems and Applications*, Hammamet, Tunisia, pp. 1035–1042, 2017. https://doi.org/10.1109/AICCSA.2017.47.
[39] S. Krishnan, M. S. Anjana and S. N. Rao, "Security considerations for IoT in smart buildings," in *2017 IEEE Int. Conf. on Computational Intelligence and Computing Research*, Coimbatore, India, pp. 1–4, 2017. https://doi.org/10.1109/ICCIC.2017.8524450.
[40] M. A. Raja, G. R. Reddy and Ajitha, "Design and implementation of security system for smart home," in *2017 Int. Conf. on Algorithms, Methodology, Models and Applications in Emerging Technologies*, Chennai, India, pp. 1–4, 2017. https://doi.org/10.1109/ICAMMAET.2017.8186705.
[41] D. A. R. Wati and D. Abadianto, "Design of face detection and recognition system for smart home security application," in *2017 2nd Int. Conf. on Information Technology, Information Systems and Electrical Engineering*, Yogyakarta, Indonesia, pp. 342–347, 2017. https://doi.org/10.1109/ICITISEE.2017.8285524.
[42] T. Adiono, S. Harimurti, B. A. Manangkalangi and W. Adijarto, "Design of smart home mobile application with high security and automatic features," in *2018 3rd Int. Conf. on Intelligent Green Building and Smart Grid*, Yilan, Taiwan, pp. 1–4, 2018. https://doi.org/10.1109/IGBSG.2018.8393574.
[43] S. K. Bhoi, S. K. Panda, B. N. Padhi, M. K. Swain, B. Hembram *et al.,* "FireDS-IoT: A fire detection system for smart home based on IoT data analytics," in *2018 Int. Conf. on Information Technology*, pp. 161–165, 2018.
[44] M. Botticelli, L. Ciabattoni, F. Ferracuti, A. Monteriù, S. Pizzuti *et al.,* "A smart home services demonstration: Monitoring, control and security services offered to the user," in *2018 IEEE 8th Int. Conf. on Consumer Electronics*, Berlin, pp. 1–4, 2018.
[45] E. Ertugrul, U. Kocaman and O. K. Sahingoz, "Autonomous aerial navigation and mapping for security of smart buildings," in *2018 6th Int. Istanbul Smart Grids and Cities Congress and Fair*, Istanbul, Turkey, pp. 168–172, 2018. https://doi.org/10.1109/SGCF.2018.8408966.
[46] V. Haţegan, V. T. Dădarlat, A. Peculea and E. Cebuc, "Secure and extensible smart home template," in *2018 17th RoEduNet Conf.: Networking in Education and Research*, Cluj-Napoca, Romania, pp. 1–6, 2018. https://doi.org/10.1109/ROEDUNET.2018.8514145.
[47] C. C. Li, P. Wu, H. Wang, E. T. H. Chu and J. W. S. Liu, "Building/environment data/information system for fine-scale indoor location specific services," in *2018 IEEE 2nd Int. Conf. on Fog and Edge Computing*, Washington, DC, USA, pp. 1–8, 2018. https://doi.org/10.1109/CFEC.2018.8358731.
[48] P. K. Madupu and B. Karthikeyan, "Automatic service request system for security in smart home using IoT," in *2018 Second Int. Conf. on Electronics, Communication and Aerospace Technology*, Coimbatore, India, pp. 1413–1418, 2018. https://doi.org/10.1109/ICECA.2018.8474684.
[49] S. Pawar, V. Kithani, S. Ahuja and S. Sahu, "Smart home security using IoT and face recognition," in *2018 Fourth Int. Conf. on Computing Communication Control and Automation*, Pune, India, pp. 1–6, 2018. https://doi.org/10.1109/ICCUBEA.2018.8697695.
[50] L. Rafferty, F. Iqbal, S. Aleem, Z. Lu, S. Huang *et al.,* "Intelligent multi-agent collaboration model for smart home IoT security," in *2018 IEEE Int. Congress on Internet of Things*, San Francisco, CA, USA, pp. 65–71, 2018. https://doi.org/10.1109/ICIOT.2018.00016.
[51] Y. Wang, H. Lv, Q. Zhang, P. Wang, D. Yan *et al.,* "Research on smart home security system based on bp neural network information fusion," in *2018 Chinese Automation Congress*, Xi'an, China, pp. 1381–1384, 2018. https://doi.org/10.1109/CAC.2018.8623606.
[52] Y. N. Aung and T. Tantidham, "Ethereum-based emergency service for smart home system: Smart contract implementation," in *2019 21st Int. Conf. on Advanced Communication Technology*, PyeongChang, Korea (South), pp. 147–152, 2019. https://doi.org/10.23919/ICACT.2019.8701987.
[53] T. Chaurasia and P. K. Jain, "Enhanced smart home automation system based on internet of things," in *2019 Third Int. Conf. on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, Palladam, India, pp. 709–713, 2019. https://doi.org/10.1109/I-SMAC47947.2019.9032685.
[54] B. Cui, Z. Lan and X. Bai, "Research on role-based access control in IPv6 smart home," in *2019 IEEE 9th Int. Conf. on Electronics Information and Emergency Communication*, Beijing, China, pp. 205–208, 2019. https://doi.org/10.1109/ICEIEC.2019.8784596.

