Indonesian Journal of Electrical Engineering and Informatics (IJEEI)
Vol. 13, No. 1, March 2025, pp. 277~293
ISSN: 2089-3272, DOI: 10.52549/ijeei.v13i1.6103

Systematic Literature Review: Security Challenges of IoT-based Smart Home Systems

Abdullah Ali Ben-Nakhi[1], Mostafa Abd El-barr[2], and Kalim Qureshi[3*]

[1,3]Department of Information Science, College of Life Sciences, Kuwait University, Kuwait,
[2]Former-Dean College of Computing Science and Engineering, Kuwait University, Kuwait

Article Info

Article history:

Received Dec 3, 2024
Revised Mar 10, 2025
Accepted Mar 25, 2025

Keywords:

Smart Homes
Security
IoT
Systematic Literature Review

ABSTRACT

Internet of things has a wide range of applications such as healthcare, agriculture, transportation, and industrial manufacturing. Smart homes automation occupies a large segment of applications. Due to the proliferation of IoT-based smart homes systems, the attack vector on these devices expanded and became a target for attackers. Although these devices are improving constantly, security is still a challenge for them. The lack of security standardizations and hardware limitations resulted in a slow or lack of security practices in these devices. In this study, we conduct a systematic literature review to identify the exposed threats in the last five years in these devices and introduce novel countermeasures to mitigate the security issues. IEEE, ACM, Scopus, Science Direct, Springer, and MDPI databases were selected for the systematic review. The result of the systematic review were 731 articles collected. Based on reading the abstract, 605 articles were excluded, and 41 articles were excluded based on reading the full text. The result 70 articles were filtered using quality assessment criteria which resulted in 35 articles related to our search domain and answering the research questions. Additionally, a survey is conducted to elicit experts in the field knowledge to enhance our findings. We were able to identify 22 unique threats that endanger smart homes systems and the proposed countermeasures classified into 5 classes.

Corresponding Author:

Kalim Qureshi,
Department of Information Science, College of Life Sciences,
Kuwait University, State of Kuwait.
Email: kalimuddinqureshi@gmail.com, kalimuddin.qureshi@ku.edu.kw

1. INTRODUCTION

Internet of Things is a broad term that covers a wide range of applications; Examples include smart homes, wearable devices, smart grids, and connected cars [1]. But, IoT-enabled smart homes application stands out as the most prominent application under IoT. By 2022 smart homes market share is expected to reach 53.45 billion dollars [2], and by 2023 the number of smart homes is expected to exceed 300 million houses [3]. The majority of IoT devices sold in 2019 and 2020 were smart home automation devices [59]. Smart homes are described as the ability to control and monitor different home devices and appliances remotely via the internet. Smart home applications encompass the needs of the residents to provide comfort, safety, security, and energy-saving for the inhabitants [61]. Although IoT-enabled smart homes devices are used for a wide range of applications, security and surveillance are the most dominant application requirements. According to the statistics, the amount of smart homes security and surveillance devices sold is expected to triple between 2017 and 2022 [5]. The reason for the enormous demand for a home security system is that these devices should give a sense of safety and security to homeowners. Another critical application for smart home automation is healthcare automation at home for the elderly and people with disabilities [6]. From these previous statistics, we infer that the demand and the usage of smart home devices are to growing over time. Hence, this growth motivates us to:

- Systematically identify the wide range of vulnerabilities threatening smart homes devices and to cover as many possible threats exist.
- Analyze the risk resulting from vulnerability to figure the severity of the vulnerability to households.

Problem Statement

Due to the popular demand for IoT-based smart home devices, the security of these devices is mandatory not an optional feature. Summarizing the problem statement as follow:

- The hardware limitations impose the designers of these devices to present special cases security mechanisms such as lightweight encryption mechanisms.
- The heterogeneous nature of these devices leads to a lack of a standard security framework for smart home systems.
- The human factor plays a prime factor in facilitating attacks on smart homes because of misconfigurations.

Therefore, mitigating the vulnerabilities encountering smart homes is becoming difficult over time and makes smart homes exposed to a wide range of attacks.

Objectives

The main aim of this study is to find out the current state of the art in smart homes devices in terms of their security. Simplify the overall view of these threats to facilitate vulnerabilities mitigation. To achieve this goal a systematic literature review (SLR) is conducted to achieve the following objectives:

- Collect the research conducted in the field of security related to IoT-enabled smart homes.
- Identify the security challenges facing smart homes.
- Understand suggested solutions to mitigate security issues.
- Mapping the security challenges to the proper mitigation method.
- Anticipate upcoming security challenges.
- Identify research gaps in collected studies. Contribution

Our contributions are summarized as follow:

1. Direct the researchers to the latest trend in IoT smart homes applications security domain.
2. Conduct a rigorous systematic literature review that helps with minizine research bias selecting articles and extracting data.
3. Analyzing then mapping the existing vulnerabilities to the mitigation proposed in the collected studied.
4. Introduce a guideline for developers of smart home systems to minimize the vulnerabilities in the designs phase of these devices and systems before deploying.
5. Identify the research gaps in the smart homes security domain to provide search space for future works.
6. Anticipates the future weaknesses in smart home devices.

