Journal of Medical Systems (2019) 43: 42
https://doi.org/10.1007/s10916-019-1158-z

SYSTEMS-LEVEL QUALITY IMPROVEMENT

Smart Home-based IoT for Real-time and Secure Remote Health Monitoring of Triage and Priority System using Body Sensors: Multi-driven Systematic Review

Mohammed Talal[1] · A. A. Zaidan[2] · B. B. Zaidan[2] · A. S. Albahri[2] · A. H. Alamoodi[2] · O. S. Albahri[2] · M. A. Alsalem[2] · C. K Lim[2] · K. L. Tan[2] · W. L. Shir[2] · K. I. Mohammed[2]

Received: 9 October 2018 / Accepted: 8 January 2019 / Published online: 15 January 2019

Abstract

The Internet of Things (IoT) has been identified in various applications across different domains, such as in the healthcare sector. IoT has also been recognised for its revolution in reshaping modern healthcare with aspiring wide range prospects, including economical, technological and social. This study aims to establish IoT-based smart home security solutions for real-time health monitoring technologies in telemedicine architecture. A multilayer taxonomy is driven and conducted in this study. In the first layer, a comprehensive analysis on telemedicine, which focuses on the client and server sides, shows that other studies associated with IoT-based smart home applications have several limitations that remain unaddressed. Particularly, remote patient monitoring in healthcare applications presents various facilities and benefits by adopting IoT-based smart home technologies without compromising the security requirements and potentially large number of risks. An extensive search is conducted to identify articles that handle these issues, related applications are comprehensively reviewed and a coherent taxonomy for these articles is established. A total number of ($n = 3064$) are gathered between 2007 and 2017 for most reliable databases, such as ScienceDirect, Web of Science and Institute of Electrical and Electronic Engineer Xplore databases. Then, the articles based on IoT studies that are associated with telemedicine applications are filtered. Nine articles are selected and classified into two categories. The first category, which accounts for 22.22% ($n = 2/9$), includes surveys on telemedicine articles and their applications. The second category, which accounts for 77.78% ($n = 7/9$), includes articles on the client and server sides of telemedicine architecture. The collected studies reveal the essential requirement in constructing another taxonomy layer and review IoT-based smart home security studies. Therefore, IoT-based smart home security features are introduced and analysed in the second layer. The security of smart home design based on IoT applications is an aspect that represents a crucial matter for general occupants of smart homes,

This article is part of the Topical Collection on *Systems-Level Quality Improvement*

✉ A. A. Zaidan
aws.alaa@gmail.com

Mohammed Talal
moha_talal2000@yahoo.com

B. B. Zaidan
bilalbahaa@fskik.upsi.edu.my

A. S. Albahri
ahmed.bahri1978@gmail.com

A. H. Alamoodi
alamoodi@outlook.com

O. S. Albahri
osamahsh89@gmail.com

M. A. Alsalem
mohammed.asum@gmail.com

C. K Lim
kim@fskik.upsi.edu.my

K. L. Tan
tankianlam@fskik.upsi.edu.my

W. L. Shir
shirli_wang@fskik.upsi.edu.my

K. I. Mohammed
khalid_ib81@yahoo.com

[1] Department of Communication Engineering, Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn Malaysia (UTHM), Parit Raja, Malaysia

[2] Department of Computing, Universiti Pendidikan Sultan Idris, Tanjong Malim, Perak, Malaysia

in which studies are required to provide a better solution with patient security, privacy protection and security of users' entities from being stolen or compromised. Innovative technologies have dispersed limitations related to this matter. The existing gaps and trends in this area should be investigated to provide valuable visions for technical environments and researchers. Thus, 67 articles are obtained in the second layer of our taxonomy and are classified into six categories. In the first category, 25.37% (*n* = 17/67) of the articles focus on architecture design. In the second category, 17.91% (*n* = 12/67) includes security analysis articles that investigate the research status in the security area of IoT-based smart home applications. In the third category, 10.44% (*n* = 7/67) includes articles about security schemes. In the fourth category, 17.91% (n = 12/67) comprises security examination. In the fifth category, 13.43% (*n* = 9/67) analyses security protocols. In the final category, 14.92% (*n* = 10/67) analyses the security framework. Then, the identified basic characteristics of this emerging field are presented and provided in the following aspects. Open challenges experienced on the development of IoT-based smart home security are addressed to be adopted fully in telemedicine applications. Then, the requirements are provided to increase researcher's interest in this study area. On this basis, a number of recommendations for different parties are described to provide insights on the next steps that should be considered to enhance the security of smart homes based on IoT. A map matching for both taxonomies is developed in this study to determine the novel risks and benefits of IoT-based smart home security for real-time remote health monitoring within client and server sides in telemedicine applications.

Keywords Internet of things · Telemedicine · Intelligent home · Remote monitoring · Smart home · Automated home · Security analysis · Security scheme · Security examination

Introduction

The Internet of Things (IoT) is a network of physical devices that are electronically embedded and are used as software sensors with network connectivity. IoT enables these devices to gather and exchange information [1]. IoT can consist of different heterogeneous layers that starts from a perception network towards the application layers [2]. Telemedicine is medical care practices that use interactive audiovisual and data communications [3, 109–112]. Telemedicine includes various points, such as medical care delivery, diagnosis [197], consultation and treatment [195], health education, electronic medical record (EMR) [115–119], medical data transfer [4, 194, 196] and ubiquitous utilisation of IoT in healthcare systems [5]. The use of IoT enables multimedia to implement deep and rich communication and interaction between patients and specialists in a remote manner and provides vast developments for the industry. The study in [6] and [7] indicated that a general three-tier pervasive telemedicine system based on a wireless body area network (WBAN) allows constant healthcare monitoring in real time. In Tier 1, vital signs are obtained by users with the use of small intelligent wireless sensors and are sent to Tier 2, which is used as the personal gateway (e.g. smartphones) based on different operating systems (e.g. android) [113, 114], in small-area networks with different protocols, such as Bluetooth, ZigBee and WBAN. Medical information is directed to healthcare providers in medical institutes (MIs) from Tier 2 to Tier 3 through wide-area wireless communication protocols or Internet services. Healthcare providers in Tier 3 apply special processes and generate services that are sent back to users as responses. Tiers 1 and 2 represent the client side that serves patients through mobile health (mHealth), whereas Tier 3 represents the server side.

Remote health monitoring system in telemedicine usually requires multiple devices to be connected. These devices include blood pressure, blood glucose, weighting, pulse, ECG and pulmonary peak flow meters [3]. A global trend has attracted wide attention in terms of smart home technology integration with the purpose of aiding health monitoring in addition to real-time care in telemedicine [8]. Psychological information of patients should be timely gathered and transferred automatically to remote specialists via network to support and aid patients with the use of smart home technologies for a real-time decent home living. This information is extremely sensitive and private; thus, most government authorities impose strict policies, such as the HIPAA Law in the United States, in the transmission of such medically related information over the network. In addition to communication security, other system security issues, such as auditing and authentication, should be considered [3]. Authentication is a necessary security service to prevent false data injection and is also required to verify a patient's identity before data access [125–151]. It is needed to secure data transfer within different applications [152–192]. Authentication, security, patient's privacy protection and data confidentiality are important for patient or doctor accessing to healthcare domain [193] and EMR [120–124]. Therefore, health data integration amongst various telehealth and telemedicine devices remains difficult and complex and hence reduces the IoT health application security.

Meanwhile, smart autonomous home is a newly emerging technology that is developed in our modern life to provide relaxation and comfortability for patients staying at their homes. However, this modern comfortable life comes with a cost, such as patient safety and privacy. The global introduction of IoT-related applications has shown a remarkable leap in the future and has attracted considerable attentions, especially in the industry and academic fields. Moreover, the importance of privacy protection has attracted the attentions of various researchers. Research plans with respect to IoT security provide great values and have been initiated. In comparison with other security mechanisms, the key management and authentication technologies of IoT are relatively mature. IoT security enhancement is a critical realisation limitation of smart visions and power-efficient homes. Thus, fundamental investigation should be conducted to understand the related risks to users/patients and critical data abuse of end users, partners and homes [9].

The aforementioned issues should be identified, and necessary means should be developed or provided in solving the security problem of IoT-based smart homes to be adopted with health monitoring technologies in telemedicine architecture. This review designs solutions to provide valuable insights in this research area. This paper consists of four sections, and each section has its own description that elaborates the steps of this systematic review. Section "Introduction" presents a comprehensive review on IoT-based telemedicine applications. The systematic review and results introduce the IoT-based hierarchical taxonomy of telemedicine architecture for remote health monitoring studies. Section "First layer: systematic review for real-time monitoring of IoT-based telemedicine applications" discusses the driven points to conduct a new mapping of a sequential review to emphasise and address the studies on the security of IoT-based smart homes and delineate the research scene from the literature to a coherent taxonomy. Section "Driven points" identifies the key aspects that describe this developing research direction. Finally, Section "Second layer: systematic review for IoT-based smart home security" summarises the conclusions of this article.

First layer: systematic review for real-time monitoring of IoT-based telemedicine applications

Method

The critical keywords in telemedicine covered in our study are 'telemedicine', 'sensor', 'triage' and 'priority'. All telemedicine-related areas and studies that are related to health domains are considered. However, our literature scope in the English language is restricted. A general study was conducted to identify the articles related to telemedicine by searching the best and most reliable databases, such as (1) Science Direct database, which provides access to journals under Elsevier Science publisher (one of the largest electronic group of science, medicine and technology and contains full-text information and references) [99, 100]; (2) Institute of Electrical and Electronic Engineers (IEEE) Xplore, which is a database of technical articles in technology and engineering [101, 198]; and (3) Web of Science (WoS), which is a database that indexes cross-disciplinary research for discovering specialised branches of fields within an academic or scientific discipline in sciences, social sciences, arts and humanities [102]. These selections cover medicinal and technical literature and provide an extensive perspective of the endeavours of developers and designers in a wide but related range of studies. The strategy used in selecting pertinent articles involves searching literature sources in two rounds. In the first round, filtering and screening are performed to exclude studies with duplicates and are unrelated to telemedicine in healthcare by reading their titles and abstracts. Then, filtering by full-text reading and screening are performed to exclude studies that are unrelated to the inclusion criteria. In the second round, filtering by accurate full-text reading of the examined articles from the first round is performed based on real-time health monitoring of IoT-based telemedicine applications. Both rounds apply the eligibility criteria in the examination process and are reviewed by the authors. Consequently, the final encompassed set is correlated to the IoT of telemedicine applications based on sensors through diverse topics (Fig. 1). Search was conducted in reliable databases, such as Science Direct, IEEE Xplore and WoS, at the end of April 2017 by using search engines, and different keywords are entered in the search bar of the explorer engine. The combinations of various keywords, including 'medical system', 'telemonitoring', 'e-health', 'telemedicine', 'telehealth', 'healthcare services', 'mHealth', 'remote monitoring', 'mobile doctor', 'triage', 'priority' and 'sensor', in various syntax of logical keywords were queried using 'AND' and 'OR' operators, as illustrated in Fig. 1. The search accepted book chapters and different types of report rather than focusing on journals and scientific conference articles because the two directions comprise recent and suitable scientific studies related to the development and creation of patterns for the IoT factors of telemedicine applications. The articles that were selected based on the criteria in Fig. 1 were included in the review. The underlying focus of mapping the scope of research on IoT factors of telemedicine applications was set to general and coarse-grained scientific classification taxonomy of two categories. The categories were obtained from a pre-overview of this study without limitations. Google Scholar engine was used to obtain a preliminary framework of the scene and directions in this study. Duplicates were eliminated by excluding articles in the two rounds because they did not satisfy the inclusion criteria [103–108]. The exclusion criteria used in the rounds are listed in Fig. 1. Each included article with its related beginning categories was identified from different sources and was assembled into a single Excel file to improve the procedures in our investigation and simplify the

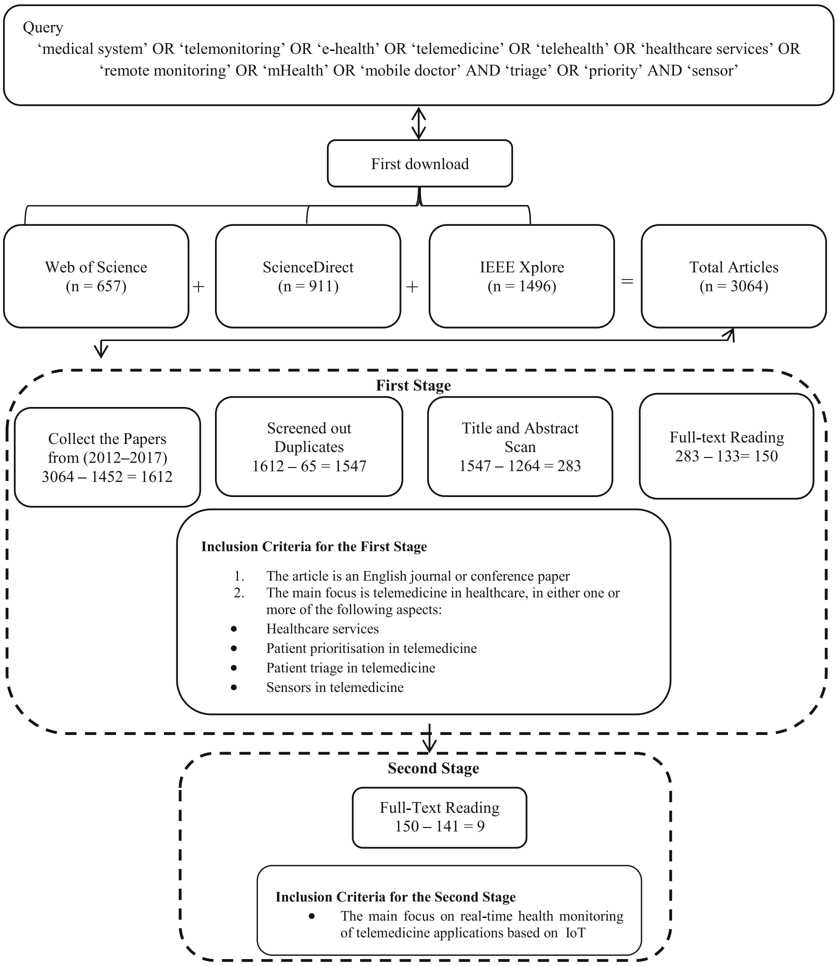

Query
'medical system' OR 'telemonitoring' OR 'e-health' OR 'telemedicine' OR 'telehealth' OR 'healthcare services' OR 'remote monitoring' OR 'mHealth' OR 'mobile doctor' AND 'triage' OR 'priority' AND 'sensor'
First download
Web of Science (n = 657)
+
ScienceDirect (n = 911)
+
IEEE Xplore (n = 1496)
=
Total Articles (n = 3064)
First Stage
Collect the Papers from (2012–2017) 3064 – 1452 = 1612
Screened out Duplicates 1612 – 65 = 1547
Title and Abstract Scan 1547 – 1264 = 283
Full-text Reading 283 – 133= 150
Inclusion Criteria for the First Stage
1. The article is an English journal or conference paper
2. The main focus is telemedicine in healthcare, in either one or more of the following aspects:
• Healthcare services
• Patient prioritisation in telemedicine
• Patient triage in telemedicine
• Sensors in telemedicine
Second Stage
Full-Text Reading 150 – 141 = 9
Inclusion Criteria for the Second Stage
• The main focus on real-time health monitoring of telemedicine applications based on IoT

Fig. 1 Explanation of the Criteria and Search Queries Adopted in the Selection of Articles for the First Layer

article classification for readers. Several full-text readings, such as contributions, objectives and comments on the surveyed studies, resulted in highlights. The articles were classified on the basis of a previous taxonomy. The entire comments and highlights were included in the body of the texts (depending on our team style, such as print-out or soft-copy versions). The main findings were described and tabulated after a summary. Word and Excel files were created to save important information, and they consisted of a list of all articles and related databases and tables of summary and details. The tables were classified on the basis of article specialisation in IoT factors of telemedicine applications. Valuable information was provided in the supplementary material as a full reference for the findings, which will be discussed in the subsequent section.

Results

The search resulted in 3064 articles, in which 1496 were from IEEE Xplore, 911 were from Science Direct and 657 were from WoS, during the period of 2007–2017. In the first round of filtering, 1612 out of the 3064 articles published from 2012 to 2017 were collected. Only 65 articles from all databases were duplicated. Subsequently, the titles and abstracts were read, which resulted in the exclusion of 1264 articles that were unrelated to our specific research topic. Thus, the result was 283 articles. Thereafter, full-text reading was performed, which led to the exclusion of 133 additional articles. The remaining 150 articles represented the final result of the first-round filtering. In the second round of filtering, the articles obtained from the previous filtering round were filtered again on the basis of the IoT factors of remote health monitoring in telemedicine applications, and ($n = 141/150$) articles were excluded after full-text filtering. Only nine articles related to IoT of telemedicine applications were obtained. These articles were thoroughly read to develop a general map of the research. Most of the articles (22.22%; 2/9 articles) comprised reviews and surveys that satisfy the current requirements by telemedicine and the importance of using IoT in telemedicine applications in future medical systems. The second group of articles (77.77%; 7/9 articles) comprised studies that contributed to IoT within real-time health monitoring of the telemedicine architecture, which involved three tiers (Tiers 1–3). Tiers 1 and 2 represent the client side, which is composed of medical sensors (i.e. ECG, BP and SpO2) connected with mHealth (i.e. laptop, smartphone and taps) to transfer the vital signs of a patient to the server side (Tier 3). The articles in this category were classified into two subsections, namely, (1) client side ($n = 1/7$ article) and server side ($n = 6/7$ articles). The general categories of the captured and re-classified articles in the literature review taxonomy are presented in Fig. 2 and can be distinguished amongst different subcategories in the general categories through the presence of overlaps.

Review

The review of articles and surveys on telemedicine aims to comprehend the current assumption and justify their requirements for future research directions on associated topics that are either not investigated or ignored. The category contains two articles. The first article [10] is a review that investigates the pipeline and state-of-the-art biosensors for blood glucose to formulate the subsequent steps. After introducing diabetes and glucose sensing, some state-of-the-art pipeline devices are analysed, especially the user friendliness and technological advancement, such as IoT. Subsequently, [11] introduced the activity recognition (AR) concept and its taxonomy and familiarises the reader with sub-classes of sensor-based AR. In addition, an overview of current health services of telecare and telehealth solutions is presented, and a hierarchical taxonomy of human behaviour analysis tasks is introduced. Fundamentally, IoT data collected in home environments are considered in this study.

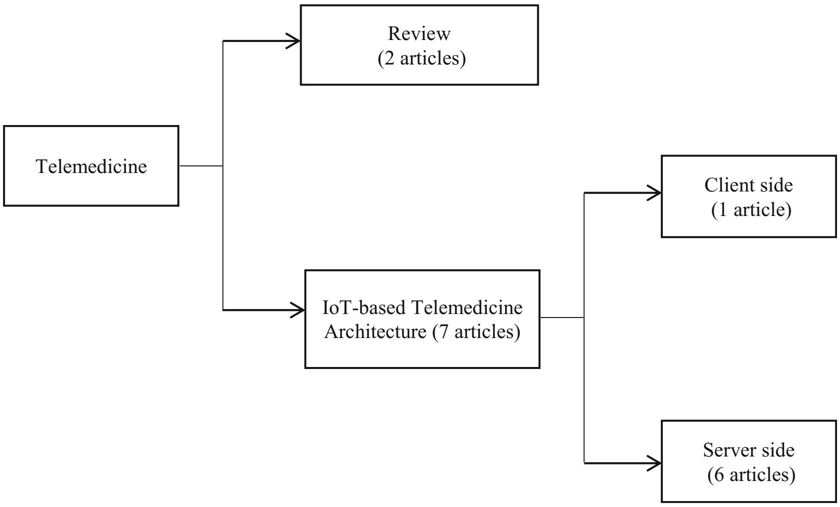
IoT-based telemedicine architecture

This category contains seven articles in two subsections, namely, client and server sides.