[55] H. Hsu, G. Jong, J. Chen and C. Jhe, "Improve IoT security system of smart-home by using support vector machine," in *2019 IEEE 4th In. Conf. on Computer and Communication Systems*, Singapore, pp. 674–677, 2019. https://doi.org/10.1109/CCOMS.2019.8821678.

[56] K. Karimi and S. Krit, "Smart home-smartphone systems: Threats, security requirements and open research challenges," in *2019 Int. Conf. of Computer Science and Renewable Energies*, Agadir, Morocco, pp. 1–5, 2019. https://doi.org/10.1109/ICCSRE.2019.8807756.

[57] V. Krundyshev and M. Kalinin, "Prevention of false data injections in smart infrastructures," in *2019 IEEE Int. Black Sea Conf. on Communications and Networking*, Sochi, Russia, pp. 1–5, 2019. https://doi.org/10.1109/BlackSeaCom.2019.8812786.

[58] V. Nguyen, H. Nguyen, Q. Huynh, N. Venkatasubramanian and K. Kim, "A scalable approach for dynamic evacuation routing in large smart buildings," in *2019 IEEE Int. Conf. on Smart Computing*, Washington, DC, USA, pp. 292–300, 2019. https://doi.org/10.1109/SMARTCOMP.2019.00065.

[59] U. Osisiogu, "A review on cyber-physical security of smart buildings and infrastructure," in *2019 15th Int. Conf. on Electronics, Computer and Computation*, Abuja, Nigeria, pp. 1–4, 2019. https://doi.org/10.1109/ICECCO48375.2019.9043207.

[60] E. Pramunanto, M. Muhtadin and W. Febrian, "Integrated smart safety home system based on wireless sensor network and internet of things as emergency preventive efforts in settlement areas," in *2019 Int. Conf. on Computer Engineering, Network, and Intelligent Multimedia*, Surabaya, Indonesia, pp. 1–7, 2019. https://doi.org/10.1109/CENIM48368.2019.8973328.

[61] H. Qusa, H. Allam, F. Younus, M. Ali and S. Ahmad, "Secure smart home using open security intelligence systems," in *2019 Sixth HCT Information Technology Trends (ITT)*, New York, US: IEEE, pp. 12–17, 2019.

[62] S. Ramapatruni, S. N. Narayanan, S. Mittal, A. Joshi and K. Joshi, "Anomaly detection models for smart home security," in *2019 IEEE 5th Int. Conf. on Big Data Security on Cloud, IEEE Int. Conf. on High Performance and Smart Computing and IEEE Int. Conf. on Intelligent Data and Security*, Washington, DC, USA, pp. 19–24, 2019. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2019.00015.

[63] J. Tang and Q. Jia, "A simulation platform for sensing system selection for occupant distribution estimation in smart buildings," in *2019 IEEE 15th Int. Conf. on Automation Science and Engineering*, Vancouver, BC, Canada, pp. 985–990, 2019. https://doi.org/10.1109/COASE.2019.8843129.

[64] T. Tantidham and Y. N. Aung, "Emergency service for smart home system using ethereum blockchain: System and architecture," in *2019 IEEE Int. Conf. on Pervasive Computing and Communications Workshops*, Kyoto, Japan, pp. 888–893, 2019. https://doi.org/10.1109/PERCOMW.2019.8730816.

[65] V. Zhmud, A. Liapidevskiy, H. Roth and J. Nosek, "The concept of a smart home: Security, additional features and augmented reality," in *2019 Int. Multi-Conf. on Industrial Engineering and Modern Technologies*, Vladivostok, Russia, pp. 1–8, 2019. https://doi.org/10.1109/FarEastCon.2019.8933841.