Table 1. Research Questions

No	Research Question	Purpose
RQ1	What research are conducted in the area of smart home security within the last five years?	To Identify literatures in the field within the last five years
RQ2	What are the categories of attacks (threats) smart homes are exposed to?	To Identify the vulnerabilities threatening smart homes
RQ3	What are the existing countermeasures to mitigate smart homes attacks?	To identify the methods to control smart homes security challenges
RQ4	What analysis is made to study security aspects of the studied work?	To account for the analysis made
RQ5	What are the expected security problems in the future?	To Anticipate the future security threats that cannot be mitigated by the current solutions

Research Questions

In conducting a SLR the first step is developing the research questions driving the SLR. Research questions reflect the targeted audience and defined purpose of the SLR Form [7] we adopted PICOC (population, intervention, comparison, outcome, context) criteria to set a base for the research questions.

We aim to identify the literature conducted related to the smart home systems security recent attacks and security threats and what are the countermeasures undertaken against these attacks and threats. Based on PICOC criteria and the problem statement we formulated the research questions and explained the purpose of each question in table 1.

2. Systematic Literature Review

The amount of research being produced in any field of science is growing tremendously. This growth of knowledge imposes hardships in keeping track of the state-of-art or the latest trends in a particular field of science. Therefore, a reliable literature review methodology is required to keep up with this growth of information. In addition, the adopted methodology must be transparent and reproducible by other researchers.

Hence, there is a need for a rigorous and reliable methodological approach to extract all the evidence needed from relevant studies to answer the proposed research questions that are derived from the problem statement. Systematic literature review (SLR) fulfills our requirements for a methodology to be followed to avoid any biases in the search process.

According to [7], a systematic literature review is a "means of identifying, evaluating and interpreting all available research relevant to a particular research question, or topic area, or phenomenon of interest". Historically, systematic literature review methodology developed for medical science research and most produced SLRs are in the medical field [8]. However, a systematic review by itself is not sufficient. Because systematic literature review is dependent on qualitative analysis. A quantitative analysis combined with a systematic review derives a stronger conclusion. Meta-analysis is a quantitative approach and is used to statistically analyze the collected data. Meta-analysis is used to find or estimate the magnitude of a vulnerability or find the pattern of attacks.

2.1 Advantages of SLR

The major advantage of systematic review over conventional review is that systematic review follows a rigorous strategy to collect and analyze data for a specific purpose, hence, this followed strategy is documented to assess its eligibility by other researchers. In our case, SLR is used as a tool to answer the research questions derived from the problem statement. This rigorous strategy facilitates collecting as much as studies in a methodological approach reduce the possibilities of biasness in selecting studies across a wide range of studies available. The biasness was reduced to a minimum by following explicit inclusion/exclusion clearly defined criteria for selecting studies. Furthermore, the methodological approach assists in quantitatively analyzing the collected using for example meta-analysis approach to support the hypothesis. The rigorous methodology of systematic review poses heavy efforts for the researcher to follow. [7] in the SLR guide states that the following reasons for conducting the systematic review:

- Collect and summarize data regarding a particular problem.
- Identify gaps in collected studies to improve upon in the future.
- Set a milestone or guidelines to start from for new researchers.

2.2 SLR Comparison

Although there is an abundance of SLR guidelines directed to the medical science field, there are two SLR guidelines designed to serve the computing research field: procedures for performing Systematic reviews [7] and a guide to conducting a systematic literature review of information systems research [62]. In this section, these two guidelines are compared to select the suitable methodology for our research to follow.

Comparing the two guidelines (Table 2) we infer that they are relatively similar in steps and phases. However, the guidelines in [62] consist of more deailed steps and gives more examples in each step. In this research, we adopted the [62] guideline because it is designed for IS and provide detailed steps. Furthermore, [62] balances between qualitative and quantitative approaches.

Table 5. SLR Guidelines Comparison

Comparison	Okoli & Schabra (2010) [62]	Kitchenham (2004) [7]
Citation number	1337 until May 2021	5379 until May 2021
Designed for	Information systems	Software engineering
Based on	Six guidelines	Three guidelines
Phases/Steps	Four phases Planning phase Selection phase Extracting phase Execution phase	Three phases Planning phase Conducting phase Reporting phase
Qualitative/Quantitative	Both	Only Qualitative

In conclusion, SLR is a significant tool to collect existing threats and identify state-of-art solutions. We are following [62] SLR guide because it's compatible with our domain of search and provides detailed steps in each phase of the review. We did not modify the proposed phases in [62], since the guide is very detailed and covers all steps needed for our research. However, there are components added to those in [62] guide to enhance the search process and validate the final results. From [7] we adopted PICOC (population, intervention, comparison, outcome, context) criteria in the search strategy phase to help with constructing

research questions and define the targeted audience. Also, validity assessment was added as the last step to cope with research bias threats in our research.

3. Search Protocol

In our developed protocol, we aim to guide collecting literatures and minimize any research bias. Following systematic documented steps through review assure the completeness of the review and helps with validating against search threats. In this section we select the digital libraries we are going to search, define the search strings, refine the search strings through conducting a preliminary search in the selected digital libraries.