Client side Patients can obtain their vital signs in Tier 1 and have them sent to Tier 2 via small-area network protocols, such as ZigBee, Bluetooth and WBAN [12]. The usage of Tier 2 in the telemedicine architecture bridges sensor-based vital signs and remote stations with the aid of interfaces, such as 3G, 4G, LAN and u-health [13]. Only one article is included in this subsection. The authors in [14] utilised a strategic positioning of bridging points (i.e. gateway) at the edge of the network to provide several high-level services, such as local storage, real-time local data processing and embedded data mining, and thus presented a gateway for smart e-health. Subsequently, they applied a fog computing concept in IoT healthcare systems and formed a geo-distributed intermediary layer of intelligence between sensor nodes and the cloud.

Server side In general MIs, the provider of healthcare services enables medical professionals with the capability to monitor and analyse the vital signs in real-time and provides suitable health care services for patients. In addition, the provider manages, organises and supports medical professionals in the area of telemedicine. In general, it comprises the MI's server, patient history, database and service generation [15]. This subsection contains six articles. The authors in [16] defined several main challenges in healthcare systems that could be effectively tackled by the recent advancements in ICT technologies. Particularly, sensing technologies, cloud computing, IoT and big data analytics systems were considered emerging technologies that can improve the efficiency of healthcare services remotely from the server side. The authors in [17] focused on the application of IoT in modern systems of health care remote monitoring. An android application was developed to be utilised as the communication interface between sensors and LTE femtocell networks. In the second level, a new scheduling method based on a dynamic scheduling technique was proposed. The authors in [18] discussed the capability of IoT in the continuous integration of devices that can

Fig. 2 Taxonomy of Research Literature on the IoT of Telemedicine Applications



connect to the Internet; they also provided the information related with the state of patients' health and real-time information of assisting doctors. Their study developed an ontology-based architecture that could monitor health and provide workout routine recommendations for patients with chronic diseases. The authors in [19] utilised IoT capabilities towards the development of a people-centric sensing framework and built an intelligent system with real-time monitoring and interaction for customised healthcare of the elderly and disabled users in their homes. The authors in [20] extended the Internet of Vehicles to the healthcare domain where patients could be immediately provided with healthcare-related services. Their study extended this novel concept and referred to it as 'healthcare services "on-the-fly"'. A concept of game theory was used amongst the vehicles to acquire an access for healthcare services while travelling. A learning automaton was coupled with the proposed game theory. The authors in [21] proposed a medicine reminder and monitoring system concerned with secure health by utilising IoT with sensing element and wireless module. Open-source IoT cloud is an effective approach for data storage of sensors.

Driven points

As previously mentioned, the telemedicine architecture contains a three-tier pervasive telemedicine system [6, 7]. Tiers 1 and 2 represent the client side, whereas Tier 3 represents the server side [12, 13, 15, 22]. Our comprehensive analysis on telemedicine applications for client and server sides focuses on the studies of real-time health monitoring based on IoT. IoT applications are vast. In healthcare, various sensors attached to any number of patients in the client side transmit data about the patients to a central management console and alert the doctors and nurses when certain conditions are detected remotely from the server side. Currently, IoT and multimedia used in smart home technologies have entered the healthcare field through ambient aid living and telemedicine [3]. In healthcare, IoT has been used to follow-up on patient recovery and assess that versus a number of parameters unique to the patient by using IoT-enabled devices based on client–server architecture [11]. For most IoT-based healthcare systems, especially on smart homes, researchers have investigated the use of smart home information-based technologies in these care facilities to enhance the quality of life and safety of residents [23], and few evaluations have been conducted on IoT-based smart home security. A review of IoT-based smart home applications in our previous work was presented in [24], in which each article related to smart homes, applications and IoT until 2017 was searched. Subsequently, two related articles were published and driven the taxonomy presented in [24]. The first article was conducted in [25] to evaluate the communication components of IoT-based technologies in smart homes. The second article was presented in [26] to assess the innovative technology on intelligent processes for smart home applications that utilise IoT. Thus, an additional survey based on our previous work in [24] was constructed to review the new security techniques used for IoT-based smart homes. The use second layer provides considerable benefits in real-time remote health monitoring within the client and server sides in telemedicine applications presented in the first layer. Furthermore, the references of the taxonomy in the previous work [24] should be updated with published studies in the last two years. The complete process of the second layer will be discussed in the following section.

Second layer: systematic review for IoT-based smart home security

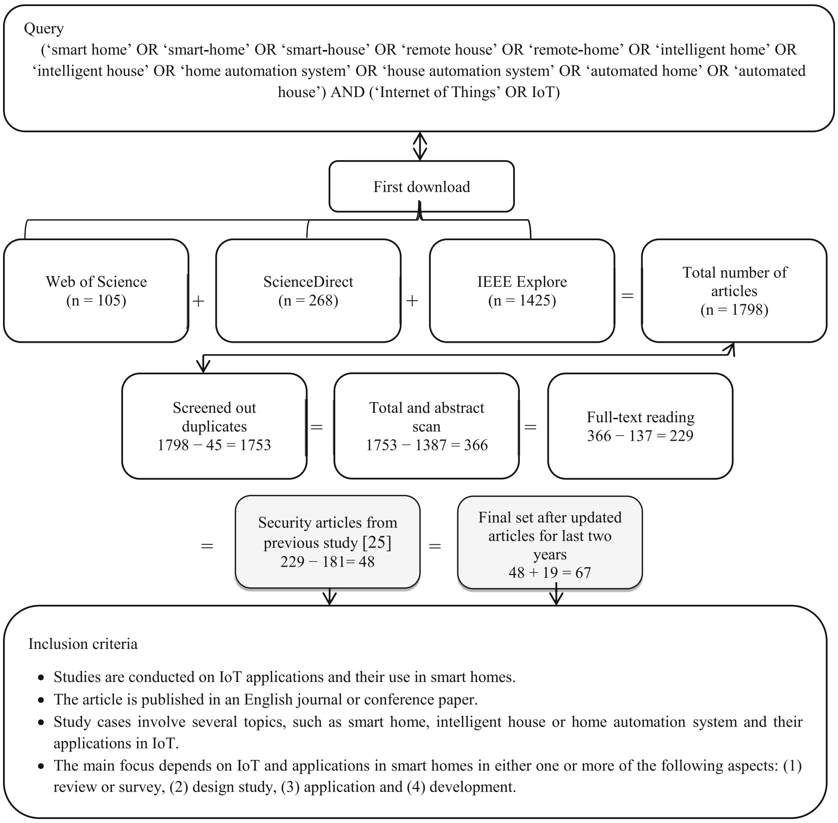
This section presents the method and result of our taxonomy design and the pattern identification of each categorised articles. This section also highlights the open concerns experienced on the security development of IoT-based smart homes. It also describes the interest of the researchers to purse the enhancement in this research area and defines the recommendations for different parties to provide a better means of development. The discussion of findings, outcomes and obstacles experienced in this study are also depicted in this section.

Method

Search was conducted on the articles collected in our previous work in [24] in 2017. The important keyword in this work is 'Internet of Things' and its applications in smart homes with direct relation to security issues. As shown in Fig. 3, 48 out of 1798 articles addressed the security aspects of smart home IoT from our previous work in [24]. Then, 19 articles were added to update the taxonomy with the studies published in the last two years. Thus, a total of 67 articles were divided to different classes based on their contents to draw a taxonomized map of the current state-of-the-art smart home IoT. Fig. 3 shows the collection procedure for the final set of articles.

Results

The result can be categorised to six different types on the basis of the specified content of each article. The taxonomy consists of 67 articles distributed amongst the following categories: development articles include 1) architecture design (17 articles, 25.37%), 2) security scheme proposal (7 articles, 10.44%), 3) security protocol (9 articles, 13.43%) and 4) security framework (10 articles, 14.92%). The remaining two categories, namely, security analysis topics (12 articles; 17.91%) and security examination (12 articles; 17.91%), describe the effort of previous works in


Query

(‘smart home’ OR ‘smart-home’ OR ‘smart-house’ OR ‘remote house’ OR ‘remote-home’ OR ‘intelligent home’ OR ‘intelligent house’ OR ‘home automation system’ OR ‘house automation system’ OR ‘automated home’ OR ‘automated house’) AND (‘Internet of Things’ OR IoT)

First download
Web of Science (n = 105)
+
ScienceDirect (n = 268)
+
IEEE Explore (n = 1425)
=
Total number of articles (n = 1798)
Screened out duplicates 1798 − 45 = 1753
=
Total and abstract scan 1753 − 1387 = 366
=
Full-text reading 366 − 137 = 229
=
Security articles from previous study [25] 229 − 181= 48
=
Final set after updated articles for last two years 48 + 19 = 67

Inclusion criteria

- Studies are conducted on IoT applications and their use in smart homes.
- The article is published in an English journal or conference paper.
- Study cases involve several topics, such as smart home, intelligent house or home automation system and their applications in IoT.
- The main focus depends on IoT and applications in smart homes in either one or more of the following aspects: (1) review or survey, (2) design study, (3) application and (4) development.

Fig. 3 Flowchart of Study Selection, Including Search Query and Inclusion Criteria for the Second Layer

investigating this area. Figure 4 shows the taxonomy of IoT-based smart home security.

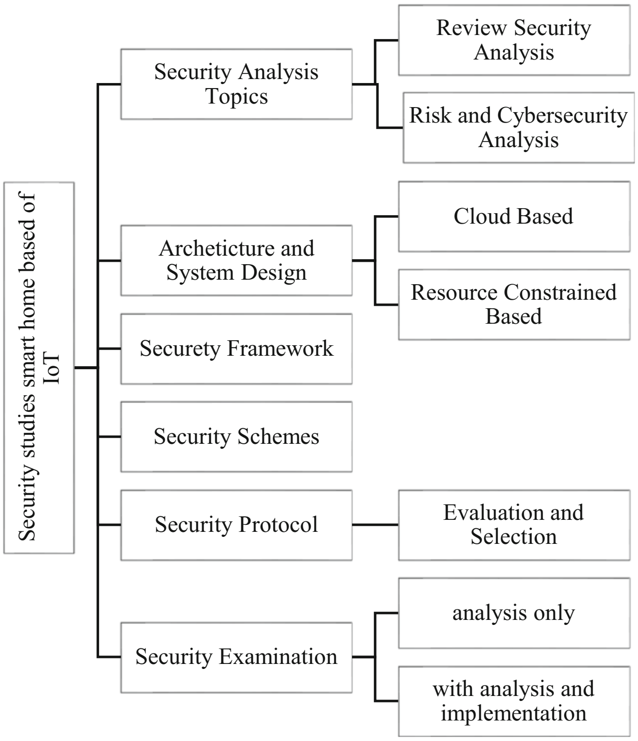


Fig. 4 Taxonomy of IoT-based Smart Home Security

Architecture Design for IoT-based Smart Homes

This section presents the taxonomy of the studies that proposed a security design for smart home IoT. Two different categories, namely, cloud-based and resource-constrained-based categories, are described in the next subsections.

Cloud based This subsection presents the studies that used cloud-based design as a resource-controlled smart device replacement to control and monitor smart home IoT. The topics of these studies can be described with a brief summary as follows. The authors in [27] used a cloud server combined with a three-level Kerberos authentication protocol to ensure the reliability of the security system design. The authors in [28] proposed a smart home system using Cloud of Things to provide additional security aspects and eliminate the resource constraints of a smart house network. In [29], the authors proposed a generic ‘service–architecture’ with DropLock platform, which provides a secure communication protocol, and described the convergence between IoT and mobile cloud computing. Furthermore, the authors in [30] contributed to smart home research by providing solutions on cloud service risk management and virtual machine contextualisation. These solutions can mitigate the challenges that might restrict any smart home device generation, especially in terms of security. A novel multilayer architecture model based on cloud was developed in [31]; the model can effectively and seamlessly interact/interoperate on heterogeneous devices/services that are provided by different IoT-based smart home vendors. A light authentication stack was proposed in [32], which was designed for IoT applications in smart homes. Cloud-connected devices in this authentication stack relays the input commands to a user's smartphone for authentication. The architecture of this model is user–device centric and handles security issues in the context of an untrusted cloud platform.

Resource constrained based This subsection presents the studies on security architecture design based on different structures to provide a security solution for smart home users. The topics of these studies can be described with a brief summary as follows.

Gateway modifications: The authors in [33] proposed an efficient and secured architecture of authorisation and authentication for IoT-based healthcare systems. The proposed system utilised a distributed smart gateway of e-health to release the medical sensors. This proposed system enabled the available IoT gateways to focus on simple tasks rather than on the challenges in authorisation and authentication. In [34], the authors designed a smart home architecture based on IoT by providing a novel and secured mechanism called the 'terminal–gateway–group system', which represents the mobile terminal, actual gateway, and sensor nodes, respectively. The safety of smart homes can reach its maximum with the cooperation amongst the sensor, network and application layers. The authors in [35] described gateway modification in establishing secure, authenticated and seamless communication between the data collected from sensors and the Internet by using a theory that utilises a middleware for achieving IoT system security reinforcement based on intelligent homes.

Access management schemes for accessing appliances remotely without user involvement: The authors in [36] presented an authentication approach for integrating identity management (IdM) from the Internet to IoT. The gateway provides the link between the two contexts; however, this gateway cannot access the message contents and acts as context parsing from the Internet to the IoT and vice versa. In [37], the authors proposed a scheme that utilises email services to notify or update users about any home access. Furthermore, [2] presented user data protection by designing a system that provides confidentiality [2]; this system is used as protection for privacy queries and authentication based on the IoT scene that is presented by designing a tailored algorithm for this purpose.

Mobile-based communication with IoT devices that use mobile applications: The authors in [38] proposed the concept of Wi-Fi-based network for smart homes. The proposed system utilised a gateway based on AllJoyn framework, where an enhanced authentication interface with Android devices is provided. The authors in [39] proposed 'hybrid applications', which are the concept of smartphone applications, on small embedded systems to increase the security details of IoT smart homes. In [40], the authors proposed a smart home with security system. An M2M system application wireless network based on mobile communication network, wireless sensor network (WSN) and the Internet was used to introduce the functionality, security mechanism, architecture, identity addressing and interfacing. Key future requirements for trusted smart home systems were identified in [41]. The gateway architecture is recognised as the most suitable device that is resource-constrained and has high system availability. Two key technologies, which aim to assist the auto-management of the system, are identified. The first technology is system auto configuration support, which enhances the system in terms of security. The second technology is automatic system update for software and firmware to maintain the security of an ongoing system operation. The authors in [42] proposed an advanced security alert system based on IoT called the alert system for smart homes. The proposed system can detect intruders or unusual activities inside a home when house owners are not around. The system requires low cost and uses a small pyroelectric infrared module and a Raspberry Pi for delay reduction during email alert process. In addition, the authors confirmed the advantages of Raspberry Pi, such as flexibility and broad usage probability.

Security review and analysis topics

This taxonomy section handles the topics that investigate the research status of smart home security IoT. The studies categorised in this section analyse the literature and provide the security issues and challenges in detail by reviewing the current researcher's effort on the security development of smart home IoT. This section is divided in two subsections as follows.

Risk and cybersecurity analysis The authors in [43] conducted an analysis and discussed the current cybersecurity implications on smart devices connected in smart homes. In [44], the authors described some security matters and corresponding keys about the sensor network, home gateway, application terminal and sensor–gateway–terminal security mechanism. The authors in [9] applied a generic risk analysis approach to evaluate threats and vulnerabilities. Furthermore, the occurrence probability and probable influence, that is, the risk exposure of the system, were presented. The authors in [45] utilised an approach based on the utilisation of virtual environments and agent-based simulation to evaluate cybersecurity solutions for the next generation of IoT applications in realistic scenarios. Particularly, the SmallWorld platform was proposed, and its effectiveness in the assessment of IoT cybersecurity concerns was illustrated via smart home applications.

Review security analysis This section addresses the studies that inspected and summarised the academic/industrial research on the security of the current state-of-the-art IoT-based smart homes. The authors in [46] presented an overview of some selected definitions combined with definition illustrations and an approach for categorising products for subsequent analysis support. Then, incident and security tests were conducted by the authors. In [47], the key techniques, security issues and critical threats in smart home networks were discussed. The authors in [48] conducted an analysis on the security challenges of IoT architecture layers. Furthermore, good suggestions were provided to improve the power of IoT technologies. The authors in [25] presented several solutions that can be utilised to overcome some IoT issues in smart homes combined with the challenges and issues experienced by smart homes that utilise IoT. In [49], the authors discussed the recent achievements on privacy and security of smart homes. Furthermore, the key observations and results were outlined by utilising a case study that involved risk analysis on automated smart home systems. In [50], the authors presented a classification of attacks from various networks related to IoT. The classification distinguished common and specific attacks from every network and used certain criteria, such as security attributes, congestion and disturbance. In addition, some current security solutions were presented in detail to reveal the security requirements towards IoT protection. In [51], the authors analysed three forms of IoT security, namely, (i) communication, (ii) application interface and (iii) data security. They reviewed the current IoT technologies, approaches and models; found the security gap in existing communication technologies, application interfaces and data security; and provided an overview of the related works in IoT. The authors in [52] conducted a comprehensive survey on existing IoT technologies and their security issues. They focused on smart homes and city environments and discussed potential IoT security solutions to improve the latter. These security solutions not only focused on the security issues of today's endpoint devices but also anticipated future attacks on data protocols and connectivity.

Security scheme proposals

This taxonomy section presents the studies that suggested a security solution for smart home IoT. The proposed security solution in these studies provides a promising development that requires to be investigated to provide a complete security solution. The topics of these studies can be described with a brief summary as follows. In [53], the authors proposed smart home system security requirements that reflect the IoT environmental characteristics. The authors in [54] proposed an IHSS using IoT devices based on agent. The proposed system design was able to monitor the sensors and independently control the actuators in constructing security services. They described their IHSS design and some prototype systems. The authors in [55] attempted to supply some secured authentication and access control solutions for 'thing' discovery. Furthermore, they presented a full description of the prototype, early performance evaluation result and its deployment in smart homes. The authors in [56] suggested a dynamic, energy-efficient authentication scheme for IoT (DAoT). DAoT utilised a feedback control scheme in dynamically selecting an energy-efficient authentication policy. IoT devices that have limited resources can be safely connected because DAoT finds the best cost-effective authentication mechanisms. The authors in [57] proposed an approach based on CP-ABE called 'fine-grained access control scheme', which is suitable for cloud–IoT paradigm. The scheme migrates the decryption and CP-ABE encryption to the cloud side and remarkably minimises the computation costs of IoT. In [58], the authors reviewed authentication usability by utilising a one-time password (OTP) for IoT. Furthermore, they proposed a scalable, robust and efficient scheme of OTP. The proposed scheme utilised 'lightweight identity-based elliptic curve cryptography' scheme principles and Lamport's OTP algorithm. In [59], two novel designs of multipath Onion and split-channel Onion IoT gateways were presented. The first design implemented a customised multipath routing protocol in Tor to construct a multi-circuit anonymous tunnel between the user and the Onion gateway. The second scheme split the command and data channels.