[66] A. K. Ray and A. Bagwari, "IoT based Smart home: Security aspects and security architecture," in *2020 IEEE 9th Int. Conf. on Communication Systems and Network Technologies*, Gwalior, India, pp. 218–222, 2020. https://doi.org/10.1109/CSNT48778.2020.9115737.

[67] V. Subbarao, K. Srinivas and R. S. Pavithr, "A survey on internet of things based smart, digital green and intelligent campus," in *2019 4th Int. Conf. on Internet of Things: Smart Innovation and Usages*, Ghaziabad, India, pp. 1–6, 2019. https://doi.org/10.1109/IoT-SIU.2019.8777476.

[68] X. Feng, Y. Wang, L. Jiang, Y. Huang and T. Li, "A survey on internet of things security based on smart home," in *2018 5th Asia-Pacific World Congress on Computer Science and Engineering*, Nadi, Fiji, pp. 84–91, 2018. https://doi.org/10.1109/APWConCSE.2018.00022.

[69] W. Ali, G. Dustgeer, M. Awais and M. A. Shah, "IoT based smart home: Security challenges, security requirements and solutions," in *2017 23rd Int. Conf. on Automation and Computing*, Huddersfield, UK, pp. 1–6, 2017. https://doi.org/10.23919/IConAC.2017.8082057.

[70] A. Jacobsson, M. Boldt and B. Carlsson, "A risk analysis of a smart home automation system," *Future Generation Computer Systems*, vol. 56, no. 1, pp. 719–733, 2016.

[71] H. M. Do, M. Pham, W. Sheng, D. Yang and M. Liu, "RiSH: A robot-integrated smart home for elderly care," *Robotics and Autonomous Systems*, vol. 101, no. 3, pp. 74–92, 2018.
[72] N. Akatyev and J. I. James, "Evidence identification in IoT networks based on threat assessment," *Future Generation Computer Systems*, vol. 93, no. 8, pp. 814–821, 2019.
[73] P. Bhoyar, P. Sahare, S. B. Dhok and R. B. Deshmukh, "Communication technologies and security challenges for internet of things: A comprehensive review," *AEU International Journal of Electronics and Communications*, vol. 99, no. 4, pp. 81–99, 2019.
[74] D. D. Furszyfer Del Rio, B. K. Sovacool, N. Bergman and K. E. Makuch, "Critically reviewing smart home technology applications and business models in Europe," *Energy Policy*, vol. 144, pp. 111631, 2020.
[75] P. P. Ray, D. Dash and N. Kumar, "Sensors for internet of medical things: State-of-the-art, security and privacy issues, challenges and future directions," *Computer Communications*, vol. 160, no. 3, pp. 111–131, 2020.
[76] L. Vadillo Moreno, M. L. Martín Ruiz, J. Malagón Hernández, M. Á. Valero Duboy and M. Lindén, "Chapter 14-The role of smart homes in intelligent homecare and healthcare environments," In: C. Dobre, C. Mavromoustakis, N. Garcia, R. Goleva, G. Mastorakis (Eds.) *Ambient Assisted Living and Enhanced Living Environments*, Oxford, United Kingdom: Butterworth-Heinemann, pp. 345–394, 2017.
[77] L. J. Fennelly and M. A. Perry, "150 things you should know about security," In: L. J. Fennelly, M. A. Perry (Eds.) *150 Things You Should Know About Security*, 2nd ed., Oxford, United Kingdom: Butterworth-Heinemann, pp. 1–218, 2018.
[78] R. Saini and D. Mishra, "Chapter 4—Privacy-aware physical layer security techniques for smart cities," In: D. B. Rawat, K. Z. Ghafoor (Eds.) *Smart Cities Cybersecurity and Privacy*, Amsterdam, Netherlands: Elsevier, pp. 39–56, 2019.
[79] W. M. Kang, S. Y. Moon and J. H. Park, "An enhanced security framework for home appliances in smart home," *Human-Centric Computing and Information Sciences*, vol. 7, no. 1, pp. 6, 2017.
[80] M. Amiribesheli and H. Bouchachia, "A tailored smart home for dementia care," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 6, pp. 1755–1782, 2018.
[81] E. Park, S. Kim, Y. Kim and S. J. Kwon, "Smart home services as the next mainstream of the ICT industry: Determinants of the adoption of smart home services," *Universal Access in the Information Society*, vol. 17, no. 1, pp. 175–190, 2018.
[82] H. Xu, L. König, D. Cáliz and H. Schmeck, "A generic user interface for energy management in smart homes," *Energy Informatics*, vol. 1, no. 1, pp. 55, 2018.
[83] M. Talal, A. A. Zaidan, B. B. Zaidan, A. S. Albahri, A. H. Alamoodi *et al.,* "Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review," *Journal of Medical Systems*, vol. 43, no. 3, pp. 42, 2019.
[84] X. Wei, T. Wang and C. Tang, "Throughput Analysis of smart buildings-oriented wireless networks under jamming attacks," *Mobile Networks and Applications*, vol. 18, no. 8, pp. 2611, 2019.
[85] D. R. dos Santos, M. Dagrada and E. Costante, "Leveraging operational technology and the Internet of things to attack smart buildings," *Journal of Computer Virology and Hacking Techniques*, 2020. https://doi.org/10.1007/s11416-020-00358-8.
[86] N. Guhr, O. Werth, P. P. H. Blacha and M. H. Breitner, "Privacy concerns in the smart home context," *SN Applied Sciences*, vol. 2, no. 2, pp. 247, 2020.
[87] S. Naoui, M. E. Elhdhili and L. Azouz Saidane, "Novel enhanced LoRaWAN framework for smart home remote control security," *Wireless Personal Communications*, vol. 110, no. 4, pp. 2109–2130, 2020.
[88] S. Naoui, M. E. Elhdhili and L. A. Saidane, "Collaborative and verifiable key derivation protocol for smart home security: CV-KDP," *Information Technology and Management*, vol. 21, no. 2, pp. 115–129, 2020.
[89] P. Tsoutsa, P. Fitsilis, L. Anthopoulos and O. Ragos, "Nexus services in smart city ecosystems," *Journal of the Knowledge Economy*, vol. 18, no. 5/6, pp. 1, 2020.