Since our topic is in the information technology domain we decided to consult a specific subject database. In the search process, we selected five scientific digital libraries, since they contain publications [55] in the field of computer science, engineering, security, privacy, and internet of things (IoT) [51]. These digital libraries are IEEE Xplore [50] (IEEE Xplore Advacned Search, n.d.), Association for Computing Machinery (ACM) [49] (ACM Digital Library , n.d.), Science Direct [56] (ScienceDirect Advanced Search, n.d.), Scopus [57] (Scopus Document Search, n.d.) and Springer [58] (SpringerLink Avanced Search, n.d.). The digital libraries were selected in particular for the following reasons:

a) Well known for their credibility and dependability in the scientific community.
b) Recommendation from an academic professor.
c) Recommendation from SLR in IoT domain [9] [10] [11]
d) Number of resulting digital libraries in google scholar

In addition, we took advantage of the Google Scholar search engine to help with finding an article that is not in selected digital libraries. Furthermore, consulting professors in the field of computer since and engineering recommenced MDPI open-access digital library contains publications related to IoT and smart homes security.

Starting the search process in digital libraries and search engines needs to develop searching strings. The search strings derived from research questions guide the search process in Table . We aim to find articles related to smart homes security and the attacks threatening smart homes security. So that, at the beginning the search string was *"smart homes" AND security AND "attack*"*. Nonetheless, during the search process in digital libraries and search engines more suggested search strings arose to help widen the search process for related articles to our subject. Thus, we decided to improve the search string to obtain better results and ensure search comprehensiveness. The improved search string was based on the pilot obtained results the search string developed following these criteria:

- Suggested words by digital libraries and search engines.
- Derived from relative papers' titles.
- Derived from relative papers' keywords.

After reading the keywords from the retrieved articles in the second iteration, we decided to change the search string. We deduced that replacing attacks with threats widen the range of articles retrieved by digital libraries. This means we can find more articles related to our search objective. With the help of the previous criteria to improve the search string Table 3 shows the factors that helped with formulating the final search string. The final search string:

(("smart home" OR "home automation") AND (iot OR "internet of things") AND ((security) OR (threat) OR ("countermeasures" OR "counter measures" OR "counter-measures")))

Table 3. Selection of search term

Search Term Form	Factor
Research Questions	RQ1, RQ2, RQ3
Relevant Papers	A taxonomy of cyber-physical threats and impact in the smart home [12], Security threats taxonomy: Smart-home perspective [13].
Synonyms/Alternative Spellings	Smart home or home automation, IoT or internet of things, security or threats, countermeasures or counter measures OR counter-measures
Boolean Operators	ANDs and Ors

3.1 Searching Literature

Using the search string developed in the search protocol section in the selected digital libraries. The search process in digital libraries resulted in hundreds of studies, we limit the search by applying the criteria in the selected libraries. The following criteria were applied for inclusion in the search:

- Published between January 2015 and the end of 2020.
- Search in title, abstract, and keywords only.

- Written in English literatures.
- Search in journals only.

The search string resulted in a total of 715 articles found and distributed as shown in Table 4.

Table 4. Selected digital libraries and journals

Source	URL	Articles Cashed
IEEE Journals	https://ieeexplore.ieee.org/search/advanced	**86**
ACM Journals	https://dl.acm.org/search/advanced	**137**
Scopus	https://www-scopus-com.kulibrary.vdiscovery.org/search/form.uri?display=basic	**209**
Science Direct	https://www.sciencedirect.com/search	**83**
Springer	https://link.springer.com/advanced-search	**200**

3.2 Practical Screen

The retrieved literatures from the five digital libraries were significantly large. A filtering process is needed to find out the applicable literatus to answer our research questions. The excluding process conducted according to the criteria is [62]:

- Eligibility of the literatures to answer the research questions.
- Defined explicitly inclusions\exclusion to reduce the number of literatures to a manageable number (Table 5).

Table 5. Inclusion and exclusion criteria

Inclusion criteria	Exclusion criteria
• Systematic Literature review, taxonomy, model, and assessment of smart homes security. • Smart homes security in general. • Attacks, threats, and vulnerabilities in smart homes devices or systems. • Solutions or countermeasures for smart homes vulnerabilities.	• Do not answer research questions • About the internet of things not including smart homes. • Duplicates study in same or different library, database, or journal. • Smart home user activity and behavior recognition. • Smart homes articles related to health monitoring.

Figure 1 illustrates the steps carried out to filter the collected studies from the selected digital libraries. These steps are adapted from PRISMA. The PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses) flow diagram plays a significant role in selecting because it ensures transparency in selecting primary studies [4]. Table 6 shows the number of collected studies after exclusion studies not applicable to our research questions.

Table 6. Number of studies after exclusion

Source	Articles Cashed
IEEE	19
ACM	6
Scopus	31
Science Direct	12
Springer	10
MDPI Sensors	4
Total	82

After applying the inclusion\exclusion criteria the number of resulting articles is shown in Table 6. Since inclusion\exclusion criteria are applied merely by reading the title and abstract in the collected studies, a further examination is required to assess the eligibility of the collected studies comprehensively in the next step.