Security examination

In this section, we address the security of smart home IoT by describing the studies that conduct security assessment on smart home IoT. The section is divided in two subsections as follows.

Security examination with analysis only This section describes the studies that conducted security examination by analysing smart home IoT design properties, architecture and protocols and by evaluating their practicality in terms of security. These studies could not provide a security solution to address the weakness of possible vulnerable scenarios that could compromise the privacy and security of smart home users. The topics of these studies can be described with a brief summary as follows. In [60], information leakage inseparable to the techniques and their probable influence on users' privacy in the context of smart home were investigated. The authors demonstrated the mechanism of visiting a website through a smartphone by utilising some machine learning and pattern checking methods to spy the encrypted traffic. The authors in [61] evaluated the security of smart home IoT and adopted an advanced malware method named 'feature-distributed malware'. A review summary was presented in [62] for possible threats (e.g. vulnerability) combined with their critical influence and occurrence probability. The authors in [63] used industrial and commercial IoT devices as cases where the network, software and hardware were analysed in terms of security. In [64], the authors investigated and illustrated various protocols by emphasising their security status. For instance, Constrained Application Protocol (CoAP) was evaluated in terms of its implementation, architecture, security and specifications. The authors in [65] assessed the influencing factors that affect smart home users in China. The adoption of old technologies was extended by including variables associated with users' utilisation of techniques, such as secure environment realisation of smart homes, compatibility, perceived technological security, social influence, cost and risk. The result was uncertain because only the probability of the selected factors was indicated. In [66], a case study on a smart plug system of a known brand was conducted by utilising its communication protocols and by successfully launching four attacks, namely, device scanning, brute force, spoofing and firmware attacks. The study also presented the guideline for securing smart plugs. In [67], traffic analysis attack on smart homes was conducted to obtain a privacy-preserving traffic obfuscation framework, where adversaries intercept the Internet traffic from/to the smart home gateway and profile residents' behaviours through digital traces.

Security examination with analysis and invention This section presents the studies in which their practicality was evaluated in terms of security. Issues and challenges were identified by the authors in their procedure. Then, solutions that aid to decrease the gap with these issues were provided. The topics of these studies can be described with a brief summary as follows. The authors in [68] presented an instinctive approach of privacy management that can detect, measure and preserve the privacy of smart data metre before sharing it with various third parties with full awareness of irregular human activities to individual privacy. The authors in [69] presented a solution in identification and blocking of threats on a network level. They utilised a third-party architecture where specialists provide 'security-as-a-service', open-source SDN platform for prototyping and protection evaluation of multiple devices in smart homes. A case study of 'proof-of-concept' based on a smart house was presented in [70]. The proposed modifications were applied to a 'danger-based deterministic dendritic cell algorithm' to demonstrate the application of a responsive artificial immune system (AIS) for system protection. The authors in [71] proposed a secure appliance scheduling for flexible and efficient energy consumption for smart home IoT and developed a homomorphic encryption-based alternating direction method of multipliers approach to solve the cost-aware appliance scheduling optimisation in a distributed manner and schedule home appliances without leaking users' privacy.

Security protocol

This section describes the studies that proposed security protocols for smart home IoT. The proposed protocols vary based on their functionalities. The topics of these studies can be described with a brief summary as follows. The authors in [72] enhanced a security protocol by proposing a hash algorithm of IoT devices that can securely send messages between them to ensure confidentiality and integrity. In [73], the authors proposed a new protocol by integrating various trust establishment techniques, and physical unclonable functions (PUFs) were recognised as the auspicious replacement that utilise the physical properties of current devices. The authors combined these techniques with physical key generation to obtain encryption and authentication services with wireless communication that influences the physical properties of communication channels. The authors in [74] constructed a protocol where the downloaded IP is kept confidential although the target device is infected with malware and cooperates with a man-in-the-middle attack. The authors in [75] presented a protocol with three bootstrap phases of unnatural devices in a network of IPv6-based wireless sensors and CoAP. In [76], the authors proposed a management platform distributed-based architecture altered from the Simple Network Management Protocol. In [77], Datagram Transport Layer Security (DTLS) protocol associated with the frequently utilised Transport Layer Security (TLS) protocol was employed. The study illustrated that DTLS is an acceptable alternative to TLS in data streaming through Internet from connected WSNs. The authors in [78] developed a lightweight authentication protocol for IoT-enabled devices in a distributed cloud computing environment. Their study identified the security vulnerabilities in multi-server cloud environment proposed by Xue et al. and Chuang et al. Another architecture that is abdicable for distributed cloud environment and based on the authentication protocol using smartcard was proposed. The differences in security and privacy issues were analysed by [79], and these issues were related to smart home systems, smart grids and WSNs. Moreover, solutions that can preserve privacy during the communication among end sensors, appliances and the controller were proposed. In [80], the authors designed an AMQP communication protocol with the existence of a data queuing scheme. All communication processes were encrypted via RSA and AES encryption algorithms to ensure security while storing the database in MySQL RDBMS. Table 1 shows the security protocol evaluation illustrated in this section for further discussion.

The explanation of each criterion is as follows.

- **Method of evaluation in security protocol:** The responsibility of evaluation components depends on their performance over the evaluation of security protocol based on simulation results. Suitable performance metrics, such as

Table 1 Security protocol evaluation

Reference	Method of evaluation	Protocol complexity	Encryption algorithm			Performance		Compatible	Applicability	Implementation cost	Security type		
			Type	Key length	Complexity	Execution time	Power consumption				Availability	Confidentiality	Integrity
[72]	Compared with other algorithms		Hash	128 bits	√	√	√					√	√
[73]	Using generalised architecture of smart home IoT		Hash				√			√		√	√
[74]	Attack model		Symmetric			√	√					√	√
[75]	Not mentioned		Symmetric ciphers									√	√
[76]	Via an experiment that involves several software and hardware implementations		AES				√						
[77]	Not mentioned					√						√	√
[78]	By comparing various parameters	√	Hash	128 bits		√		√	√				
[79]	Not mentioned		Hash			√				√		√	√
[80]	Not mentioned		RSA and AES				√		√				
Total number of articles = 9	5	1	9	2	1	5	5	2	2	2	0	6	6
Percentage	55.55%	11.11%	100%	22.22%	11.11%	55.55%	55.55%	22.22%	22.22%	22.22%	0%	66.66%	66.66%

algorithm encryption complexity, packet loss rate, communication overhead, handover delay and throughput, should be determined in advance [81].

- **Protocol complexity:** Protocol complexity is identified based on its role in measuring the required effort towards conducting the study, and is an essential component to guarantee its success from various perspectives, such as scientific, execution and financial planning. Protocol complexity is mainly specified by the number/frequency and/or the complexity of individual procedures that are required in the study [82].
- **Encryption algorithm:** A mathematical related procedure is utilised for data encryption. Information is transformed into incomprehensible elements, such as cipher texts, by using a specific algorithm, which require the use of a key to transform them to their original state. Different examples for such algorithms, include AES, Blowfish, RC$, RC5 and RC6 [83].
- **Performance:** This criterion can be generally defined as the working stability of the device over a period of time.
- **Compatible**: This criterion ensures that all devices with IoT are well-matched with each other and can be connected to different types of device that are provided by different vendors.
- **Implementation cost:** The required expenditures to install and commission a connection protocol and any other services that should be implemented to ensure the efficiency of this protocol.
- **Confidentiality:** In information security, confidentiality 'is identified as the property that information is not made available or disclosed to unauthorised individuals, entities or processes' [84]. Although similar to 'privacy', the two words are not interchangeable. Rather, confidentiality is a privacy component that is implemented to protect data from unauthorised viewers. Examples of confidentiality of electronic data that are compromised includes laptop theft, password theft or sensitive emails sent to wrong people [85].
- **Integrity:** In information security, data integrity is defined as maintaining and ensuring the completeness and accuracy of data over their entire lifecycle. [86] It indicates that data cannot be modified in an unauthorised or undetected manner. Data integrity is different from referential integrity in databases, although it can be viewed as a special case of consistency as understood in a classic ACID model of transaction processing. Information security systems typically provide message integrity and data confidentiality.
- **Availability:** Information must be available when required for any information system to function in its intended means and serve its purpose. This condition indicates that computing systems store and process the information, security controls protect them and communication channels used to access them must be functioning correctly. High-availability systems remain available at all times and prevent service disruptions due to power outages, hardware failures and system upgrades. Ensuring availability involves the prevention of denial-of-service attacks, such as a flood of incoming messages to the target system by essentially forcing it to shut down [87].
- **Discussion and conclusion for security protocol evaluation in** Table 1**:**

As shown in Table 1, several criteria are used to provide the most suitable smart home secure communication protocol, which attempts to be compatible with the confidentiality, availability and integrity (CIA) triad model and guides policies for information security within IoT. The mentioned criteria should be employed during the evaluation of the proposed protocols to assess how these studies fulfil the CIA triad model requirements. However, no study in Table 1 addressed all these criteria to achieve high security level for IoT-based smart homes. Only 55.55% (5/9) of the studies provided the evaluation method of their protocol. Only one study [11.11% (1/9)] attempted to cover protocol complexity; whereas 100% (9/9) used an encryption algorithm, most of which used a hash algorithm with 128-bit key length whereas others used either RSA or AES algorithm. The complexity of encryption algorithms is addressed in only one study 11.11% (1/9). The performance evaluation with its first and second sub-criteria (i.e. execution time and power consumption) is measured in 55.55% (5/9) of the studies. A total of 22.22% (2/9) of the studies analysed the compatibility, applicability and implementation cost criteria and attempted to adapt their protocols with these criteria.

In comparison with the previous studies that proposed smart home protocols, IoT security is a special challenge that is frequently unpatched and configured with default or weak protocols. Given that many protocols with the capacity to be networked are developed, the above criteria should be considered in protocol development to achieve the CIA triad model requirement. In this context, the results of the studies that achieved the crucial components of triad elements are weak, representing 0% availability and 66.66% (6/9) confidentiality and integrity.

Security framework

This section describes the studies that defined the steps and procedures for obtaining a clear security solution to improve smart home IoT security. The topics of these studies can be described with a brief summary as follows. In [88], the design and implementation of a framework with an efficient secured heterogeneous WSN data transmission of IoT was illustrated. The authors in [89] designed a software framework called ' heterogeneous network interconnection embedded gateway,' which can interconnect various heterogeneous networks. Firstly, the software was provided, and the structure of main data was then introduced with the Internet data format of client side and tables of information record. Finally, a detailed discussion on the main modules of the software was presented. Several characteristics of this gateway, such as instantaneity and customisable modularisation, were illustrated. In [90], the authors presented a BlinkToSCoAP framework by integrating three software libraries and by implementing lightweight CoAP, Internet Protocol version 6 (IPv6) over Low-power Wireless Personal Area Network (6LoWPAN) and DTLS protocols over TinyOS. They proposed a toolkit based on the security model in [91]. A management framework was utilised to integrate this toolkit for IoT devices. Furthermore, an efficient, supported security evaluation of security policies was conducted to enable user data protection. The design and implementation of 'synthetic packet-injection framework' was presented in [92]. This framework was utilised to mitigate the challenges by making the traffic analysis complicated to be utilised by attackers. With the absence of a channel encryption, a security approach based on applications was developed to prevent any sort of private data manipulation, as described in [93]. An IoT security framework was presented by [94], which was designed for smart infrastructures, such as smart homes and smart buildings and features a general threat model to be used for developing a security protection methodology for IoT services against known or unknown cyberattacks. The authors in [95] proposed a secure IFTTT-based smart home framework that incorporates suitable captcha-based OTP authentication scheme and PUF. In [96], the authors investigated and outlined the different core components and functions of the smart home tier. Every smart home was equipped with an always online, high-resource device known as the 'miner'. The miner device is responsible for handling all communications within and external to the home. The miner also preserves a private and secure BC and is used for controlling and auditing communications. The authors in [97] proposed a modelling framework that aids in IoT security; the framework consists of five phases, namely, data processing, security model generation, security visualisation, security analysis and model updates. The framework is used to determine the possible attack scenarios in IoT and analyses its security via well-defined security metrics. The framework assesses the effectiveness of various defence strategies. Table 2 displays the security framework evaluation illustrated in this section for discussion.

The framework evaluation criteria are explained as follows.

- **Performance:** Generally, this criterion can be defined as the working stability of the device over a period of time.
- **Memory footprint:** The memory footprint of different frameworks of IoT smart home applications is provided by using a software tool, such as the GCC MSP430 Toolchain, which displays the total ROM and RAM bytes written during the phase of device programming [90].
- **Packet overhead:** Packet overheads are calculated by using a wireless packet sniffer board interfaced to a Linux system that runs the Wireshark packet analyser software. This device is used to capture packets, such as handshake messages. A software tool, such as Wireshark, can parse captured data to differentiate between different protocol headers, thereby providing access to all their fields, size and effective DTLS header dimension [90].
- **Latency:** Time measurement for packet transmissions are events that occur either before or after CPU-intensive time periods. The length details of each handshake message should be specified. The CoAP adds a total overhead of 17 bytes per frame, whereas DTLS protocol adds 29 bytes [90].
- **Energy consumption:** Energy consumption of the employed hardware platform is acquired by conducting experimental measurements of voltage across a current sensing resistor placed in series with the IoT smart home board and power cable utilised as power supply. A digital storage oscilloscope can be used to measure the power consumed by each device in the IoT smart home network. The performance factors should be considered during the design of IoT system while introducing end-to-end security [90].
- **Reliability:** Generally, reliability is identified as the attribute for any computer-related component, such as software, hardware or network that continuously operates based on its specifications.
- **Complexity:** The complexity of a protocol is defined as the maximum (overall inputs) of the average message length [98].
- **Network type:** A guide to explain the types of network used in the articles includes either heterogeneous or homogeneous WSNs.
- **Discussion and conclusion for security framework evaluation in** Table 2**:**

Several IoT frameworks can be evaluated based on the above criteria to secure smart infrastructures, such as smart homes, and apply mitigation strategies. Table 1 shows the architecture criteria that can be used to guide the security development of IoT smart infrastructures. These frameworks are supposed to secure the smart home environment against the existing malware attacks and enhance the usage and utility to support automation and upgrade of living in large scale.

Although these frameworks adopted different criteria, remarkable correlations are observed between the number of sensor nodes and security type in terms of network scalability. Scalability approach should easily scale to any number of agents. However, IoT frameworks have been proposed to

Table 2 Security framework evaluation

Reference	Protocol	Network type		Categories of sensors			Number of sensors (nodes)	Evaluation method	Complexity	Reliability
		Heterogeneous WSN	Homogeneous WSN	Movement sensors	Physiologic sensors	Contextual sensors				
[88]	ZigBee	√			√		>30	Proposed simulator	√	√
[89]	ZigBee	√			√		n/a			
[90]	DTLS, CoAP and 6LoWPAN	√			√		2	Four performance metrics		
[91]	Packet Data Protocol	√			√		2	Policy Enforcement Point		
[92]	ZigBee	√				√	2	Attack scenario		
[93]	HTTPS, FTP and IP	√		√	√	√	10	GET over HTML-protocol		
[94]	ZigBee wireless protocol	√			√		1 and 9 but in WSN with 1000	Three scenarios	√	√
[95]	Universal Authentication Framework and Universal Second Factor	√			√		n/a	Adversarial model		
[96]	6LoWPAN and IPv6	√			√	√	5	Scenario in Cooja simulator		
[97]	ZigBee	√			√		n/a	Evaluation tool (SHARPE) for three scenarios	√	√
Total number of articles = 10	10	10		10			7	9	3	3
Percentage	100%	100%		100%			70%	90%	30%	30%

Reference	Cost	Performance				Security type		
		Memory footprint	Energy consumption	Latency	Packet overhead	Availability	Confidentiality	Integrity
[88]					√			
[89]					√			
[90]		√	√	√	√			√
[91]		√	√	√	√		√	
[92]							√	
[93]			√	√		√	√	√
[94]	√						√	√
[95]	√				√			
[96]			√		√	√	√	√
[97]	√							
Total number of articles = 10	3	2	4	3	6	2	5	4
Percentage	30%	20%	40%	30%	60%	20%	50%	40%

experience general challenges, such as heterogeneity, and scalability still has major challenges in each of these aspects. Thus, 70% (7/10) of the studies mentioned the number of sensors within the proposed frameworks and most of them adopted various types of sensor without considering scalability. The heterogeneity of IoT network type, the categories and large number of nodes and the different types of protocol provided important challenges in this context. Particularly, scalability, interoperability, trust and privacy requirements are difficult to address, although considerable amounts of existing frameworks are found in the research and standardisation community. The number of sensors has a wide range of variation in the visualisation within the network architecture. This condition emphasises the question about network scalability. The increase in the number of different types of sensors requires the application of many intense security measures (e.g. encryption algorithm and reliable protocol) and leads to the argument between network performance and security because most of the sensors are light and resource constrained.

In addition, many different types and methods of evaluation are mentioned based on the information required to be assessed that are represented by 90% (9/10) of the studies. Thus, complexity, reliability and cost are only mentioned in 30% (3/10) of the studies based on the diversity of these evaluation methods. The problems include insufficient relevance of performance evaluation (especially memory footprint 20% (2/10)), 40% (4/10) of the studies represent energy consumption, and 30% (3/20) represents latency. The performance shows that the lack of effective processes is a barrier to the evolution of its original performance measurement frameworks. A secure framework requires authentication and identity security based on the CIA triangle [93], and the weaknesses addressed in availability, confidentiality and integrity represent 20% (2/10), 50% (5/10) and 40% (4/10) of the studies, respectively.

Open challenges

IoT-based smart homes are still limited in their capability to provide full security and privacy for normal users. Many researchers have elaborated their concerns about the current security challenges faced by the automation systems of IoT-based smart homes. This subsection elaborates the gaps and problems that require solutions to enhance the security of smart home IoT. The identification of these problems represents the first step of keeping users safe and ensuring their privacy. Figures 5a and b show the summarised points of security concerns. The problems are categorised in 16 subsections based on their nature depicted with their cited references to enable the readers to find the detailed description of these issues.