[90] F. McCreary, A. Zafiroglu and H. Patterson, "The contextual complexity of privacy in smart homes and smart buildings," in *HCI in Business, Government, and Organizations: Information Systems*, Cham: Springer, pp. 67–78, 2016.

[91] J. R. C. Nurse, A. Atamli and A. Martin, "Towards a usable framework for modelling security and privacy risks in the smart home," in *Human Aspects of Information Security, Privacy, and Trust*, Cham: Springer, pp. 255–267, 2016.

[92] R. Chowdhury, H. Ould-Slimane, C. Talhi and M. Cheriet, "Attribute-based encryption for preserving smart home data privacy," in *Enhanced Quality of Life and Smart Living*, Cham: Springer, pp. 185–197, 2017.

[93] M. Buf, B. Guerra and M. Manso, "Smart devices for automated emergency calls," in *Interoperability, Safety and Security in IoT*, Cham: Springer, pp. 27–37, 2018.

[94] P. K. Sharma, B. W. Kwon and J. H. Park, "DSS-SL: Dynamic signage system based on SDN with LiFi communication for smart buildings," in *Advances in Computer Science and Ubiquitous Computing*, Singapore: Springer, pp. 805–810, 2018.

[95] P. S. Ramya and D. Nandan, "Analysis of security issues and possible solutions in the internet of things for home automation system," in *Soft Computing: Theories and Applications*, Singapore: Springer, pp. 825–836, 2020.

[96] V. Varadharajan and S. Bansal, "Data security and privacy in the internet of things (IoT) environment," In: Z. Mahmood (Ed.) *Connectivity Frameworks for Smart Devices: The Internet of Things from a Distributed Computing Perspective*, Cham: Springer International Publishing, pp. 261–281, 2016.

[97] M. Manso, B. Guerra, C. Carjan, E. Sdongos, A. Bolovinou *et al.,* "The application of telematics and smart devices in emergencies," In: R. Gravina, C. E. Palau, M. Manso, A. Liotta, G. Fortino (Eds.) *Integration, Interconnection, and Interoperability of IoT Systems*, Cham: Springer International Publishing, pp. 169–197, 2018.

[98] R. M. Aileni, G. Suciu, M. Serrano, R. Maheswar and C. A. Valderrama Sakuyama, "The perspective of smart dust mesh based on ioee for safety and security in the smart cities," In: S. Rani, R. Maheswar, G. R. Kanagachidambaresan, P. Jayarajan (Eds.) *Integration of WSN and IoT for Smart Cities*, Cham: Springer International Publishing, pp. 151–179, 2020.