4. Quality Assessment

In the practical screening section, prime studies that do not fulfill inclusion criteria were eliminated. In this section, the selected prime studies undergo a quality assessment to ensure inclusion and exclusion criteria are met and rank the literature according to their importance and infer recommendations for future research [7]. Quality assessments improve prime study selection by examining the selected studies closely to ensure they meet the quality standards for our systematic review. Rating the collected studies in the inclusion/exclusion phase helps with eliminating the prime studies that do not meet the systematic review quality criteria since the quality of selected studies affects the final output of our systematic review [14]. Quality assessment is a group of questions that assess the quality of the prime studies. The guidelines for Reviews [7] adopted DARE criteria to assess the quality of each study. However, the DARE criteria were designed specifically to assess the SLR article's quality.

In our case, we did not find SLRs related to our domain of work in our search for prime studies. The refence iin [15] states that there is no standard quality assessment checklist due to the subjectivity of the assessment checklist. Therefore, the quality assessment questions derived from DARE criteria to fulfill the rating needs of assessing our collected prime studies [7].

Table 7 embodies the quality assessment checklist for assessing the quality of the selected prime studies. In quality assessment checking the article marked with “Yes” if the question in the list is answered, marked with “No” if the question is not answered. In case the question is partially answered it is marked with “Partially”. The scoring system works as follows: “Yes” = 1, “Partially” = 0.5, or “No” = 0. This study is eliminated immediately because it will not benefit the research. After evaluating all the selected studies against the quality assessment questions, the aggregated score was calculated for each study [10].

Then a threshold was defined if the study score was less than 3 excluded. If the study scored equal or greater than 3 included for the systematic review if the study doesn’t score 1 for QA2 the disqualified because it does not answer the research question. The scoring for each article presented in Appendix A and Figure 2 depicts the quality assessment process stages.

Table 7. PSs Quality Assessment

Q ID	Question	Score
QA1	Is the objective of the article clearly defined?	Y/N
QA2	Does the article answer research questions?	Y/N/P
QA3	Is the research method described?	Y/N/P
QA4	Are the suggested countermeasure/solutions validated?	Y/N/P
QA5	Are the contributions and limitations of the article explained?	Y/N/P
QA6	Does the article provide a space for future work?	Y/N

4.1 Data Extraction

In this section, the designed data extraction form was applied to collect key data to answer the research questions. We included the 50 studies selected in the data selection section in data extraction.

4.2 Quantitative Data Analysis

In quantitative analysis the frequencies used to evaluate the selected studies in terms of publication years, active journals in the field of smart homes, threat or vulnerabilities, mitigations, and area of concern. Table 8presents the included and excludes the number of studies from each searched database and depicts (Figure) that the most included database is IEEE and most excluded Scopus. In addition, from Appendix A scoring table IEEE scored the highest average of quality scoring, whereas ACM scored the lowest. Furthermore, the IEEE database dominate of the field of IoT [52] research than any other selected database.

In Figure 3 and 4, the distribution of selected studies over years from 2015 to 2020 proves our statement that propagation of IoT-enabled smart homes rapidly increases over a narrow time of frame, and security of these devices and systems has been the subject of study in the domain of Internet of Things.

When comparing the extracted vulnerabilities, we infer that the collected studies are homogeneous. The total number of extracted threats is 22 unique threats (Table 9). The most frequent attacks as shown in Figure 5, concern smart homes are denial of service, data leakage, and eavesdropping attacks. Where, lack of encryption, open ports, masquerade attack, gain initial access and unsecured interface are the least mentioned in the prime studies. In Figure the distribution of selected studies over years from 2015 to 2020 proves our statement that propagation of IoT-enabled smart homes rapidly increases over a narrow time of frame, and security of these devices and systems has been the subject of study in the domain of Internet of Things.