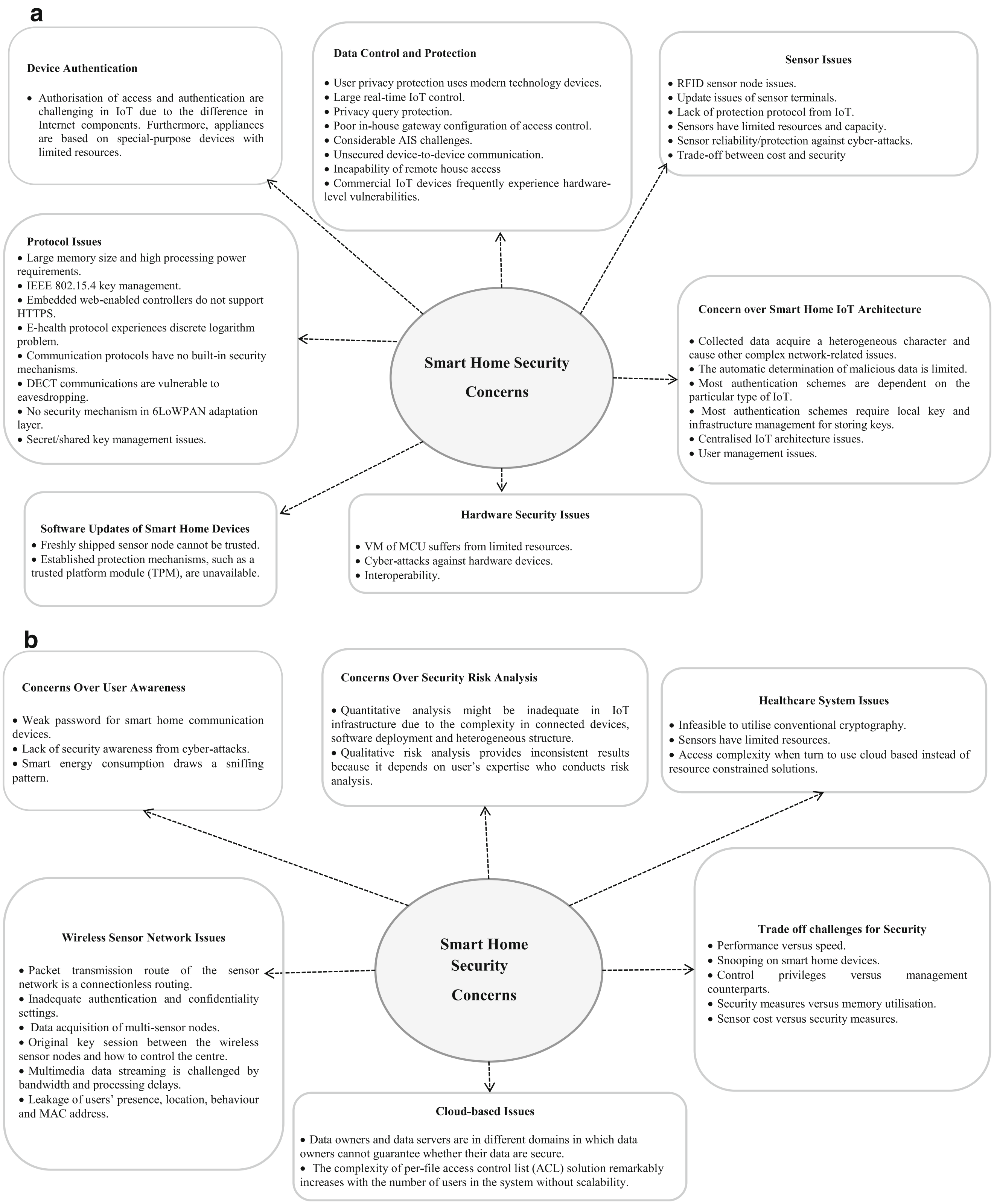
Concerns about device authentication

Authorisation of access and authentication are challenging in IoT due to the difference in Internet components. Furthermore, appliances are based on special-purpose devices with limited resources. An IdM system grants authorisation of access and authentication for Internet users. However, the integration of Internet IdM with IoT is challenging due to the limitations of IoT appliances. The appliances are based on special-purpose devices with limited resources, and a lack of communication security exists between the Internet and IoT, such as authentication mechanisms, difference in protocol stack and public key infrastructures [10, 36]. The end-to-end authentication establishment amongst the applications and devices in IoT is a challenging issue. The available authentication mechanisms are currently vulnerable to security threats due to their heterogeneity from communication, security protocols, topology and IoT devices [58].

Concerns about control and protection

The research problems addressed by authors in [91] are expressed as follows. (1) A validation of users' privacy and security requirements is achieved with the IoT evolution over the Internet. (2) The confidence level between IoT and users can be measured. IoT increases the interaction between the digital and real worlds compared with the Internet. The amount of collected data from IoT sensors is remarkably larger than that of the Internet, and the collected data are completely detailed and correspond to daily human activities. Critical privacy issues might emerge in this data flow, and the data flow should be effectively monitored and controlled to protect data privacy and overcome these issues. The authors in [41] presented particular challenges to security and privacy. In addition, privacy query protection was reported in [2]. Privacy query is recognised as the query and mining of critical information. Privacy query protection is considered a privacy protection issue in data processing, and privacy protection requires privacy technology assurance. Furthermore, a major security challenge is identified with the diverse and dynamic utilisation of resources. Traditional IT security solutions are not suitable to IoT. Multiple access points for devices can be utilised as means to overcome existing vulnerabilities, and some IoT devices and services can be shared and can have different aspects, such as ownership, policy and connectivity domains [94].

Inadequate access control might cause a critical risk to the consequent processed data in in-house gateways [62]. Device-to-device communication technology is unsecured and requires consecrated communicating servers between the end devices and the client. Furthermore, the granting of access to industries and houses remains unresolved and mainly relies on users' presence at home. Real-time monitoring systems do not



a

Smart Home Security Concerns

Device Authentication

- Authorisation of access and authentication are challenging in IoT due to the difference in Internet components. Furthermore, appliances are based on special-purpose devices with limited resources.

Data Control and Protection

- User privacy protection uses modern technology devices.
- Large real-time IoT control.
- Privacy query protection.
- Poor in-house gateway configuration of access control.
- Considerable AIS challenges.
- Unsecured device-to-device communication.
- Incapability of remote house access
- Commercial IoT devices frequently experience hardware-level vulnerabilities.

Sensor Issues

- RFID sensor node issues.
- Update issues of sensor terminals.
- Lack of protection protocol from IoT.
- Sensors have limited resources and capacity.
- Sensor reliability/protection against cyber-attacks.
- Trade-off between cost and security

Protocol Issues

- Large memory size and high processing power requirements.
- IEEE 802.15.4 key management.
- Embedded web-enabled controllers do not support HTTPS.
- E-health protocol experiences discrete logarithm problem.
- Communication protocols have no built-in security mechanisms.
- DECT communications are vulnerable to eavesdropping.
- No security mechanism in 6LoWPAN adaptation layer.
- Secret/shared key management issues.

Concern over Smart Home IoT Architecture

- Collected data acquire a heterogeneous character and cause other complex network-related issues.
- The automatic determination of malicious data is limited.
- Most authentication schemes are dependent on the particular type of IoT.
- Most authentication schemes require local key and infrastructure management for storing keys.
- Centralised IoT architecture issues.
- User management issues.

Software Updates of Smart Home Devices

- Freshly shipped sensor node cannot be trusted.
- Established protection mechanisms, such as a trusted platform module (TPM), are unavailable.

Hardware Security Issues

- VM of MCU suffers from limited resources.
- Cyber-attacks against hardware devices.
- Interoperability.

b

Smart Home Security Concerns

Concerns Over User Awareness

- Weak password for smart home communication devices.
- Lack of security awareness from cyber-attacks.
- Smart energy consumption draws a sniffing pattern.

Concerns Over Security Risk Analysis

- Quantitative analysis might be inadequate in IoT infrastructure due to the complexity in connected devices, software deployment and heterogeneous structure.
- Qualitative risk analysis provides inconsistent results because it depends on user's expertise who conducts risk analysis.

Healthcare System Issues

- Infeasible to utilise conventional cryptography.
- Sensors have limited resources.
- Access complexity when turn to use cloud based instead of resource constrained solutions.

Wireless Sensor Network Issues

- Packet transmission route of the sensor network is a connectionless routing.
- Inadequate authentication and confidentiality settings.
- Data acquisition of multi-sensor nodes.
- Original key session between the wireless sensor nodes and how to control the centre.
- Multimedia data streaming is challenged by bandwidth and processing delays.
- Leakage of users' presence, location, behaviour and MAC address.

Trade off challenges for Security

- Performance versus speed.
- Snooping on smart home devices.
- Control privileges versus management counterparts.
- Security measures versus memory utilisation.
- Sensor cost versus security measures.

Cloud-based Issues

- Data owners and data servers are in different domains in which data owners cannot guarantee whether their data are secure.
- The complexity of per-file access control list (ACL) solution remarkably increases with the number of users in the system without scalability.

Fig. 5 **a** Challenges of IoT-based Smart Homes. **b** Challenges of IoT-based Smart Homes allow owners to control the access to their house remotely. In addition, some systems, such as remote surveillance systems do not provide the essential information and filtration of critical adversary. House control access mainly depends on middleware services to grant permissions [37].

Few devices that add security protection frequently use software-level solutions. However, these solutions do not consider the usage pattern differentiation that IoT devices have when they are competed with traditional embedded systems or personal computers. This condition proves the insufficiency of these mechanisms that are bypassed and software-level protection schemes. These protection schemes unintentionally leave the hardware vulnerable, which allow for new attack vectors. The security features of commercial IoT devices are usually added in an ad hoc manner where remote attacks are addressed as main threats. Therefore, IoT devices in the commercial sector are usually prone to hardware-level vulnerabilities that may be remotely utilised [63].

The development of AIS fits the IoT security protection and maintenance from two perspectives. Firstly, the characteristics of security problems are ideal for AIS due to the powerful connection between the required properties of AIS and for suitable security system design. These characteristics are error tolerance, decentralisation, robustness, lightweight embedded computation and adaption. Secondly, an interesting challenge is provided on new AIS development with the definition of scenario for AIS testing [70].

A typical AIS design should have secured IoT. However, available AISs have huge limitations because immune-inspired algorithms, which are previously utilised for secured computers, are focused on attack detection. However, no automated detection responses are reported in threat detection. Thus, the developed responsive AIS can automatically respond during detection [70].

Concerns related to sensors

In home sensor networks, especially WSNs, the prominent security issue is mainly the security issues of sensor nodes because the information must be collected and transmitted by the nodes. Sensor nodes are miniature devices that have a simple function, which limits their computing power, storage capacity and communication capability. Thus, a complex security agreement against DOS attacks is difficult to design. Packet data are easily lost or confused through their transmission when a sensor node produces inaccurate or false data due to dysfunction. An intruder may increase its own nodes, enter false data and plug the message transmission in the sensor network. The false node that has a strong computing power can pretend to be a sensor node. The intruder can control the sensor nodes and obtain the transmission message through the nodes when a captured sensor node is compromised (e.g. communication between nodes within the sensor network and the shared key of telemetric platform) [44]. Specifically, some rising issues and challenges, such as data storage, scalability, energy saving and data processing capability, are observed in environments with heterogamous resources [29].

Currently, security breaches and threats have increased with the number of IoT devices because the generic nodes of sensors cease from seasoned security measures and intense resources. Sensor terminal-related security problems in IoT comprise access and imitation of air interface information, duplication of SIM information, unauthorised access and theft or damage of confidential information. Furthermore, data are collected from multiple sensor nodes, which will be transmitted to the processing unit and reach the users or applications [48, 74].

The physical layer of smart home IoT mainly experiences different issues, including security of acquiring information and physical hardware, such as sensor terminals, RFID nodes and sensor devices. A single security protocol for IoT cannot be achieved due to of the functionality of various sensor nodes that have poor protection systems. Hence, a lack of appropriate arrangements of security approaches might affect the security of routers, sensor terminals, WSNs and RFID sensor nodes. RFID sensor nodes have high vulnerability level to theft or damage, especially when they are utilised in severe environments. Thus, security policies should be designed and implemented to replace the damaged nodes in WSNs. RFID security issues are man-in-the-middle attacks, replay attacks, information leakage of tags and user location, cloning attacks and tampering. The trade-off between cost and security must be neutralised. Furthermore, appropriate security policies for RFID applications must be developed. RFID security is primarily executed via code mechanisms, physical methods or their combination. In addition, some problems related to the security of acquiring information, such as, cheating, tampering, replay attacks and wiretapping, must be addressed in the perception layer [48].

Concerns about smart home IoT architecture

The IoT architecture, which is based on generic communication framework, is prone to risks, such as man-in-the-middle attacks, unauthorised accesses, denial-of-service attacks, confidentiality and integrity of data comptonization and virus attacks. Furthermore, the data acquisition from multiple sensor nodes with various formats and the collected data have heterogeneous characteristics. This condition causes several problems in addition to the sophisticated network issues, such as network congestion through data transfer of multiple sensor nodes in this network [48]. Several technical problems are still observed in the IoT architecture, especially in the middleware layer, such as information processing security, privacy and reliability. The critical security issues in the application layer are the design flaws and malicious programs [48].

A system information-processing platform is mainly reflected in smart homes and can efficiently process large amounts of data. The automatic determination of malicious data is limited. Intelligent processing can filter and determine malicious data on the basis of certain rules, in which the attacker can easily avoid the rules and complete the attack. The reduction of losses caused by attacks to a minimum and the return to normal working condition are major security challenges for smart home systems when intelligent processing makes mistakes. Smart systems should set different access rights based on different application requirements, and different permissions to access the same database can obtain various results [16, 44].

IoT authentication schemes can be divided as follows: (a) mutual authentication, (b) directed path-based authentication, (c) two-party authentication through a trusted party with key exchange, (d) two-way authentication, (e) session key-based authentication, (f) OTP and SecureID authentication and (g) group authentication. The IoT architecture defines the schemes that can be utilised on various IoT protocol layers. However, these schemes are still vulnerable to hackers because they require local key management and storage [58].

Currently, the available architecture has a centralised data analysis unit. Furthermore, the available architecture requires encryption on device identity verification in sending messages amongst others. The incontrovertible secured authentication of digital certificates within lightweight devices is expensive. Furthermore, the authentication is an ideal target for attackers with the centralised in-house data analysis unit. Hence, protection approaches, such as antivirus, firewalls and intrusion detection methods, should be applied on the centralized data analysis unit. However, the techniques demonstrate some challenges, especially on experienced home users. The system output analysis might be sophisticated with the utilisation of classic intrusion methods, such as signature-based intrusion detection. Hence, intensive education must be elaborated to home users for problem solving. However, this condition might contradict the IoT concept where minimum user interactions are required [70].

Concerns about protocols

Communication protocols utilised in automated control systems of homes and buildings were proprietary and were not integrated with other legacy systems. This issue was solved with the increase on the power of embedded microcontrollers to run a complete IP stack. However, predictable security protocols require large memory sizes and processing [30]. The existing implementations of security tools are continuously challenging; thus, a complete expertise in applied security engineering is required to achieve high level of IoT security [75].

TLS is the standardised protocol utilised for secured data transmission through the Internet. However. TLS is designed to be utilised in computing devices that consume high power and are not executed on time-serious applications [77]. Furthermore, no HTTPS support is reported on several embedded web-enabled controllers. Meanwhile, SHA-3 is not widely available yet. HTTPS introduction increases power consumption due to data encryption overhead and the effect on transmission times [93].

Medical health protocols should consider two perspectives, namely, medical constrained sensor and smart gateway e-health. The handshake based on a symmetric key requires undisclosed 'pre-shared' keys, which are eagerly valid at each end point of communication. Furthermore, the gain of undisclosed issues in a generic handshake key suggests the 'elliptic curve discrete logarithm computation' issue, which concerns the determination of a solution to fix the discrete logarithm integer factorisation [33].

Various applications cause the variation in communication protocols, which makes them vulnerable to critical security threats. Message Queue Telemetry Transport and CoAP are communication protocols utilised in IoT; however, they lack built-in security mechanisms. Nevertheless, CoAP and other IoT protocols have security solution compounds, such as TLS, DTLS and Secure Sockets Layer, although they are still vulnerable to some threats [58].

DECT eavesdrops without encryption because it is a 'radio frequency' protocol. DECT 'passive eavesdropping' communication simplicity has been illustrated. However, user information leak is observed whether encryption is applied or not. Voice data and their control are protected during transmission when DECT encryption is applied. However, establishing and receiving of calls over the phones are 'negotiated' and can be reached by an eavesdropper prior to encryption. In addition, voice transmission is exposed via the B-Field availability in DECT whether encryption is applied or not [60].

The Time-Synchronised Channel Hopping protocol of IEEE 802.15.4, which handles physical and MAC layers, provides protection from replay attacks. However, the disadvantage of this protocol in terms of security is the management modelling of keys that takes confederation in sending messages where the receiver might strongly reuse the currently used values [64]. 6LoWPAN is a crooked abbreviation of combines IPv6 and LoWPAN. One disadvantage of 6LoWPAN is that no security methodology exists in the adaptation layer. The identification of 6LoWPAN is an issue; for example, the EUI-64 interface scenario is replicated, where the unique interface identifier of this protocol can be compromised. Furthermore, another disadvantage of this protocol is the utilisation of compression User Datagram Protocol (UDP), which reduces the number of its bits from 16 to 4. A possibility of risk exists when the data received by the application are incorrect [31, 64].

The market interest towards IoT technology has increased due to the several CoAP implementations because they have the capability to change future applications. The protocol application layer is initially created to transfer web with limited IoT networks and nodes. The CoAP is a remarkable version of HTTP that matches the IoT requirements with efficient cost and multicast support. Both protocols share a similar REST structure and utilise similar approaches. The CoAP can be defined as a compressed HTTP version. HTTP is an old protocol that provides stability and is widely utilised, whereas CoAP is a new protocol and is undergoing continuous research. HTTP is a huge IP because it requires considerable code space implementation and network utilisation. However, CoAP is particularly designed as a lightweight protocol for network utilisation and implementation. This condition makes CoAP efficient and preferred for small Class 1 devices. HTTP is supported in TCP, whereas CoAP utilises UDP (asynchronous request/repose), which carries messages and send lost packets [64].

A secret key material is required by all security and privacy-preserving protocols and is a challenge in this context. However, many solutions presume that this type of keys is ‘magical’, and is pre-distributed on the sensor nodes by an unspecified mechanism. In some cases, a solution for creating a protected key depends on these pre-distributed shared keys. However, several arguments exist on the distribution of static keys. Sensor nodes can be tampered by attackers within the distribution chain and can learn shared keys, including the entire security system. Manufacturers must be trusted by customers in appropriate key management. Liability is not assumed as a key management by manufacturers [73].

Concerns about software updates of smart home devices

Various interconnected devices—from temperature sensors to smart fridges—can be remotely accessed from the Internet in IoT. This condition poses new security threats to business models, especially to IP providers, who prefer their software to be downloaded and executed in a trusted environment. Typical IoT devices (e.g. smartphones) do not have comparable hardware or computational capabilities with traditional computers; thus, a secured software update on a lightweight device is a challenging task in terms of security and privacy. The design of security solutions is prone to many challenges, especially the critical challenges in this area with respect to smart home scenarios. The challenges with smart home scenarios are that multiple elements are not under user control. Another considerable challenge is the integration of security solutions with an existing software infrastructure and the consideration of the elements of user experience [32]. The challenge associated with the secure update is twofold. Firstly, a freshly shipped sensor node cannot be trusted. In the distribution chain, an attacker can alter the firmware and infect it with a malicious code by installing an additional code that discloses the inherent sensitive data from one’s smart home sensor. Secondly, established protection mechanisms, such as TPM, are unavailable due to the lightweight nature of sensor nodes. Therefore, the integrity of the target device, including the absence of malware, must be guaranteed before the actual IP update occurs [74].

Concerns about WSNs

A WSN is an internal network of a smart home system, in which its task is fully aware in the home environment and collects and passes information to the external network. The packet transmission route of the sensor network is a connectionless routing. The channel error, unsecured wireless communication channel, collision and time delay may result in packet transmission loss. In addition, an attacker may undermine the tasks undertaken by the sensor network through causal analysis, information communication mode or the information exposed by the sensor. Unencrypted addressing and routing information are easy to be attacked through traffic analysis [44]. Critical risks might arise from poor confidentiality and authentication configurations. Certainly, a possibility of emerging new issues and challenges exists in the integration of WSNs with Internet network as IoT. Furthermore, cryptography is important to WSN security [72].