[99] R. T. Kreutzer and M. Sirrenberg, "Fields of application of artificial intelligence—Energy sector, smart home, mobility and transport," in *Understanding Artificial Intelligence: Fundamentals, Use Cases and Methods for a Corporate AI*, Cham: Springer International Publishing, pp. 195–210, 2020.

[100] D. N. Mekuria, P. Sernani, N. Falcionelli and A. F. Dragoni, "Smart home reasoning systems: A systematic literature review," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 9, pp. 2265, 2019.

[101] J. Dahmen, D. J. Cook, X. Wang and W. Honglei, "Smart secure homes: A survey of smart home technologies that sense, assess, and respond to security threats," *Journal of Reliable Intelligent Environments*, vol. 3, no. 2, pp. 83–98, 2017.

[102] H. Ai and T. Li, "A smart home system based on embedded technology and face recognition technology," *Intelligent Automation & Soft Computing*, vol. 23, no. 3, pp. 405–418, 2017.

[103] J. E. Kim, T. Barth, G. Boulos, J. Yackovich, C. Beckel *et al.,* "Seamless integration of heterogeneous devices and access control in smart homes and its evaluation," *Intelligent Buildings International*, vol. 9, no. 1, pp. 23–39, 2017.

[104] D. Choi, H. Choi and D. Shon, "Future changes to smart home based on AAL healthcare service," *Journal of Asian Architecture and Building Engineering*, vol. 18, no. 3, pp. 190–199, 2019.

[105] R. Mulcahy, K. Letheren, R. McAndrew, C. Glavas and R. Russell-Bennett, "Are households ready to engage with smart home technology?," *Journal of Marketing Management*, vol. 35, no. 15, 16, pp. 1370–1400, 2019.

[106] M. C. Chiu, W. D. Lai and C. M. Chiu, "A smart home system with security and electrical appliances," *Journal of Information and Optimization Sciences*, vol. 56, no. 4, pp. 1–17, 2020.

[107] B. Mbarek, A. Meddeb, W. Ben Jaballah and M. Mosbah, "A secure electric energy management in smart home," *International Journal of Communication Systems*, vol. 30, no. 17, pp. e3347, 2017.

[108] S. Sicari, A. Rizzardi, D. Miorandi and A. Coen-Porisini, "Securing the smart home: A real case study," *Internet Technology Letters*, vol. 1, no. 3, pp. e22, 2018.

[109] G. Zhao, L. Xing, Q. Zhang and X. Jia, "A hierarchical combinatorial reliability model for smart home systems," *Quality and Reliability Engineering International*, vol. 34, no. 1, pp. 37–52, 2018.

[110] F. Ghasemi, A. Rezaee and A. M. Rahmani, "Structural and behavioral reference model for IoT-based elderly healthcare systems in smart home," *International Journal of Communication Systems*, vol. 32, no. 12, pp. e4002, 2019.

[111] A. Ali, M. Ahmed, M. Imran and H. A. Khattak, "Security and privacy issues in fog computing," in *Fog Computing: Theory and Practice*, New York, US: IEEE, pp. 105–137, 2020.

[112] M. Wills, "Network and communications security," in *The Official (ISC)2 SSCP CBK Reference*, Mountain View, California, United States, California, United States: Coursera, pp. 467–647, 2019.

[113] P. Spachos and K. Plataniotis, "Environmental monitoring for smart buildings," in *Transportation and Power Grid in Smart Cities*, Communication Networks and Services, pp. 327–354, 2018.

[114] S. Wendzel, J. Tonejc, J. Kaur, A. Kobekova, H. Song *et al.,* "Cyber security of smart buildings," in *Security and Privacy in Cyber-Physical Systems*, Wiley, pp. 327–351, 2017.

[115] H. F. Rashvand and J. M. A. Calero, "Smart home, smart office," in *Distributed Sensor Systems: Practice and Applications*, Hoboken, New Jersey, United States: Wiley, pp. 189–219, 2012.

[116] S. Gunasingh, N. Wang, D. Ahl and S. Schuetter, "Climate resilience and the design of smart buildings," In: H. Song, R. Srinivasan, T. Sookoor and S. Jeschke (Eds.) *Smart Cities: Foundations, Principles, and Applications*, pp. 641–667, 2017. https://doi.org/10.1002/9781119226444.ch22.

[117] S. Kolhe, S. Nagpal, P. Makwana and C. Bhatt, "Smart home: Personal assistant and baby monitoring system," in *Emerging Technologies for Health and Medicine: Virtual Reality, Augmented Reality, Artificial Intelligence Internet of Things, Robotics, Industry 4.0*, pp. 259–284, 2018.