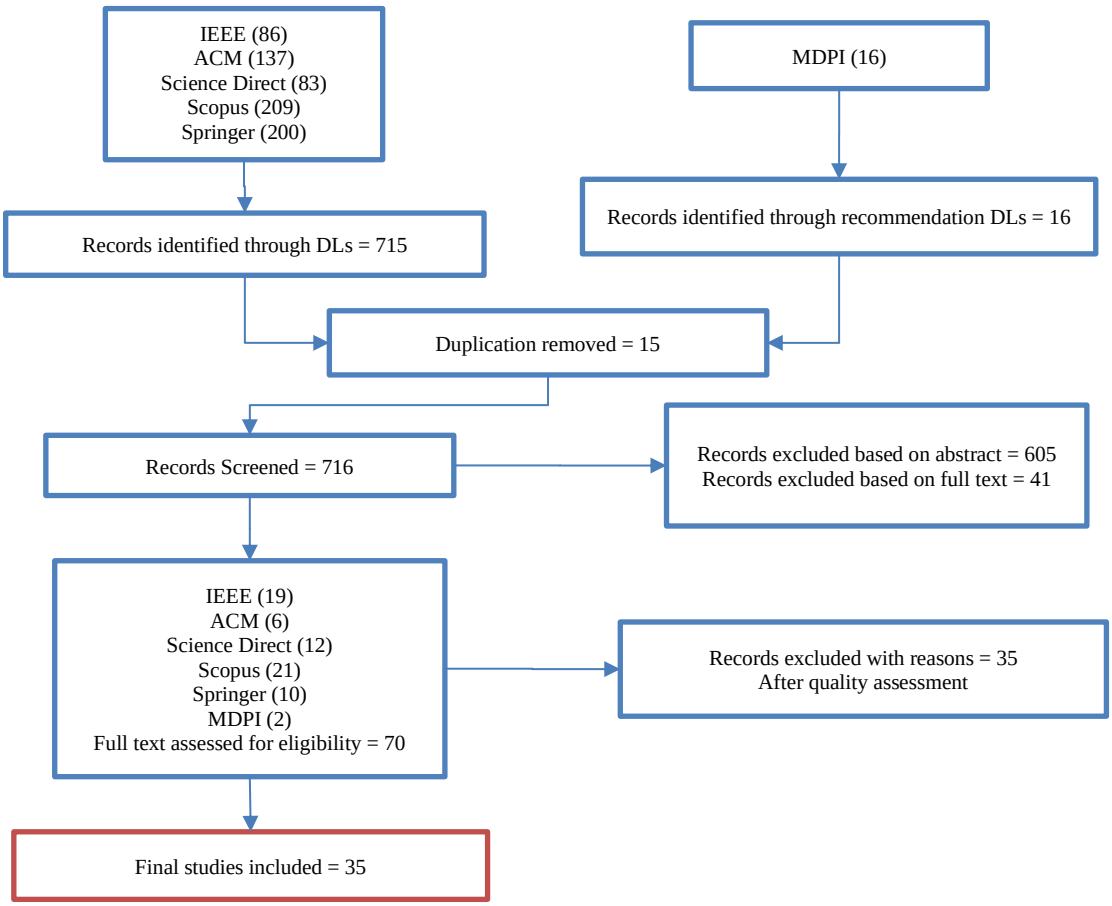

Figure 1. Steps to filter prime studies

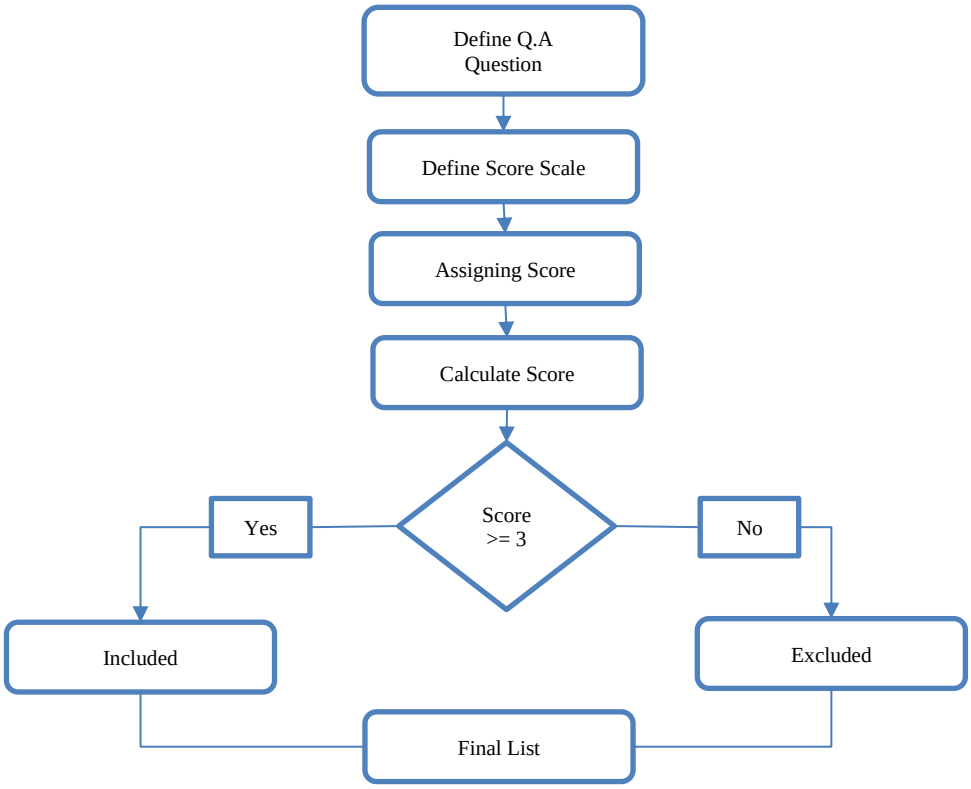

Figure 5. Quality Assessment Proces

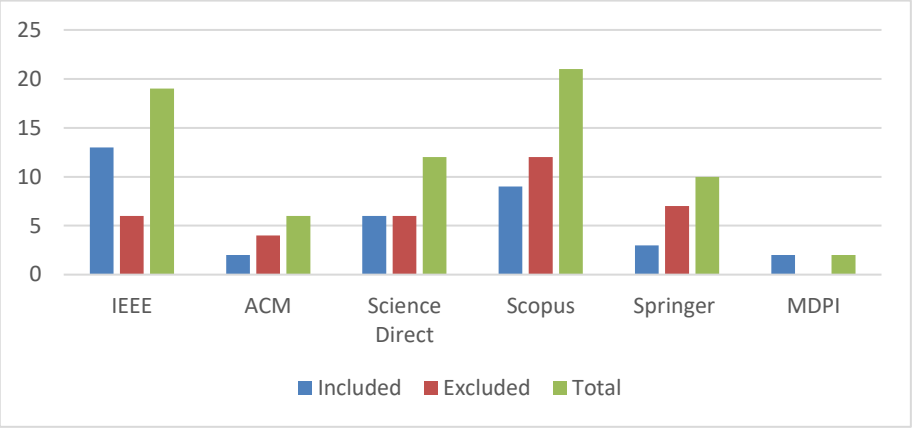

Figure 3. Database Statistics

Table 8. Database Statistics

Database	Included	Excluded	Total
IEEE	**13**	**6**	**19**
ACM	**2**	**4**	**6**
Science Direct	**6**	**6**	**12**
Scopus	**9**	**12**	**21**
Springer	**3**	**7**	**10**
MDPI	**2**	**0**	**2**

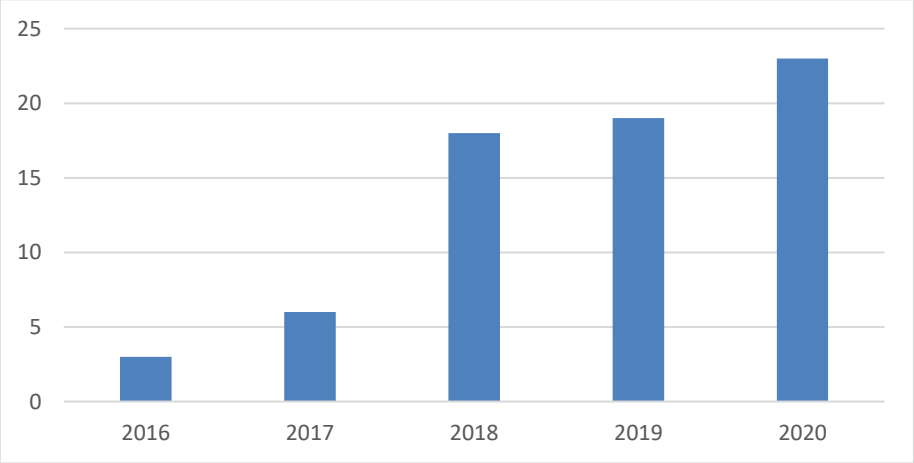

Figure 4. Frequency of Studies

Table 9. Extracted Vulnerabilities

#	Vulnerability	Frequency	#	Vulnerability	Frequency
1	DDoS or DoS	19	12	Impersonation	4
2	Data leakage	13	13	Spoofing	4
3	Eavesdropping	11	14	Brute force attack	3
4	Forgery	11	15	Insecure communication	2
5	MITM	10	16	Abuse attack	2
6	Lack of authentication	7	17	Jamming or interruption attacks	2
7	Unauthorized access	6	18	Lack of encryption	1
8	Malicious code injection	6	19	Open ports	1
9	Over privileged	5	20	Masquerade attack	1
10	Replay attack	4	21	Gain initial access	1
11	Physical attack	4	22	Unsecured interfaces	1

4.3 Qualitative Analysis

In this section researched questions were answered and explained in detail to pave the way for the conclusion. In this section the analysis is descriptive, however, it is complemented with quantitative analysis to answer the research questions. The similarities and differences are highlighted in this analysis [7].