In IoT environment, the data acquisition from a multi-sensor network is a major issue in industrial WSNs. The use of microcontrollers for data acquisition cannot be implemented in a parallel platform because they collect data from nodes based on interrupted signals. However, microcontrollers have low cost and power consumption [50]. Multiple nodes are connected within the WSN to the Internet. This condition is prone to security issues. The key issue is the establishment of the original key session between wireless sensor nodes and centre control [50].

Some network-related challenges are observed on multimedia data that are streamed on WSNs; these challenges are related to bandwidth and processing delays. Real-time streaming of multimedia data requires high bandwidth, low end-to-end delay and low losses during transmission. Several challenges in the efficient transmission of multimedia data in WSN are expressed as follows. Firstly, multimedia encoding at the sensor nodes is challenged by low-power nodes and computational limitation. Subsequently, encoded data transport is challenged by the real-time requirements of bursty multimedia traffic and loss over the hops between the sensor node and wireless station [88].

Smart home contents should be known before breaching privacy. A remarkable advantage for any attacker is the overall nature of wireless ICT of smart home structure. The transmitted information has no protection when encryption is applied because the MAC addresses of the transmitter and receiver are still transmitted in the air, which might be used by attackers for active operation identification in smart homes [60]. Private user data, such as location, behaviour and attendance, can be breached, whether encryption is applied over Wi-Fi and DECT protocol for smart home communications or due to multiple factors. These factors can be summarised as follows. 1) The information sent over the air exceeds the physical limitations of a smart home, which makes smart homes easy to be breached. 2) However, better authentication and confidentiality of private user information can be obtained when several security approaches are applied, although attackers still have the possibility to breach the security and leak information [60].

Concerns about hardware security

Considerable challenges of constrained resources include the device operating from battery power and the VM's execution must be energy efficient. Moreover, the VM complexity increases with each security or interoperability. This situation imposes the requirement for considerable MCU resources, and these resources are complex and power-hungry [39]. Furthermore, commercial and industrial IoT devices are vulnerable to specific IoT attacks, such as posing, replay, data theft, virus attack and denial-of-service attack. A security warning must be considered on the development of IoT devices with limited protection. The flooding of IoT devices in the next decade would cause serious security and privacy concerns when the existing IoT device design flow is continuously utilised [44, 63]. The compatibility of existing smart home systems lacks cooperation in the smart home system. This condition is due to the existing market practice fastening the users with imperial technologies effectively, thereby forcing customers to purchase devices confirmed by manufacturer services to utilise full interoperability [50].

Concerns about IoT-based smart home healthcare systems

The privacy and security of healthcare IoT applications are critical concerns due to the wireless nature of systems and devices. Secure and strong data communication through sensors, users, caregivers and actuators should be ensured because direct human involvement exists in healthcare IoT applications. IoT-based healthcare applications might be restricted by users due to privacy and misuse issues. Traditional protection and security mechanisms that utilise existing cryptography solutions might not be re-utilised due to several issues, such as resource limitations, IoT architecture of healthcare applications and security level requirements. Traditional cryptographic approaches cannot be used on IoT-based healthcare applications. Furthermore, IoT gateways focus on simple tasks without considering authorisation and authentication issues. In addition, medical sensor nodes are easily lost due to their small size. In addition, huge constraints are required by medical application sensors, and cryptographic approaches with heavy computation requirements cannot be utilised [33]. Another solution for medical-based devices is by designing a system based on the cloud. In view of the requirements of the immediate provision of personal medical and flexible data, the data stored in the cloud must constantly remain encrypted and must be operated with data encryption and fine-grained in access control to support and provide various accessibilities. However, a plain combination of encryptions prior to access control is not robust and flexible [57].

Concerns about security risk analysis Generally, risk analysis approaches can be divided into quantitative and qualitative. Qualitative analysis utilises a 'formal model description' in calculating probability, whereas quantitative analysis utilises the developed statistical and mathematical tools to represent the risk in numerical values. Risk analysis that utilises quantitative analysis might be inadequate in IoT infrastructures, where systems have some complex relationships of connected devices, heterogeneous structure, widespread use and deployed software. However, a considerable disadvantage of qualitative risk analysis is its nature of producing results with inconsistency. Qualitative methods are typically not based on mathematics and statistics in modelling risk exposure; thus, their result immensely relies on people who perform the risk analysis, which might be viewed as a merit. Quantitative risk analysis provides each threat, the mean of consequence and probability values to be measured with a mean risk value over the threat accessible range [62].

This state strengthens the issues that emerged through the heterogeneity and complexity of inter-connected services and devices. Furthermore, an established design practice for designing this system is lacking. This condition creates some sophisticated states with the incapability to avoid locking-in of customers. This condition might create 'system–hygienic' complexity issues, such as enforcing information security, enhancing privacy and analysing risks in such environments [49].

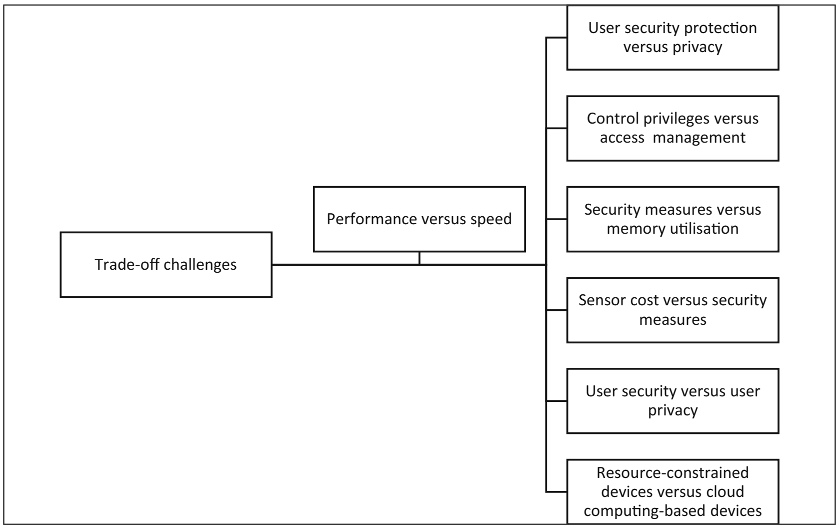
Concerns about user awareness Setting of weak passwords is a high-ranked risk that concerns the IoT related to smart homes. In addition, the default settings of a user's account might make it a hot spot for hackers' man-in-the-middle attacks. Furthermore, the recognition of risk sources on humans span from guideless user that usually constitute targets. For instance, the interruption on employees through social engineering attacks causes them to leak classified data, which results in earning money or the deterioration of employers. In smart home automation systems, information registry related to the power consumption of customers is sensitive, because routines and situations might be concluded by knowing the amount of consumed power and estimation about daily life, which might cause criminal actions based on these data, such as stalking and burglary [62]. However, power consumption can pose serious concerns to users' privacy because the traffic in smart home IoT is sensitive to timeliness, security and privacy. Such usage of information provides detailed consumption about the homes in which they are connected and devices that are used. The collection of such sensitive information over time can allow third parties to infer strongly about users' lifestyle, such as their presence at home or day-to-day routines, thereby breaching user privacy [71].

Concerns about cloud and smart devices Recently, the popularity of cloud computing paradigm has increased. Cloud computing do not include the required elements despite the popularity of wireless sensors and mobile phones to support new applications in different areas, including medical home monitoring. Commonly, traditional access control architecture presumes that the owner and data server are in the same trusted domain, and the data servers that store data are considered the trusted party. For example, ACL is applied in to grant the corresponding access rights to an authenticated user based on ACL permissions. However, data owners and servers in the cloud computing architecture are not in the same domain. Therefore, data owners cannot guarantee the security of their data. In this case, cloud data servers cannot be trusted or semi-trusted, and the data cannot be protected against attackers by the ACL in the cloud. In addition, per-file ACL should be applied towards the provision of fine-grained data access control. However, per-file ACL has its own issues, such as scalability. The complexity of per-file ACL solution rapidly increases with the number of users in the system without scalability [57].

Trade-off challenges The security of smart home based-IoT is vigorous because it handles critical collected data from the sensor nodes from the user side to the destination via the Internet. Hence, trust, privacy and security are the key factors that should be considered by manufacturers when developing smart home IoT. The detailed descriptions of some trade-offs and challenges experienced in the security development of smart home IoT are expressed below, and Fig. 6 shows the summary points of trade-off challenges.

1. Performance and speed are crucial parameters used in smart home IoT in terms of security. The light features of IoT devices allow manufacturers to focus on reducing the processing speed and making a minimum memory size. Hence, users can communicate with each sensor node of IoT devices with minimum delay and without interfering the system throughput [64]. In addition to managing the regular operations of home devices, smart home clouds must cope with the increasing demands of home entertainment and some other applications and must provide the interactions/interoperations between the heterogeneous devices and services from various vendors, in which advanced developments in optimising the utilisations of computing, storage and network resources are required [31].
2. The increasing uptake of smart home appliances, such as power switches, smoke alarms, weighing scales, lights and children monitors, raises privacy and security concerns at unprecedented scale, which allows legitimate and illegitimate entities to snoop and intrude in family activities [53, 69]. Thus, a security system, which balances the security measures between the protection and privacy of users. Numerous stakeholders, such as device and service vendors, are involved in smart home clouds, and complex dependencies exist amongst these stakeholders; thus, global standards are essential to avoid the incompatibilities and conflicts between privately developed platforms and solutions. However, the establishment of global standards to lower the complexity and make smart home clouds compatible and cost effective remains a challenge [31].
3. Access control management: IoT is a developing approach that promises several motivating solutions to multiple issues on many domains. The constantly expanding networks of sensors, actuators and smart devices on the IoT raise interesting challenges for service and network management. For example, the fully connected smart home IoT provides several assistances to customers. Access control for doors, appliances and lights are necessary technologies. However, trade-offs exist between the control privileges versus their management counterparts. These trade-offs include issues, such as ongoing maintenance, interaction control and security. Given the high accessibility of unsecured networks via the Internet, security plays a central role in appropriate IoT management. Therefore, access controls to data, such as the date, time, location and who has access to things and produces data, are examples of security and privacy requirements in IoT [76].
4. Security measures versus memory utilisation: On the basis of a specific device and its restrictions in the IoT, one is frequently required to refrain from implementing expensive public key cryptography to solve the key distribution problem [73]. IoT security has caused increasing concerns because Internet-connected embedded devices can be hacked for malicious network activities, such as remote attacks, spamming and private information theft. Accordingly, enabling arbitrary code execution on millions of such devices turns them into desired targets of hackers. On this basis, a great challenge is balancing the security measures with memory utilisation and computational overhead and maintaining the flexibility of the execution platform. In addition to external risks, certain internal functionalities of the device should be protected from any access by the interpreted code. Buggy or malicious programs might crash the device or cause physical harm when they have unrestricted access to the hardware [39].

Fig. 6 Trade-off Challenges


Trade-off challenges
Performance versus speed
User security protection versus privacy
Control privileges versus access management
Security measures versus memory utilisation
Sensor cost versus security measures
User security versus user privacy
Resource-constrained devices versus cloud computing-based devices

5. Sensor cost versus security measures: The cybersecurity issue is similar to the home environment. Thus, the cybersecurity problem extends beyond computers and is a threat to portable devices. Attackers may utilise these technological progressions to target previously considered secure devices. The information stored and managed within such devices and home networks form part of the critical information infrastructure of individuals. One challenge is that simple or sensor devices are expensive on a mass scale and are vital to embed security in device networks before they are installed rather than attempt to retrofit them later [43]. In addition, a main source of risk is connected to the software components, especially in mobile applications and APIs [62].
6. User security versus user privacy: Each device in a smart home becomes a service for winder clouds of smart homes. This remote integration has the potential to create a new domain of consumers in computing applications and associated services. However, initial attempts on the compulsory adoption of home-based devices have created problems, especially in terms of data privacy [2, 30, 62].
7. Resource-constrained devices versus cloud computing-based devices: A traditional smart home automation system mainly depends on industrial devices that has limited capability in memory, battery usage and data processing speed. However, other solutions that depends on cloud-based mechanism provide a promising means to solve this problem, although the access control of devices to the cloud experiences the complexity without scalability [57].

Motivation

The requirements that drive researchers to pursue their effort in conducting studies in this area are listed in a detailed manner to understand the security concept of smart home IoT. On the basis of previous researcher works, cited studies are included in this section for authentication to obtain a reliable source of knowledge for future research in this domain. Fig. 7 shows the motivations of smart home IoT security.

Smart home security

In view of the remarkable increase in proliferation and miniaturisation of digital computing devices, numerous everyday life aspects have been transferred into digital and have become interconnected by IoT. Some of the common non-digital products, such as smart grids and logistics, energy management, distributed monitoring, mHealth care, household appliances and watches are now permanently connected to the Internet. This phenomenon poses new challenges with regard to technologies and business models. The aspects that are relevant to this proliferation are the security and privacy challenges [73, 90]. These security and privacy problems are widespread amongst IoT devices in the market; hence, solutions should be developed on smart home devices [69]. Furthermore, a remarkable variation exists between the obtainable resources, such as financial and human resources, that are used to implement security and privacy. The variation occurs among the application domains. Human issues are considered equally important as the technical issues in domestic environments. [41]. Security issues are still overlooked despite the large claim by previous studies, and existing studies have claimed that considerable economic impact will be observed in the coming years. However, all existing research proposals are not entirely protected against security threats [59, 78].

Few things are important for all products to make them secured and verified against vulnerability for the prevention of security breaches while facing future threats [34, 46]. Understanding the usage risks of customers and critical

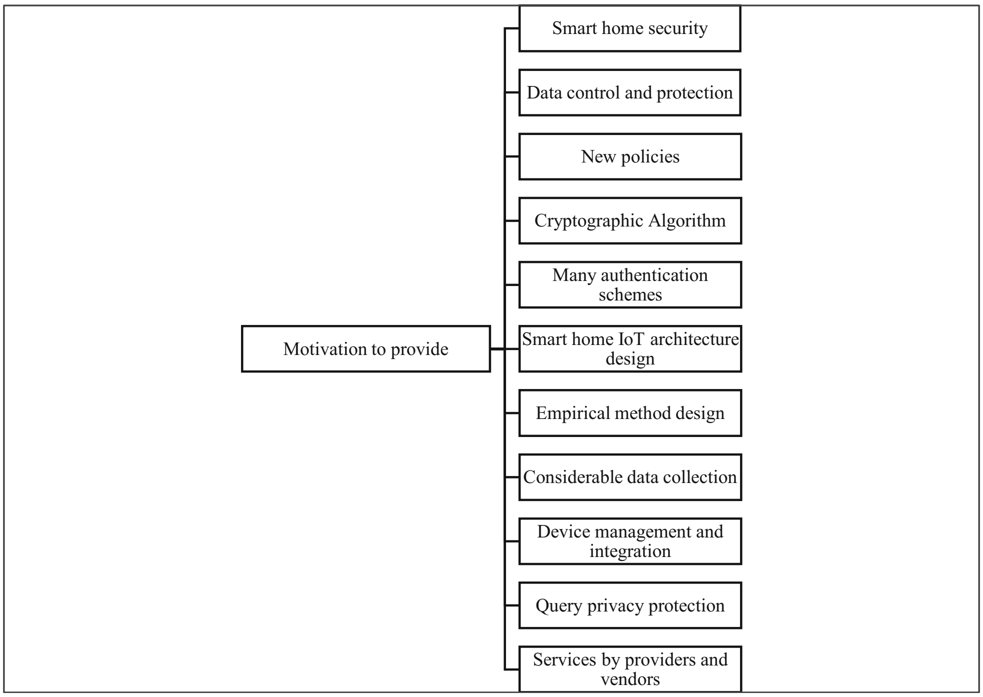

Motivation to provide
Smart home security
Data control and protection
New policies
Cryptographic Algorithm
Many authentication schemes
Smart home IoT architecture design
Empirical method design
Considerable data collection
Device management and integration
Query privacy protection
Services by providers and vendors

Fig. 7 Motivations of Smart Home IoT Security

information abuse is not a straightforward task, and integration methods for security-enhancing measures should be created in the design [62]. Privacy is an important aspect in different aspects, and its protection is a great challenge in different technology areas, including the IoT. In addition, emerging security technologies that have the potential to protect IoT data should be immediately adopted. Therefore, a balance must be achieved between privacy protection and the rapid development of science and technology [2].

However, constant reporting of smart homes' usage information to utility providers can pose serious concerns to user privacy because the traffic in smart home IoT is sensitive to timeliness, security and privacy [71].

Data control and protection

Controlling and protecting private data are critical aspects in the IoT design and deployment. A great challenge emerges due to several issues, such as various roles and users, large systems and device number and IoT heterogeneity technologies. Addressing the trust and privacy requirements, interoperability and scalability is a sophisticated task based on the existing studies and standardisation community [91]. Furthermore, the e-health data of patients and records that can be accessed by various users or insurance corporations aim to follow up patient treatment and aid in emergency cases. They should be provided with access rights to different parts of data because medical records are personal sensitive data, and strong privacy protection should be provided in actual solutions [57].

Security vulnerability is a critical security issue of smart homes. It makes smart home connection to new energy wireless smart grids critical and might lead to total power disruption, and the interconnected multitude of smart devices in IoT becomes a target for cyber-attack or robot network (botnet) and security nightmare for smart space users and national infrastructures. Furthermore, additional concerns arise from the capability of hackers to access various home network resources and convert them to a botnet and launch cyber-attacks on several infrastructures. Some third-party Android applications can access the device root function to make it a botnet without the approval from users. Hence, 'multi-tier user-centred security system–blending safeguards' are required for personal servers, applications, devices and networks. Furthermore, this system provides content management, robust access controls and network monitoring to mitigate the main strategies of old systems [43, 63]. The gateway is a critical network device that recognises several tasks and functions, such as data buffering and protocol conversion. On this basis, strong security protection should be provided on this part of smart home network [89].

The growing number of sensor networks and smart devices in IoT causes various issues and challenges in the management and service of networks. A fully-connected IoT-based smart home provides several services and benefits to customers. These services can be summarised as door access control, lighting control and control of most devices and technologies available in the house. On this basis, access control on data, such as location, time and date, and access to things and their data, are good instances of privacy and security requirements in the IoT to solve the balance between the privilege control versus management counterparts [76].

New policies

New tools and technologies must address the existence of digital divide and must support users while interacting with IoT. Security and privacy are critical issues in IoT rather than the Internet. The safety of citizens can be used by IoT actuators when an attacker malware occupies them or transmit fake information to impair with the decision procedure. Hence, a technology or tool should be developed to enforce IoT actuator policies and evade the execution of actions that affect safety. Furthermore, the ‘dynamic context’ must be addressed in the design and deployment of privacy and security solutions in IoT [91].

Cryptographic algorithm for secure sensor communication

A cryptographic approach is required in ensuring security within the WSN to achieve a secure communication among sensors that communicate with one another. This algorithm should be developed for sensor nodes because sensor devices have limited resources in terms of power consumption, processing power and memory size, thereby making the sensor nodes non-software oriented [72]. Thus, the development of this algorithm should consider these design limitations. Adequate mechanisms should be implemented on data integrity encryption maintenance at the information-processing layer. Furthermore, the proposed mechanisms must be applied to ensure secure data transfer and protection from unauthorised access or interference in the entire network [48].