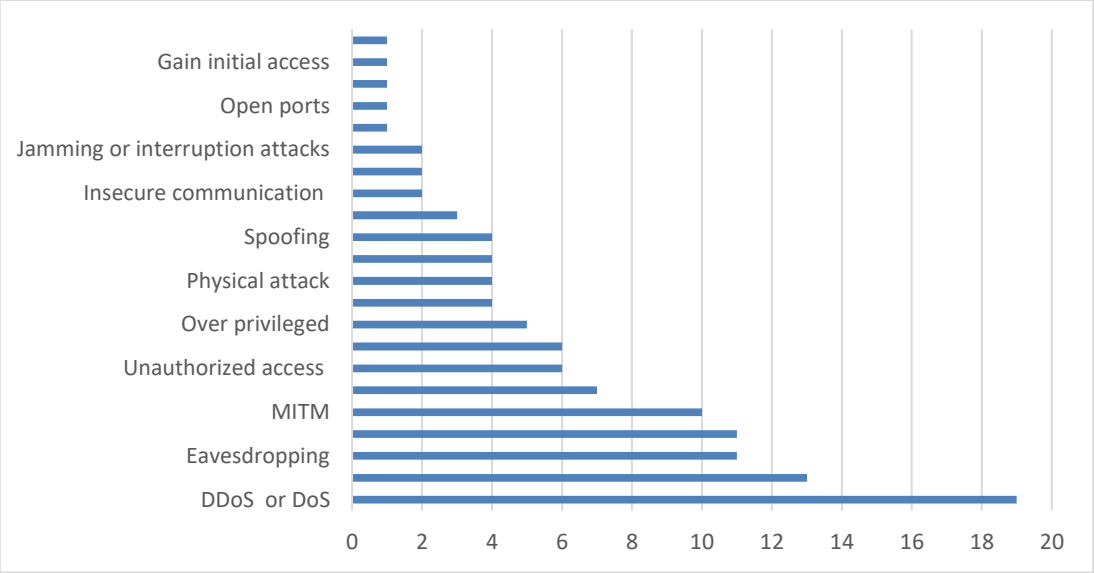

Figure 5. Most Common Attacks

Table 10 Area of Interest in Smart Homes

Concerns	Frequency	Studies
Authentication and secure communication protocol	16	[16], [17], [18], [19],[20], [21], [22], [23], [48], [25],[26], [27], [28], [29],[30], [31]
Study of security and privacy challenges	7	[32], [63], [33], [34], [24], [35]
Analysis of a smart home device security	4	[36], [28, [38], [40]
Attacks detection method	4	[40], [41], [42], [43]
Examination of specific attacks on smart homes	4	[44], [45] [37], [46],[47]

RQ1: What research are conducted in the area of smart home security within the last five years?

In the last five years, the demand for smart home systems and devices has increased exponentially due to the benefits it brings to conventional homes. These increases attracted researchers' attention to its weak points. Figure depicts the active area of search in smart homes security expanded directly with sales of these devices. From the collected prime studied the researchers demonstrated interest in five areas (Table 10): authentication and secure communication protocol, the study of security and privacy challenges, analysis of a smart home device security, attacks detection method, and examination of specific attacks on smart homes.

RQ2: What are the categories of attacks (threats) smart homes are exposed to?

From Table we extracted 22 unique threats. These threats can be classified according to IoT layers. There are three main layers: the perceptual layer, network layer, and application layer [14]. Although some of the collected prime studies focus on one type of attack, however, from the collected prime studies there are different attacks classifications. In [32] the researchers classify attacks into four categories: physical, network, software, and encryption. In [45] [37] classified attacks into IoT five layers: physical, network, processing, application, and business. Similarly, [35] classified attacks into physical, network, middleware, and application. In [25], [34] and [19] they classify the attacks under the umbrella of the CIA triad (confidentiality, integrity, availability). In [42] and the researchers only focused on the software attacks class. The rest of the selected studies have only one class which is network or communication because they focus on specific attacks related to the network layer. Table summarizes the attack categories in the selected prime studies.

Table 11. Attacks Categories

Classification	Articles
Network Layer	24
Software layer	2
CIA triad	3
Physical, network, software, encryption	1
Physical, network, processing, application, business	1
physical, network, Middleware, application	1
Software, hardware, information, communication, human	1
Based on the attacker goals	1
Communication or authentication attacks	1

RQ3: What are the existing countermeasures to mitigate smart homes attacks?

The collected prime studies are divided into two groups, studies that discuss the security and privacy of smart homes in general and studies that focus on special vulnerabilities. This is reflected in the proposed mitigation solutions in these studies. From the extracted data we infer that the countermeasures can be divided into four classes: authentication solutions, detection, and identification solutions, blockchain-based solutions, communication solutions, and the last class containing solutions that do not belong to any classes (Table 12).

Table 12. Countermeasures Classifications

Countermeasure	Frequency
Authentication	9
Detection and identification	8
Secure communication	6
Blockchain-based	3
Others	8

4.4 Authentication Solutions

The referenc in [25] proposed a credential-less authentication lightweight framework to combat over-privileged and open ports vulnerabilities. [26] designed anti-tracking mutual authentication scheme with a key agreement based on IFTTT service to improve authentication when remotely accessing smart homes systems. Where [38] proposed self-signing and access control techniques that prevent data modification or leakage by an authorized party. The reference in [27] claims their proposed anonymous authentication scheme provides a more secure communication medium than exiting authentication solutions. The reference in [28] states that their three Three-factor mutual authentication protocol for multi-gateways systems proved immunity against user impersonation, spoofing, and session key disclosure found in existing two-factor authentication. In [29] proposed lightweight mutual authentication protocol designed for heterogeneous smart homes environment. Since smart homes devices and users communicate over insecure medium [30] propose an anonymous authentication scheme using ECC that doesn't keep authentication table, this random number generator method combat attacks like a replay. In [31] propose user authentication method using the JSON Web Token and International Mobile Equipment Identity to solve the problem of untheorized devices in smart homes which are abused by hackers.

4.5 Detection and Identification Solutions

The referenc in [41] proposed an intrusion detection system based on a supervised approach to detect network attacks on smart homes systems. A novel approach to detect threats proposed in [17] by power profiling in smart home devices. The referenc in [44] designed a tool to detect data leakage to combat attacks such as eavesdropping. In [42] took advantage of machine learning capabilities to design anomalies detection schemes in smart homes by investigating the trustworthiness of the devices in a smart home environment. Due to large DoS attacks on IoT smart homes [46] focused on proposing lightweight algorithms to detect DoS attacks based on forecasting and chaos theory. Also,[43] used machine learning to detect threats by the

correlation between homeowner and services provider. In [40] A dynamic intrusion prevention system was designed incorporating user side and service provider. In [39] they detect attack behavior through adaptive smart hub design uses "uses dynamically loadable add-on modules to communicate with diverse IoT devices, provides policy-based access control, limits exposure of local IoT devices through cloaking, and offers a canary-function based capability to monitor attack behaviors".