Authentication schemes

IoT authentication schemes should be addressed in terms of peer-to-peer functionality and communication (sense and actuate), heterogeneity, mobility, feasibility of adapting available authentication schemes, computing power, storage and battery life. Currently, an archiving process is applied to the IoT device data on private and public cloud platforms, and multiple analyses are conducted on data over the cloud. Thus, data request is only granted to authorised application and user to process any command from IoT devices. Authorisation and authentication approaches should be addressed to facilitate this scheme. The dependence on a single authentication scheme in deploying IoT devices with connection to the Internet is a critical risk [58]. IoT security challenges include secure end-to-end connection, authentication and privacy. Furthermore, inter-compatibility must be applied for any security approach due to the availability of several market standards for smart homes. Authentication is considered a major challenge in IoT; however, majority of consumer electronic devices lack a user interface in inserting authentication information. Therefore, a convenient and robust authentication procedure should be developed for smart home systems [31, 38, 58].

Smart home IoT architecture design

Basic points should be addressed to achieve a robust and strong smart home IoT structure. These points identify the requirements based on real issues and challenges, and these requirements should be considered by developers, manufactures and providers during smart home IoT system design.

A) Availability: To maintain the reliability and safety of smart home devices, unauthorized user access or device should not be allowed. Private user data delivered during the intercommunication of smart home devices and the key information used in the encryption algorithm should not be forged or tampered. On this basis, data integrity should be provided on the data that are sent from the smart home device to the outside or another device. The mutual authentication between devices constitutes a smart home service, and a reliable communication environment must be configured. For a fully secured smart home, authentication should be ensured to protect it from attackers, in which access is only given to verified and authorised users [55, 50].

B) Confidentiality

Private user data delivered during the intercommunication of smart home devices and the key information used in the encryption algorithm should be securely managed to prevent the possibility of outside exposure. The data from smart home devices that are sent to another device should be converted into a cipher text form. Smart home devices and their identification information should be securely managed to prevent outsiders from replicating and modification. Smart home devices should provide a highly secure password setting function and periodic password change feature. Home gateways must strengthen the security through a robust and complex password setting [55, 50].

C) Availability

External attack detection capabilities are essential and required towards responding to several security threats, such as hacking and cyber-attacks. In addition, software updates as part of security features must be provided for smart home devices. Furthermore, the settings of device security policy should be considered, which reflect various characteristics and specifications of the device. A device management system should be provided to understand the physical status of smart home devices accurately. In addition, periodic status monitoring of smart home devices should be developed to block unnecessary remote access. Furthermore, appropriate actions should be conducted when smart home devices generate any abnormal operation and abnormal event history [53]. Assortment amongst things, processes, programs and humans that are globally connected is required [50].

D) Risk Analysis

Generally, IoT design and security integration are critical requirements. Unfortunately, risk analysis is not considered during the design and development of smart home automation systems. To address the IoT connection threats, the adaption of security design aids in fixing most of these threats in terms of privacy disclosure, control access and malware mitigation. Furthermore, this security design contributes in the entire system requirements and facilitates the solutions in system development [9]. In addition, security issues at each layer of the IoT architecture require detailed discussion, analysis and solutions to maximise the extent of IoT [34, 48].

E) Different Access Rights

Furthermore, smart systems should set different access rights based on different application requirements, and different permissions to access the same database can obtain different results [44].

Empirical method design for risk analysis

Generally, empirical approaches should be developed based on real data quality and should support risk evaluation in smart homes [9, 49]. The outcome of risk evaluation approaches that support risk acquaintance is essential for the resultant risk of smart home privacy and security. These methods can be categorised based on data collection approaches, such as qualitative, quantitative or semi-quantitative. Access to original data with risk analysis includes evaluation methods that support privacy and security measures. Hence, human social behaviours, such as 'benevolent users and villains' should be considered in this analysis [49].

Data collection

Data sources that are required for probabilistic risk assessments should be identified to evaluate security risks in several domains, especially device security. Any future application of smart home requires reliable data sources. The data quality issue in decision making is not specific to smart homes. The amount of collected and processed data increases with the tremendous increase of IoT applications. The required memory to handle these large data is challenging and is considered a critical issue. 'Artificial intelligence' (AI) algorithms should be utilised in extracting important data from redundant ones [50].

Device integration and management

Ignoring applications is a critical challenge in the IoT environment. All the challenges and issues related to multi-device network management must be addressed to utilise the smart home concept fully. One of these issues is resource usage management in the home through enhanced device usage, which can be achieved by integrating the devices with a wide environment [31, 50]. However, IoT infrastructures and services introduce outstanding challenges related to security for different reasons, such as the considerable increase in the attack surface, complexity, heterogeneity and number of resources [94].

Query privacy protection Sense RFID tags can store larger volumes of data compared with conventional bar codes and have more efficient data processing capabilities. However, consequently, more privacy and security concerns about sensitive data emerge. In addition, greater data vulnerability exists when people utilise wireless terminals in communication, which can be stolen by malicious users. Thus, participants in IoT applications prefer to maintain anonymity in networking environments. Nevertheless, query privacy protection should be considered to block illegal theft and malicious data mining queries in terms of personal privacy data [2].

Services by providers and vendors Users can be considered the weakest point in any chain of IoT security, and 'human factor' is the most challenging factor in mobile device security. Smart home users assume that all the devices in their home are working properly. They depend on the default settings of each device without using technical device manuals. Hence, device content management and network security should be considered and maintained by content and service providers. Furthermore, they should support users by providing security add-ons to improve device security [43]. The smart home network traffic analysis might not be handled for complex patterns; however, smart home network traffic analysis may be conducted on some products and applications. Several hubs have 'built-in operating systems' and can generate 'synthetic packets' to imitate the live packet flows, and the overall process must be automated within the hub. In addition, a synthesis task might be required in the application server-side related to the acknowledgement of packets; however, a limitation on synthesis task might be observed on application developers during its implementation. Thus, the smart home industry should utilise similar solutions within products [92]. An IP address is required for the Internet access request of each device. Currently, machines that utilise IPv4 have extremely low address space. IPv4 should be migrated to IPv6, which has a larger address space [50].

Recommendation pathway solution

This section provides various suggestions and steps that should be considered in investigating smart home IoT security. The described points refer to a previous effort to provide direction and steps that can be a good asset to enhance smart home security. Recommendations are given to multiple parties, such as users, researchers and service providers or vendors. Fig. 8 shows the requirements for smart home IoT design and possible research direction.

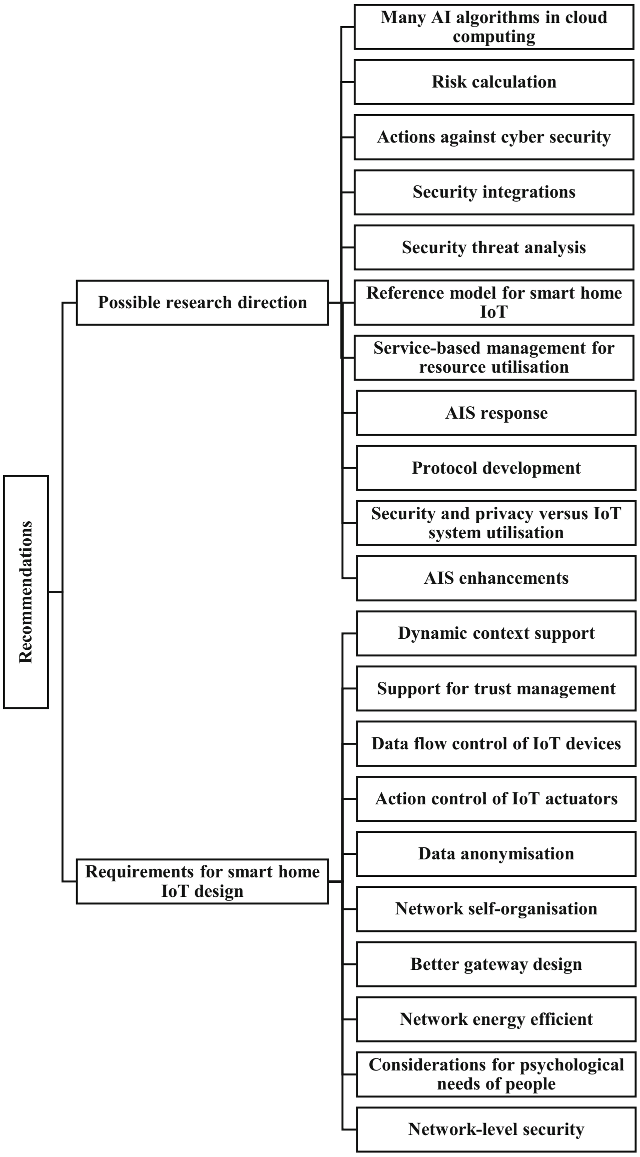

Recommendations
Possible research direction
Many AI algorithms in cloud computing
Risk calculation
Actions against cyber security
Security integrations
Security threat analysis
Reference model for smart home IoT
Service-based management for resource utilisation
AIS response
Protocol development
Security and privacy versus IoT system utilisation
AIS enhancements
Requirements for smart home IoT design
Dynamic context support
Support for trust management
Data flow control of IoT devices
Action control of IoT actuators
Data anonymisation
Network self-organisation
Better gateway design
Network energy efficient
Considerations for psychological needs of people
Network-level security

Fig. 8 Requirements for Smart Home IoT Design and Possible Research Direction

Smart home IoT design requirements

A number of recommended steps for the smart home IoT design to deliver good services for users, service providers and/or vendors are described as follows.

1. Dynamic context support: The design of privacy and security techniques in IoT should contain dynamic context support to meet the privacy and security requirements.
2. Trust management support: IoT rules of security policy must have a considerable level of confidence between users and IoT devices. An explicit definition of the confidence level should be achieved through semantics and precise scope.
3. Digital divide support: Different capabilities and experience are observed from various IoT users that access the IoT. Various levels of technical proficiency on privacy risks and issues and knowledge level should be addressed. Hence, privacy and security designs must provide solutions to divide users digitally into categories.
4. Data flow control from IoT device: The amount and type of transmitted data from IoT devices must be defined by users. Data flow should be automatically monitored and controlled to enhance IoT usability rather than using the current flow that is based on end-user license agreement.
5. Control actions of IoT actuators: Suggested security solutions must prohibit harmful actions that might affect user safety.
6. Data anonymisation: IoT privacy solution must support collected data anonymisation by IoT devices. For example, pseudonyms can be generated to replace user identity for privacy protection [60, 91].
7. Self-organisation of network: The structure of any network must be developed to enable the self-organising capability of each device connected to this network [50].
8. Better gateway design: The gateway functionalities are data buffering, protocol conversion and safety authentication. Thus, the gateway can recognise the interconnection amongst different networks. Currently, the embedded gateway research focuses on the realisation of one or two connecting embedded networks to the Internet. However, few studies have focused on designing gateways with interconnection among one another and connection with several heterogeneous networks. This condition should be considered in IoT development and the connection of things and other things [89].
9. Network energy-efficient: sensor devices have restricted resources in terms of power consumption, processing power and memory size. Security encryption algorithms in IoT must consider these limitations in designing sensor-based systems. Power consumption limitation affects the network lifetime. Hence, basic operations, such

as addition, shifting and EX-OR, must be utilised with the encryption algorithm, and the security should be still reliable during this hardware reduction. WSN lifetime can be enhanced based on this reduction in resources [72].

10. Considerations for psychological needs of people: In addition to typical sense of security, the psychological needs of people are fundamentally a sociology-related question. Therefore, security technologies and people's psychological needs should be considered in discovering privacy issues. In view of the privacy issues and individual differences in different privacy scenarios, typical security technologies do not necessarily handle privacy protection problem of things [2].
11. Network-level security: This security level can be applied in a wide range of IoT devices compared with the device-level security. By contrast, device-level security is embedded within the device itself, which makes it difficult to upgrade. Furthermore, network-level security can be deployed in the cloud with continuous maintenance. In addition, network-level security can be provided by experienced third parties, and device-level security should be maintained by manufacturers who might lack proper security implementation. Network-level security applies an additional protection layer with the capability to augment any device-level security [69].
12. Development process of IoT: A remarkable importance is given to security during the IoT development process. By contrast, the number of security vulnerabilities associated with business and consumers will be enhanced in the future and will lead to catastrophic scenarios for both sides [45].
13. IoT data/standard platform: IoT data are critical in different aspects, such as computing, storage, access and analysis. In addition, a standard platform, which can handle large volumes of heterogeneous data and devices effectively, should exist given the exponential growth of data and devices [78].
14. Smart home IoT security: Solutions remain in their early stage, in which the security factor is considered critical and can affect its adoption rate [32].

Possible research directions

This section describes the recommended research directions that can be conducted by academic and industrial researchers to provide a better security solution for smart home IoT.

1- In the future, AI algorithms can be developed to simplify the extraction of required data from redundant data [50].

2- In cloud computing, specifically in the context of home resource management, 'risk calculation integration' and risk expression in IoT-based spheres should be extensively investigated [62].

3- Critical risks contain instantiating malware and various hacking methods. Hence, they are critical breaches, and should be mitigated; for example, cryptography and authentication amongst connecting things. Furthermore, considerable efforts are required to investigate features of security designs in infrastructures and system features and plans [62].

4- Risk analysis must be utilised to obtain appropriate and efficient security integration of IoT smart home systems. A methodology should possess central security concepts, such as availability, integrity and confidentiality, which are crucial for enabling the reasonable security level identification of smart home systems.

5- A complete approach of robust IoT security is required. Segmentation between threats affect individual users, and the threats that affect the entire system must be considered in future works. Mainly, human actions are the corresponding critical challenges because they do not rely on standardised security features.

6- End-users require an increase in transparency regarding the collection of information and its utilisation within the system. Hence, available automation techniques for smart homes should be intensively investigated [62].

7- Studies on future IoT security issues should focus on physical hardware security and collected information privacy that is transmitted and processed in the network. Furthermore, a chain of policies, regulations and laws is required to make IoT security robust [48].

8- A generic and precise smart home concept description is required, which serves as the reference model for future development. Privacy and security characteristics correspond to users' interaction and connected smart home design products.

9- Flux is an important challenge in making private and secure smart home application, which remains in the evaluation and risk analysis that corresponds to the information. Hence, the privacy and security design that supports the systems must be effective and must overcome the unsecured Internet connection and inefficient power consumers [49]. Currently, a shortage is observed in the research on 'home resource utilisation management' based on services [30].

10- Better AIS response is required to have robust communication amongst 'computation immunology subfield' and development of new 'immune-inspired systems' to utilise fully the generated models. A theoretically robust component that ensues a rigorous algorithm must be utilised in accepting the responsive AIS by the security community as an intense rival approach of IoT protection. Firstly, the modification of existing AIS should adopt the existing research efforts of 'underlying immunology' of response. Previous AIS studies show that some approaches, such as the DCA algorithm, are developed based on a targeted application. This condition could aid the development and verification of a new novel algorithm by combining responsive AIS and IoT security enhancement [70].

11- The IoT vision will simplify daily life and create safety environments. IoT security enforces researchers to consider hardware and source codes, such as application, network, compliance and physical codes, in creating new designs Several research efforts have covered the IoT protocols; however, wide gaps, such as privacy, security and suitable solutions of IoT issues are observed, which should be investigated [64].

12- Research efforts should focus on data management solutions and advanced cryptography protocols in terms of integrity, confidentiality and availability. Furthermore, the importance of security-enhancement technologies from 'cross-network authentication' and 'authorisation' on multiple 'cyber entities' should be emphasised [9].

13- In addition, the vast distribution of RFID and IoT sensor devices, which are used for data processing in handling data methods, makes them diverse and accurate. To make a scientific decision, some commercial departments or research institutions should rely on statistical analysis by utilising IoT data. Therefore, the completion of multiple data mining is an aspect of IoT privacy protection [2].

14- AIS enhancement: Several challenges should be mitigated to solve AIS issues in terms of application and algorithm. The utilised methodology depends on the input from various approaches, such as network security, algorithm design, immunology, smart object vendors and computational modelling. Interdisciplinary coordination performs a challenging research and develops a framework that should be systematically designed. Framework modelling should be utilised as a community to make AIS reconsider its definition [70].

15- Cloud-based platforms and IoT will become the future cornerstone of smart homes, and they aim to make living experience convenient and interesting. However, smart home studies on IoT and cloud computing are still in their primary stages, and the existing body of research related to this area is still lacking [31].

Discussion: key solutions and points

Homes are occupied with electronic devices and computations, and smart TVs, sensors, monitoring and security devices and home energy management systems, which are connected in a network, serve the users. Previous studies have investigated smart home issues, and these issues are divided into multiple categories, such as hardware sensors, protocols, encryption algorithms, architecture design, wireless network issues and user awareness. Smart home hardware devices, such as sensors, experience limited resources, such as memory, data processing, storage and battery usage. Cloud-based computing as an alternative solution is a good means to solve the resource constraints of hardware devices, although it still experiences potential security issues. Standardisation and clear design methods are issues encountered during the development of smart home security. Seamless communication between smart home devices, sensors and the Internet remains a challenge and should be intensively investigated.

The developed architecture design of security systems represents 27.08% of researchers' efforts in their attempt to solve the security challenges of smart home IoT. However, these solutions have mainly focused on resource-constrained devices rather than finding alternative solutions (e.g. cloud computing) that solve limited resource capabilities, which add complexity and impracticality to the overall performance. The development of security protocols and security framework is still in its early stages because they both share the same researchers' effort percentage of 14.58%. In comparison with development studies, security examination studies only represent 18.75% of the previous studies, which indicates that the developed security systems should be evaluated and their reliability performance should be identified in terms of integrity, confidentiality and authenticity. In addition, security analysis topics represent 16.66% of researchers' effort to define previous studies to provide valuable insights in this research area. However, considerable efforts should be exerted to identify the problems that arise with the fast development of technology.

Conclusion

This study highlights a few key issues, including the IoT for telemedicine environments, for future investigation. This study aims to provide an updated security substructure in telemedicine architectures based on IoT technologies. It focused on the directions that handle this subject. The first taxonomy, namely, taxonomy of research literature on the IoT of real-time health monitoring in telemedicine applications, was presented, and studies related to the IoT issues were analysed and discussed in client and server sides. The security limitation in describing or understanding the factors in real-time health monitoring led to the investigation of an additional taxonomy layer and enhanced the security level. In the second taxonomy, a comprehensive survey was conducted on the academic and industrial efforts performed in the area of smart home IoT security. This research approach is at its initial development stage and requires further investigation to provide solid security solutions to overcome the threats that currently compromise smart home users/patients. The trade-off between the home security and privacy of users/patients is still the key issue regarding the protection of smart home patients. In addition, open issues, such as data/identity management, network protocols, cryptographic mechanisms, patient privacy, self-management and resilient architectures, remained in several approaches. The IoT is still in its development stage, thereby affecting the development and security of smart homes. IoT has several issues in its layers that should be enhanced to improve the security of health monitoring in IoT-based smart homes. Moreover, service providers and vendors are responsible for providing better-quality hardware devices to ensure the security of smart homes because the current devices lack security standards. Meanwhile, users/patients are responsible for their protection because they can increase their security awareness regarding cyber security attacks that target their smartphones, computers, tablets or other smart devices during diagnosis or monitoring. The current security issues require collaborative academic and industrial work with the rapid development of smart devices to overcome cyber security attacks and enhance or improve the security and privacy levels in telemedicine and healthcare monitoring systems based on IoT.

Compliance with ethical standards

Conflict of interest The authors declare no conflict of interest.

Ethical approval All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Declaration of Helsinki and its later amendments or comparable ethical standards.

Informed consent Informed consent was obtained from all individual participants included in the study.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

1. Zanella, A., Bui, N., Castellani, A., Vangelista, L., and Zorzi, M., Internet of Things for Smart Cities. IEEE Internet Things J. 1(1): 22–32, 2014.
2. Tian, C., Chen, X., Guo, D., Sun, J., and Liu, L., Analysis and design of security in Internet of things. *2015 8th Int.*, 2015.
3. Zhang, X. M., and Zhang, N., An open, secure and flexible platform based on internet of things and cloud computing for ambient aiding living and telemedicine. In: *2011 International Conference on Computer and Management, CAMAN 2011*, pp. 1–4, 2011.
4. Stowe, S., and Harding, S., Telecare, telehealth and telemedicine. European Geriatric Medicine 1(3. No longer published by Elsevier):193–197, 2010.
5. Thota, C., Sundarasekar, R., Manogaran, G., Varatharajan, R., and Priyan, M. K., Centralized fog computing security platform for IoT and cloud in healthcare system. In: *The Convergence of Big Data and*, IGI Global, pp. 141–154, 2017.
6. Rajan, S. P., Review and investigations on future research directions of mobile based telecare system for cardiac surveillance. Rev. Mex. Trastor. Aliment. 13(4):454–460, 2015.
7. Negra, R., Jemili, I., and Belghith, A., Wireless Body Area Networks : Applications and technologies. Procedia - Procedia Comput. Sci. 83:1274–1281, 2016.
8. Martin, S., Kelly, G., Kernohan, W. G., McCreight, B., and Nugent, C., Smart home technologies for health and social care support. *Cochrane Database of Systematic Reviews*, 2008.
9. Jacobsson, A., Boldt, M., and Carlsson, B., A risk analysis of a smart home automation system. Elsevier 56:719–733, 2016.
10. Aggidis, A. G. A., Newman, J. D., and Aggidis, G. A., Investigating pipeline and state of the art blood glucose biosensors to formulate next steps. Biosens. Bioelectron. 74:243–262, 2015.
11. Woznowski, P., Kaleshi, D., Oikonomou, G., and Craddock, I., Classification and suitability of sensing technologies for activity recognition. Comput. Commun. 89–90:34–50, 2016.
12. Albahri, A. S., Zaidan, A. A., Albahri, O. S., Zaidan, B. B., and Alsalem, M. A., Real-Time Fault-Tolerant mHealth System: Comprehensive Review of Healthcare Services, Opens Issues, Challenges and Methodological Aspects. J. Med. Syst. 42(8): 137, 2018.
13. Albahri, O. S., Zaidan, A. A., Zaidan, B. B., Hashim, M., Albahri, A. S., and Alsalem, M. A., Real-Time Remote Health-Monitoring Systems in a Medical Centre: A Review of the Provision of Healthcare Services-Based Body Sensor Information, Open Challenges and Methodological Aspects. J. Med. Syst. 42(9): 164, 2018.
14. Rahmani, A. M. et al., Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. Futur. Gener. Comput. Syst. 78(2):641–658, 2018.
15. Albahri, O. S. et al., Systematic Review of Real-time Remote Health Monitoring System in Triage and Priority-Based Sensor Technology: Taxonomy, Open Challenges, Motivation and Recommendations. J. Med. Syst. 42(5):80, May 2018.
16. Sakr, S., and Elgammal, A., Towards a Comprehensive Data Analytics Framework for Smart Healthcare Services. Big Data Res. 4:44–58, 2016.
17. Hindia, M. N., Rahman, T. A., Ojukwu, H., Hanafi, E. B., and Fattouh, A., Enabling remote health-caring utilizing IoT concept over LTE-femtocell networks. PLoS One 11(5):e0155077, 2016.
18. Gómez, J., Oviedo, B., and Zhuma, E., Patient Monitoring System Based on Internet of Things. Procedia Comput. Sci. 83:90–97, 2016.
19. Hussain, A., Wenbi, R., Da Silva, A. L., Nadher, M., and Mudhish, M., Health and emergency-care platform for the elderly and disabled people in the Smart City. J. Syst. Softw. 110:253–263, 2015.
20. Kumar, N., Kaur, K., Jindal, A., and Rodrigues, J. J. P. C., Providing healthcare services on-the-fly using multi-player cooperation game theory in Internet of Vehicles (IoV) environment. Digit. Commun. Networks 1(3):191–203, 2015.
21. Zanjal, S. V., and Talmale, G. R., Medicine Reminder and Monitoring System for Secure Health Using IOT. Phys. Procedia 78:471–476, 2016.
22. Kalid, N. et al., Based on Real Time Remote Health Monitoring Systems: A New Approach for Prioritization 'Large Scales Data' Patients with Chronic Heart Diseases Using Body Sensors and Communication Technology. J. Med. Syst. 42(4):69, 2018.
23. Courtney, K. L., Demiris, G., Rantz, M., and Skubic, M., Needing smart home technologies: The perspective of older adults in continuing care retirement communities. Radcliffe Medical Press, 2008.
24. Alaa, M., Zaidan, A. A., Zaidan, B. B., Talal, M., and Kiah, M. L. M., A review of smart home applications based on Internet of Things. J. Netw. Comput. Appl. 97. Academic Press:48–65, 2017.

25. Zaidan, A. A. et al., A survey on communication components for IoT-based technologies in smart homes. Telecommun. Syst. 69(1): 1–25, 2018.
26. Zaidan, A. A. and Zaidan, B. B., A review on intelligent process for smart home applications based on IoT: coherent taxonomy, motivation, open challenges, and recommendations. *Artificial Intelligence Review*, Springer Netherlands, pp. 1–25, 2018.
27. Gaikwad, P. P., Gabhane, J. P., and Golait, S. S., 3-level secure Kerberos authentication for smart home systems using IoT. In: *Proc. 2015 1st Int. Conf. Next Gener. Comput. Technol. NGCT 2015*, pp. 262–268, 2016.
28. Alohali, B., Merabti, M., and Kifayat, K., A secure scheme for a smart house based on Cloud of Things (CoT). *2014 6th Comput. Sci. Electron. Eng. Conf. CEEC 2014 - Conf. Proc.*, pp. 115–120, 2014.
29. Le Vinh, T., Bouzefrane, S., Farinone, J., Attar, A., and Kennedy, B. P., Middleware to Integrate Mobile Devices, Sensors and Cloud Computing. Procedia Comput. Sci. 52:234–243, 2015.
30. Kirkham, T., Armstrong, D., Djemame, K., and Jiang, M., Risk driven Smart Home resource management using cloud services. *Futur. Gener. Comput. Syst.* 38: 2013.
31. Tao, M., Zuo, J., Liu, Z., Castiglione, A., and Palmieri, F., Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. Futur. Gener. Comput. Syst. 78:1040–1051, 2018.
32. Chifor, B. C., Bica, I., Patriciu, V. V., and Pop, F., A security authorization scheme for smart home Internet of Things devices. Futur. Gener. Comput. Syst. 86:740–749, 2018.
33. Moosavi, S. R. et al., SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. Procedia Computer Science 52(1):452–459, 2015.
34. Yuan, X. and Peng, S., A research on secure smart home based on the Internet of Things. In: *2012 IEEE International Conference on Information Science and Technology*, pp. 737–740, 2012.
35. You-Guo, L., and Ming-Fu, J., The reinforcement of communication security of the internet of things in the field of intelligent home through the use of middleware. In: *Proceedings - 2011 4th International Symposium on Knowledge Acquisition and Modeling, KAM 2011*, pp. 254–257, 2011.
36. Witkovski, A., Santin, V., Abreu, J. M., Management, and undefined 2015. An IdM and key-based authentication method for providing single sign-on in IoT, 2015. *researchgate.net*.
37. Rajiv, P., Raj, R., and Chandra, M., Email based remote access and surveillance system for smart home infrastructure. Perspect. Sci. 8: 459–461, 2016.
38. Santoso, F. K. and Vun, N. C. H., Securing IoT for smart home system. *Proc. Int. Symp. Consum. Electron. ISCE*, 2015, 2015.
39. D. Yunge, P. Kindt, M. B.-… (HPCC), 2015 IEEE 7th, and U. Hybrid apps: Apps for the internet of things, 2015. *ieeexplore.ieee.org*.
40. Jiang, T., Yang, M., and Zhang, Y., Research and implementation of M2M smart home and security system. Secur. Commun. Networks 8(16):2704–2711, 2015.
41. Lin, H., and Bergmann, N. W., IoT privacy and security challenges for smart home environments. *Information*. 7(3), 2016.
42. S. Tanwar, P. Patel, K. Patel, … S. T.-C., and undefined, An advanced Internet of Thing based security alert system for smart home, 2017. *Ieeexplore.Ieee.Org*.
43. A. A.-P. C. Science and undefined, Cyber security challenges within the connected home ecosystem futures. *Elsevier,* 2015.
44. Li, F., Wan, Z., Xiong, X., and Tan, J., Research on sensor-gateway-terminal security mechanism of smart home based on IOT. *Internet of Things*, 2012.
45. Furfaro, A., Argento, L., Parise, A., and Piccolo, A., Using virtual environments for the assessment of cyberseturity issues in IoT scenarios. Simul. Model. Pract. Theory 73:43–54, 2017.
46. M. S.-I. S. I. M. & I. Forensics and undefined, Smart home definition and security threats, 2015. *Ieeexplore.Ieee.Org*.
47. Lee, C., Zappaterra, L., Choi, K., and Choi, H., Securing smart home : Technologies, security challenges , and security requirements. In: *Workshop on Security and Privacy in Machine-to-Machine Communications (M2MSec'14)*, pp. 67–72, 2014.
48. Matharu, G. S., Upadhyay, P., and Chaudhary, L., The Internet of Things: Challenges &amp; security issues. In: *2014 International Conference on Emerging Technologies (ICET)*, pp. 54–59, 2014.
49. Jacobsson, A. and Davidsson, P., Towards a model of privacy and security for smart homes. *IEEE World Forum Internet Things, WF-IoT 2015 - Proc.*, pp. 727–732, 2016.
50. Suryani, V., Sulistyo, S., and Widyawan, A survey on trust in internet of things. In: *2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE)*, pp. 1–6, 2016.
51. Sain, M, Kang, Y. J., and Lee, H. J., Survey on security in Internet of Things: State of the art and challenges. In: *2017 19th International Conference on Advanced Communication Technology (ICACT)*, pp. 699–704, 2017.
52. Bastos, D., Shackleton, M., and El-Moussa, F., Internet of things: A survey of technologies and security risks in smart home and city environments. In: *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, pp. 7–30, 2018.
53. Han, J. H., Jeon, Y., and Kim, J., Security considerations for secure and trustworthy smart home system in the IoT environment. *Int. Conf. ICT Converg. 2015 Innov. Towar. IoT, 5G, Smart Media Era, ICTC 2015*, pp. 1116–1118, 2015.
54. Peng, Z., Kato, T., Takahashi, H., and Kinoshita, T., Intelligent home security system using agent-based IoT devices. *ieeexplore.ieee.org*, pp. 313–314, 2015.
55. Datta, S. K., Towards securing discovery services in Internet of Things. In: *2016 IEEE International Conference on Consumer Electronics, ICCE 2016*, pp. 506–507, 2016.
56. Kim, Y. P., Yoo, S., and Yoo, C., DAoT: Dynamic and energy-aware authentication for smart home appliances in Internet of Things. *2015 IEEE Int. Conf. Consum. Electron. ICCE 2015*, pp. 196–197, 2015.
57. Ren, W., Ren, Y., Wu, M. E., and Lee, C. J., A Robust and Flexible Access Control Scheme for Cloud-IoT Paradigm with Application to Remote Mobile Medical Monitoring. In: *Proceedings - 2015 3rd International Conference on Robot, Vision and Signal Processing, RVSP 2015*, pp. 130–133, 2016.
58. Shivraj, V. L., Rajan, M. A., Singh, M., and Balamuralidhar, P., One time password authentication scheme based on elliptic curves for Internet of Things (IoT). In: *2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW)*, pp. 1–6, 2015.
59. Yang, L., Seasholtz, C., Luo, B., and Li, F., Hide your hackable smart home from remote attacks: The multipath onion IoT Gateways, pp. 575–594, 2018.
60. Sanchez, I., *et al.*, Privacy leakages in Smart Home wireless technologies. *Proc. - Int. Carnahan Conf. Secur. Technol.* 2014, 2014.
61. Min, B. and Varadharajan, V., Design and Evaluation of Feature Distributed Malware Attacks against the Internet of Things (IoT). In: *Proceedings of the IEEE International Conference on Engineering of Complex Computer Systems, ICECCS*, vol. 2016, pp. 80–89, 2016.
62. Jacobsson, A., Boldt, M., and Carlsson, B., On the Risk Exposure of Smart Home Automation Systems. *2014 Int. Conf. Futur. Internet Things Cloud*, pp. 183–190, 2014.
63. Wurm, J., Hoang, K., Arias, O., Sadeghi, A. R., and Jin, Y., Security analysis on consumer and industrial IoT devices. *Proc.*

Asia South Pacific Des. Autom. Conf. ASP-DAC, vol. 25–28, pp. 519–524, 2016.

64. Rahman, R. A. and Shah, B., Security analysis of IoT protocols: A focus in CoAP. In: *2016 3rd MEC International Conference on Big Data and Smart City, ICBDSC 2016*, pp. 172–178, 2016.
65. Bao, H., Chong, A. Y. L., Ooi, K. B., and Lin, B., Are Chinese consumers ready to adopt mobile smart home? An empirical analysis. Int. J. Mob. Commun. 12(5):496, 2014.
66. Ling, Z., Luo, J., Xu, Y., Gao, C., Wu, K., and Fu, X., Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System. IEEE Internet Things J. 4(6):1899–1909, 2017.
67. Liu, J., Zhang, C., and Fang, Y., EPIC: A Differential Privacy Framework to Defend Smart Homes Against Internet Traffic Analysis. IEEE Internet Things J. 5(2):1206–1217, 2018.
68. Ukil, A., Bandyopadhyay, S., and Pal, A., Privacy for IoT: Involuntary privacy enablement for smart energy systems. IEEE International Conference on Communications 2015:536–541, 2015.
69. Sivaraman, V., Gharakheili, H. H., Vishwanath, A., Boreli, R., and Mehani, O., Network-level security and privacy control for smart-home IoT devices. In: *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob 2015*, pp. 163–167, 2015.
70. Greensmith, J., Securing the Internet of Things with Responsive Artificial Immune Systems. *Proc. 2015 Genet. Evol. Comput. Conf. - GECCO '15*, pp. 113–120, 2015.
71. S. Errapotu, J. Wang, Y. Gong, … J. C.-I. I. of, and U, SAFE: Secure Appliance Scheduling for Flexible and Efficient Energy Consumption for Smart Home IoT, 2018. ieeexplore.ieee.org.
72. Vinayaga Sundaram, B., Ramnath, M., Prasanth, M., and Varsha Sundaram, J., Encryption and hash based security in Internet of Things. In: *2015 3rd International Conference on Signal Processing, Communication and Networking, ICSCN 2015*, pp. 1–6, 2015.
73. Huth, C., Zibuschka, J., Duplys, P., and Güneysu, T., Securing systems on the Internet of Things via physical properties of devices and communications. In: *9th Annual IEEE International Systems Conference, SysCon 2015 - Proceedings*, pp. 8–13, 2015.
74. Huth, C., Duplys, P., and Guneysu, T., Secure software update and IP protection for untrusted devices in the Internet of Things via physically unclonable functions. In: *2016 IEEE International Conference on Pervasive Computing and Communication Workshops, PerCom Workshops 2016*, 2016.
75. Bergmann, O., Gerdes, S., Schäfer, S., Junge, F., and Bormann C., Secure bootstrapping of nodes in a CoAP network. In: *2012 IEEE Wireless Communications and Networking Conference Workshops, WCNCW 2012*, pp. 220–225, 2012.
76. Elkhodr, M., Shahrestani, S., and Cheung, H., A Smart Home Application Based on the Internet of Things Management Platform. In: *2015 IEEE International Conference on Data Science and Data Intensive Systems*, pp. 491–496, 2015.
77. Fisher, R. and Hancke, G. P., DTLS for lightweight secure data streaming in the internet of things. In: *Proceedings - 2014 9th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 3PGCIC 2014*, pp. 585–590, 2014.
78. Amin, R., Kumar, N., Biswas, G. P., Iqbal, R., and Chang, V., A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment. Futur. Gener. Comput. Syst. Int. J. Escience 78:1005–1019, 2018.
79. Song, T., Li, R., Mei, B., Yu, J., Xing, X., and Cheng, X., A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes. In: *2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI)*, pp. 519–524, 2016.
80. Adiono, T., Marthensa, R., Muttaqin, R., Fuada, S., Harimurti, S., and Adijarto, W., Design of database and secure communication protocols for Internet-of-things-based smart home system. *IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON*, vol. 2017, pp. 1273–1278, 2017.
81. Y. Chao, M. Jianfeng, D. X.-J. of Communications, and undefined, A New Evaluation Model for Security Protocols. *Citeseer,* 2011.
82. Getz, K. A., Wenger, J., Campo, R. A., Seguine, E. S., and Kaitin, K. I., Assessing the impact of protocol design changes on clinical trial performance. Am. J. Ther. 15(5):450–457, 2008.
83. Nadeem, A. and Javed, M. Y., A performance comparison of data encryption algorithms. In: *2005 International Conference on Information and Communication Technologies*, pp. 84–89, 2005.
84. Beckers, K., *Pattern and Security Requirements*. 2015.
85. Michael, K., The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Comput. Secur. 31(4):634–635, 2012.
86. Boritz, J. E., IS practitioners' views on core concepts of information integrity. Int. J. Account. Inf. Syst. 6(4):260–279, 2005.
87. Loukas, G., and Öke, G., Protection against denial of service attacks: A survey. Comput. J. 53(7):1020–1037, 2010.
88. Suryadevara, J., Sunil, B., and Kumar, N., Secured multimedia authentication system for wireless sensor network data related to Internet of Things. In: *2013 Seventh International Conference on Sensing Technology (ICST)*, pp. 109–115, 2013.
89. Xie, X., Deng, D., and Deng, X., Design of embedded gateway software framework for heterogeneous networks interconnection. *Proc. 2011 Int. Conf. Electron. Optoelectron.*, vol. 2, no. ICEOE, pp. V2–306-V2–309, 2011.
90. Peretti, G., Lakkundi, V., and Zorzi, M., BlinkToSCoAP: An end-to-end security framework for the Internet of Things. *2015 7th Int. Conf. Commun. Syst. Networks, COMSNETS 2015 - Proc.*, pp. 1–6, 2015.
91. R. Neisse, G. Steri, I. Fovino, G. B.-C. & Security, and undefined, SecKit: a model-based security toolkit for the internet of things. *Elsevier,* 2015.
92. Yoshigoe, K., Dai, W., Abramson, M., and Jacobs, A., Overcoming invasion of privacy in smart home environment with synthetic packet injection. In: *Proceedings of 2015 TRON Symposium, TRONSHOW 2015*, 2016.
93. Cebrat, G., Secure web based home automation: Application layer based security using embedded programmable logic controller. In: *2014 2nd International Conference on Information and Communication Technology, ICoICT 2014*, pp. 302–307, 2014.
94. Pacheco, J. and Hariri, S., IoT security framework for smart cyber infrastructures. In: *Proceedings - IEEE 1st International Workshops on Foundations and Applications of Self-Systems, FAS-W 2016*, pp. 242–247, 2016.
95. Baruah, B., and Dhal, S., A two-factor authentication scheme against FDM attack in IFTTT based Smart Home System. Comput. Secur. 77:21–35, 2018.
96. Dorri, A., Kanhere, S. S., Jurdak, R., and Gauravaram, P., Blockchain for IoT security and privacy: The case study of a smart home. In: *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 618–623, 2017.
97. Ge, M., Hong, J. B., Guttmann, W., and Kim, D. S., A framework for automating security analysis of the internet of things. J. Netw. Comput. Appl. 83:12–27, 2017.
98. Kalyanasundaramf, B., and Schnitgerf, G., THE PROBABILISTIC COMMUNICATION COMPLEXITY OF SET INTERSECTION*. SIAM J. Disc. MATH 5(4):545–557, 1992.
99. Ahmed, M. A. et al., A Review on Systems-Based Sensory Gloves for Sign Language Recognition State of the Art between 2007 and 2017. Sensors 18(7):2208, 2018.

100. Zaidan, A. A., et al., A review on smartphone skin cancer diagnosis apps in evaluation and benchmarking: coherent taxonomy, open issues and recommendation pathway solution. Health Technol. (Berl)., 2018.

101. Alsalem, M. A. et al., Systematic Review of an Automated Multiclass Detection and Classification System for Acute Leukaemia in Terms of Evaluation and Benchmarking, Open Challenges, Issues and Methodological Aspects. J. Med. Syst. 42(11):204, 2018.

102. Alsalem, M. A. et al., A review of the automated detection and classification of acute leukaemia: Coherent taxonomy, datasets, validation and performance measurements, motivation, open challenges and recommendations. Comput. Methods Prog. Biomed. 158:93–112, 2018.

103. Zughoul, O., et al., Comprehensive Insights into the Criteria of Student Performance in Various Educational Domains. IEEE Access, 2018.

104. Mohsin, A. H. et al., Real-Time Remote Health Monitoring Systems Using Body Sensor Information and Finger Vein Biometric Verification: A Multi-Layer Systematic Review. J. Med. Syst. 42(12):238, 2018.

105. Mohsin, A. H., et al., Real-time Medical Systems based on Human Biometric Steganography: A Systematic Review. J. Med. Syst. 42(12), 2018.

106. Yas, Q. M. et al., A systematic review on smartphone skin cancer apps: coherent taxonomy, motivations, open challenges and recommendations, and new research direction. Journal of Circuits, Systems and Computers 27(05):1830003, 2018.

107. Hamada, M. et al., A Systematic Review for Human EEG Brain Signals Based Emotion Classification, Feature Extraction, Brain Condition, Group Comparison. J. Med. Syst. 42(9):162, 2018.

108. Tareq, Z., et al., A review of disability EEG based wheelchair control system: Coherent taxonomy, open challenges and recommendations. Computer methods and programs in biomedicine, 2018.

109. Zaidan, B. B. et al., Impact of data privacy and confidentiality on developing telemedicine applications: A review participates opinion and expert concerns. Int. J. Pharmacol. 7(3):382–387, 2011.

110. Mat Kiah, M. L. et al., Design and Develop a Video Conferencing Framework for Real-Time Telemedicine Applications Using Secure Group-Based Communication Architecture. J. Med. Syst. 38(10):133, 2014.

111. Kalid, N. et al., Based Real Time Remote Health Monitoring Systems: A Review on Patients Prioritization and Related ‘Big Data’ Using Body Sensors information and Communication Technology. J. Med. Syst. 42(2):30, 2018.

112. Salman, O. H. et al., Novel Methodology for Triage and Prioritizing Using ‘Big Data’ Patients with Chronic Heart Diseases Through Telemedicine Environmental. Int. J. Inf. Technol. Decis. Mak. 16(05):1211–1245, 2017.

113. Hussain, M., et al., Conceptual framework for the security of mobile health applications on Android platform. Telematics and Informatics, 2018.

114. Hussain, M. et al., A security framework for mHealth apps on Android platform. Comput. Secur. 75:191–217, 2018.

115. Alanazi, H. O. et al., Secure topology for electronic medical record transmissions. Int. J. Pharmacol. 6(6):954–958, 2010.

116. Alanazi, H. O. et al., Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance. Journal of Medicinal Plants Research 4(19): 2059–2074, 2010.

117. Nabi, M. S. A. et al., Suitability of using SOAP protocol to secure electronic medical record databases transmission. Int. J. Pharmacol. 6(6):959–964, 2010.

118. Mat Kiah, M. L. et al., An enhanced security solution for electronic medical records based on AES hybrid technique with SOAP/XML and SHA-1. J. Med. Syst. 37(5):9971, 2013.

119. Alanazi, H. O. et al., Meeting the security requirements of electronic medical records in the ERA of high-speed computing. J. Med. Syst. 39(1):165, 2015.

120. Iqbal, S., et al., Real-time-based E-health systems: design and implementation of a lightweight key management protocol for securing sensitive information of patients. Health Technol. (Berl)., 2018.

121. Enaizan, O., et al., Electronic Medical Record Systems: Decision Support Examination Framework for Individual, Security and Privacy Concerns Using Multi-Perspective Analysis. J. Health Technol. pp 1–28, 2018.

122. Zaidan, A. A. et al., Multi-criteria analysis for OS-EMR software selection problem: A comparative study. Decis. Support. Syst. 78: 15–27, 2015.

123. Kiah, M. L. M. et al., Open source EMR software: Profiling, insights and hands-on analysis. Comput. Methods Prog. Biomed. 117(2):360–382, 2014.

124. Zaidan, A. A. et al., Evaluation and selection of open-source EMR software packages based on integrated AHP and TOPSIS. J. Biomed. Inform. 53:390–404, 2015.

125. Zaidan, B. et al., Enhancement of the amount of hidden data and the quality of image. Kuala Lumpur: Faculty of Computer Science and Information Technology, University of Malaya.

126. Zaidan, A. A. et al., Novel approach for high secure data hidden in MPEG video using public key infrastructure. Int. J. Comput. Netw. Secur. 1(1):1985–1553, 2009.

127. Naji, A. W. et al., Challenges of hidden data in the unused area two within executable files. J. Comput. Sci. 5(11):890, 2009.

128. Hameed, S. A. et al., Novel Simulation Framework of Three-Dimensional Skull Bio-Metric Measurement. Int. J. Comput. Sci. Eng. 1(3):269–274, 2009.

129. Naji, A. W. et al., New approach of hidden data in the portable executable file without change the size of carrier file using distortion techniques. Proceeding of World Academy of Science Engineering and Technology (WASET) 56:493–497, 2009.

130. Majeed, A. et al., Novel approach for high secure and high rate data hidden in the image using image texture analysis. International Journal of Engineering and Technology 1(2):63–69, 2009.

131. Zaidan, A. A., et al., Implementation stage for high securing cover-file of hidden data using computation between cryptography and steganography. International Association of Computer Science and Information Technology (IACSIT), indexing by Nielsen, Thomson ISI (ISTP), IACSIT Database, British Library and EI Compendex, 20, 2009.

132. Naji, A. W. et al., New approach of hidden data in the portable executable file without change the size of carrier file using statistical technique. International Journal of Computer Science and Network Security (IJCSNS) 9(7):218–224, 2009.

133. Zaidan, B. B. et al., New Comprehensive Study to Assess Comparatively the QKD, XKMS, KDM in the PKI encryption algorithms. Int. J. Comput. Sci. Eng. 1(3):263–268, 2009.

134. Naji, A. W. et al., (2009). "Stego-Analysis Chain, Session One" Investigations on Steganography Weakness vs Stego-Analysis System for Multimedia File. In: Computer Science and Information Technology-Spring Conference. IACSITSC'09. International Association of (pp. 405–409). IEEE, 2009.

135. Khalifa, O. O. et al., Novel approach of hidden data in the (unused area 2 within EXE file) using computation between cryptography and steganography. International Journal of Computer Science and Network Security (IJCSNS) 9(5):294–300, 2010.

136. Zaidan, A. A. et al., High securing cover-file of hidden data using statistical technique and AES encryption algorithm. World

Academy of Science Engineering and Technology (WASET) 54: 468–479, 2009.

137. Zaidan, B. B., et al., An empirical study for impact of the increment the size of hidden data on the image texture. ICFCC09, 2009.

138. Eltahir, M. E. et al., High rate video streaming steganography. In: Information Management and Engineering, 2009. ICIME'09. International Conference on (pp. 550–553). IEEE, 2009.

139. Zaidan, A. A., et al., Approved undetectable-antivirus steganography for multimedia information in PE-file. In: International Conference on IACSIT Spring Conference (IACSIT-SC09), Advanced Management Science (AMS), Listed in IEEE Xplore and be indexed by both EI (Compendex) and ISI Thomson (ISTP), Session (Vol. 9, pp. 425–429), 2009.

140. Naji, A. W., et al., "Stego-Analysis Chain, Session Two" Novel Approach of Stego-Analysis System for Image File. In: Computer Science and Information Technology-Spring Conference, 2009. IACSITSC'09. International Association of (pp. 410–413). IEEE, 2009.

141. Taqa, A. et al., New framework for high secure data hidden in the MPEG using AES encryption algorithm. International Journal of Computer and Electrical Engineering (IJCEE) 1(5):566–571, 2009.

142. Zaidan, B. B. et al., Stego-image vs stego-analysis system. International Journal of Computer and Electrical Engineering 1(5):572, 2009.

143. Zaidan, A. A. et al., New technique of hidden data in pe-file with in unused area one. International Journal of Computer and Electrical Engineering (IJCEE) 1(5):669–678, 2009.

144. Jalab, H., et al., Frame selected approach for hiding data within MPEG video using bit plane complexity segmentation. arXiv preprint arXiv:0912.3986, 2009.

145. Ahmed, M. A. et al., A novel embedding method to increase capacity and robustness of low-bit encoding audio steganography technique using noise gate software logic algorithm. J. Appl. Sci. 10(1):59–64, 2010.

146. Al-Frajat, A. K. et al., Hiding data in video file: An overview. Journal of Applied Sciences (Faisalabad) 10(15):1644–1649, 2010.

147. Zaidan, A. A. et al., Novel approach for high (secure and rate) data hidden within triplex space for executable file. Sci. Res. Essays 5(15):1965–1977, 2010.

148. Alam, G. M. et al., Using the features of mosaic image and AES cryptosystem to implement an extremely high rate and high secure data hidden: Analytical study. Sci. Res. Essays 5(21):3254–3260, 2010.

149. Hameed, S. A. et al., An accurate method to obtain bio-metric measurements for three dimensional skull. J. Appl. Sci. 10(2): 145–150, 2010.

150. Naji, A. W. et al., Novel approach for cover file of hidden data in the unused area two within EXE file using distortion techniques and advance encryption standard. Proceeding of World Academy of Science Engineering and Technology (WASET) 56(5):498–502, 2010.

151. Naji, A. W., et al., Novel framework for hidden data in the image page within executable file using computation between advanced encryption standard and distortion techniques. arXiv preprint arXiv:0908.0216, 2009.

152. Zaidan, B. B. et al., On the differences between hiding information and cryptography techniques: An overview. Journal of Applied Sciences(Faisalabad) 10(15):1650–1655, 2010.

153. Hmood, A. K. et al., An overview on hiding information technique in images. Journal of Applied Sciences(Faisalabad) 10(18):2094–2100, 2010.

154. Hamdan, A. et al., New frame work of hidden data with in non multimedia file. Int. J. Comput. Netw. Secur. 2(1):46–54, 2010.

155. Jalab, H. A. et al., New design for information hiding with in steganography using distortion techniques. International Journal of Engineering and Technology 2(1):72, 2010.

156. Abomhara, M. A. S., Enhancing selective encryption for H. 264/AVC using advanced encryption standard (Doctoral dissertation, University of Malaya), 2011.

157. Zaidan, A. A., et al., Securing cover-file without limitation of hidden data size using computation between cryptography and steganography. In: Proceedings of the World Congress on Engineering (Vol. 1, pp. 1–7), 2009.

158. Zaidan, B. et al., Quality of Image vs. Quantity of Data Hidden in the Image. IPCV 6:343–350, 2009.

159. Othman, F., et al., An extensive empirical study for the impact of increasing data hidden on the images texture. In: Future Computer and Communication, 2009. ICFCC 2009. International Conference on (pp. 477–481). IEEE, 2009.

160. Islam, R., et al., New system for secure cover file of hidden data in the image page within executable file using statistical steganography techniques. arXiv preprint arXiv:1002.2416, 2010.

161. Elnajjar, M., et al., Optimization digital image watermarking technique for patent protection. arXiv preprint arXiv:1002.4049, 2010.

162. Alanazi, H., et al., Intrusion detection system: overview. arXiv preprint arXiv:1002.4047, 2010.

163. Zaidan, B. B. et al., Towards corrosion detection system. International Journal of Computer Science Issues (IJCSI) 7(3): 46, 2010.

164. Zaidan, A. A. et al., A New System for Hiding Data within (Unused Area Two+ Image Page) of Portable Executable File Using Statistical Technique and Advance Encryption Standared. International Journal of Computer Theory and Engineering 2(2): 218, 2010.

165. Alanazi, H., et al., New Classification Methods for Hiding Information into Two Parts: Multimedia Files and Non Multimedia Files. arXiv preprint arXiv:1003.4084, 2010.

166. Alanazi, H., et al., New comparative study between DES, 3DES and AES within nine factors. arXiv preprint arXiv:1003.4085, 2010.

167. Al-Ani, Z. K., et al., Overview: Main fundamentals for steganography. arXiv preprint arXiv:1003.4086, 2010.

168. Hmood, A. K. et al., On the capacity and security of steganography approaches: An overview. Journal of Applied Sciences (Faisalabad) 10(16):1825–1833, 2010.

169. Abomhara, M. et al., Suitability of Using Symmetric Key to Secure Multimedia Data: An Overview. Journal of Applied Sciences (Faisalabad) 10(15):1656–1661, 2010.

170. Hmood, A. K. et al., On the accuracy of hiding information metrics: Counterfeit protection for education and important certificates. International Journal of Physical Sciences 5(7):1054–1062, 2010.

171. Yahya, A. N., et al., A new system for hidden data within header space for EXE-File using object oriented technique. In: Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on (Vol. 7, pp. 9–13). IEEE, 2010.

172. Zaidan, A. A. et al., Investigate the capability of applying hidden data in text file: An overview. Journal of Applied Sciences (Faisalabad) 10(17):1916–1922, 2010.

173. Zaidan, B. B. et al., StegoMos: A secure novel approach of high rate data hidden using mosaic image and ANN-BMP cryptosystem. International Journal of Physical Sciences 5(11):1796–1806, 2010.

174. Zaidan, A. A. et al., Novel multi-cover steganography using remote sensing image and general recursion neural cryptosystem. International Journal of Physical Sciences 5(11):1776–1786, 2010.

175. Raad, M. et al., Impact of spam advertisement through e-mail: A study to assess the influence of the anti-spam on the e-mail marketing. Afr. J. Bus. Manag. 4(11):2362–2367, 2010.

176. Salem, Y. et al., A review on multimedia communications cryptography. Res. J. Inf. Technol. 3:146–152, 2011.

177. Mat Kiah, M. L. et al., A review of audio based steganography and digital watermarking. International Journal of Physical Sciences 6(16):3837–3850, 2011.

178. Watari, M. A. et al., Securing m-Government Transmission Based on Symmetric and Asymmetric Algorithms: A review. Asian Journal of Scientific Ressearch 8:80–94, 2013.

179. Hussain, M. et al., The rise of keyloggers on smartphones: A survey and insight into motion-based tap inference attacks. Pervasive and Mobile Computing 25:1–25, 2016.

180. Zaidan, A. A. et al., Spam influence on business and economy: Theoretical and experimental studies for textual anti-spam filtering using mature document processing and naive Bayesian classifier. Afr. J. Bus. Manag. 5(2):596–607, 2011.

181. Zaidan, A. A. et al., Commercialization Strategy and Implementation Plans for the Proposed Vitual Anti-Spam System based on Feasibility Study. Asian Journal of Scientific Research 8(3):403–412, 2015.

182. Medani, A. et al., Review of mobile short message service security issues and techniques towards the solution. Sci. Res. Essays 6(6): 1147–1165, 2011.

183. Al-Bakri, S. H. et al., Securing peer-to-peer mobile communications using public key cryptography: New security strategy. International Journal of Physical Sciences 6(4):930–938, 2011.

184. Naji, A. W. et al., Security improvement of credit card online purchasing system. Sci. Res. Essays 6(16):3357–3370, 2011.

185. Abomhara, M. et al., An experiment of scalable video security solution using H. 264/AVC and advanced encryption standard (AES): Selective cryptography. International Journal of the Physical Sciences 6(16):4053–4063, 2011.

186. Nabi, M. S., et al., Suitability of adopting S/MIME and OpenPGP email messages protocol to secure electronic medical records. In: Future Generation Communication Technology (FGCT), 2013 Second International Conference on (pp. 93–97). IEEE, 2013.

187. Zaidan, B. B. et al., A new digital watermarking evaluation and benchmarking methodology using an external group of evaluators and multi-criteria analysis based on 'large-scale data'. Softw. - Pract. Exp. 47(10):1365–1392, 2017.

188. Zaidan, B. B., and Zaidan, A. A., Software and Hardware FPGA-Based Digital Watermarking and Steganography Approaches: Toward New Methodology for Evaluation and Benchmarking Using Multi-Criteria Decision-Making Techniques. J. Circuits, Syst. Comput. 26(07):1750116, 2017.

189. Zaidan, B. B. et al., A New Approach based on Multi-Dimensional Evaluation and Benchmarking for Data Hiding Techniques. Int. J. Inf. Technol. Decis. Mak.:1–42, 2017.

190. Zaidan, B. B., and Zaidan, A. A., Comparative study on the evaluation and benchmarking information hiding approaches based multi-measurement analysis using TOPSIS method with different normalisation, separation and context techniques. Meas. J. Int. Meas. Confed. 117:277–294, 2018.

191. Ali, A. H. et al., High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain. Multimed. Tools Appl. 77(23):31487–31516, 2018.

192. Abdul-Talib, Y. Y., et al., Optimizing security and flexibility by designing a high security system for e-government servers. ICOCI09, Univ. Utara Malaysia, pp. 355–358, 2009.

193. Zaidan, B. B. et al., A security framework for nationwide health information exchange based on telehealth strategy. J. Med. Syst. 39(5):51, 2015.

194. Kiah, M. L. M. et al., MIRASS: medical informatics research activity support system using information mashup network. J. Med. Syst. 38(4):37, 2014.

195. Zaidan, A. A. et al., Challenges, Alternatives, and Paths to Sustainability: Better Public Health Promotion Using Social Networking Pages as Key Tools. J. Med. Syst. 39(2):7, 2015.

196. Abdulnabi, M. et al., A distributed framework for health information exchange using smartphone technologies. J. Biomed. Inform. 69:230–250, 2017.

197. Nidhal, S. et al., Computerized algorithm for fetal heart rate baseline and baseline variability estimation based on distance between signal average and alpha value. Int. J. Pharmacol. 7(2):228–237, 2011.

198. Hussain, M. et al., The landscape of research on smartphone medical apps: Coherent taxonomy, motivations, open challenges and recommendations. Comput. Methods Prog. Biomed. 122(3):393–408, 2015.