4.6 Secure Communication

Because of the limited computational limitation in the devices which limits the ability to encrypt session keys in communication between devices. [16] Proposed communication protocol based on a home limited channel to cope with this issue. Similarly, [21] proposed a lightweight session key establishment scheme based on the Diffie-Hellman method. For the same reason, [22] designed a key-free secure communication method based on a home limited channel. In [23] lightweight secure communication protocol was proposed based on the nested lattice technique of the networking layer codding. Baruah et al combat communication attacks using a secure IFTTT-based framework with captcha and one time-based authentication scheme. In [16] designed a session-key agreement scheme based on the Merkle puzzle to establish secure communication.

4.7 Blockchain-based Solutions

The referenc in [19] claims that traditional security controls will not be effective. Therefore, they decided to adopt a decentralized database blockchain technology to overcome conventional IoT security [53] limitations. Similarly, [48] proposed mutual authentication methodology incorporating blockchain technology to overcome the single server exiting solutions. Also, [28] states that single server security controls present vulnerabilities such as integrity, certification, and availability. So that, they proposed a blockchain-based smart home gateway where data is stored in the blockchain.

4.8 Other Solutions

In [36], [63], [33] [34] they suggested multi solutions because they conducted surveys to identify vulnerabilities and map exiting solutions to them. The referenc in [60] conducts ISRA risk analysis to identify threats then map exiting solutions. Similarly, [32] conducted studies on well-known and lesser-known devices and suggested keeping devices up to date as a solution. In [18] they focus on availability vulnerabilities by proposing an edge-of-things solutions which put management of the home at the edge. The referenc in [45] [37] focus on information leakage in smart homes and propose a framework to measure the risk of the devices to give the owner an overview of the risk they are facing.

Table 13. Article's analysis method frequency

Analysis method	Number of Articles
Survey existing literature review	28
Analyze specific attacks	5
Reverse engineering	1
Assets assessment approaches	1

RQ4: What analysis is made to study security aspects of the studied work?

The collected studies for our systematic review vary in analysis method because some focus on specific issues where others survey vulnerabilities in general. The selected 35 studied distributed among four clusters in terms of the analysis method to reach the goal. First, survey existing literature review most common way to identify pitfalls in the interesting issues, then improve upon that. Second, focus on a specific issue or attack and analyze it in terms of security to propose security control or identify vulnerabilities. Third, reverse engineering a device or system which is a common way among security researchers to find security bugs and mitigate them. Fourth, assets assessment conducted to identify the vulnerability magnitude, then suggest a countermeasure based on that. Table present the number of articles relating to the analysis methodology.

RQ5: What are the expected security problems in the future?

The continued expansion of use of IoT devices in homes due to their advantages in modern lifestyles will expand the attack surface. The expected growth in use will make these devices valuable targets for D\DoS attacks since most attacks come from outside the house [34]. This will make these smart homes a hub to initiate attacks against targets. Since there are still no security standards designed for smart homes and more

manufacturers will produce these popular devices, the threats will remain open for a long period and new threats will arise due to neglected security considerations in design phase.

5. Results and Analysis

The motivation behind this research was the growth of the use of IoT devices specifically in smart homes applications. Because such systems give the households a sense of security and control over the house. The smart home system consists of newly emerged IoT-enabled devices known for their limitations. IoT devices limitations have imposed security concerns because security control mechanisms require major computational power. For this reason, we conducted a rigorous systematic literature review to identify the recent vulnerabilities threatening smart homes systems and security control proposed to mitigate these vulnerabilities.

5.1 Systematic Literature Review Findings

We conducted a systematic review using Okoli & Schabram [62] guideline for information systems after comparison with [7] guideline. The systematic literature review provides a rigorous methodology to find the state of the art in smart home security. In addition, a pilot search resulted in not finding a systematic literature review in the field of IoT-enabled smart homes. In search of related previous works, we found 11 articles distributed into three categories: taxonomies, surveys and reviews, and frameworks. Critically analyzing related works, we found these articles identify threats but do not map countermeasures to them. Also, the classification of threat lack uniformity.

5.2 Answering Research Questions

Answering the proposed research question (Table) for our research clarify major challenges in IoT-enabled smart home system.

Analysis of Research Question 1

From the collected prime studies inferred that there are five major areas of concern researchers were active at authentication and secure communication protocol, the study of security and privacy challenges, analysis of a smart home device security, attacks detection method, and examination of specific attacks on smart homes. Out of 35 selected studies, 16 articles focused on authentication and secure communication. The reason behind this is from Table majority of the attack executed at the network or physical layer. Preventing such attacks require authentication and encryption mechanism with high computational power. The nature of IoT devices operates on the low power consumption concept. Thus, these limitations motivated the researcher to find a lightweight efficient to encrypt the transmitted data between devices and gateways. Also, the heterogeneity of these devices in the smart home environment requires an authentication method to ensure the connected devices belonging to the home environment have not been compromised by an attacker to modify the transmitted data. Other groups of researchers addressed the challenges by identifying the threat from different resources to classify them and propose the mitigations mechanism. These threats were obtained from real-life incidents; however, the proposed countermeasure has not been validated. Another method used to obtain threats is by conducting an information assets assessment to highlight the risk prone to these assets. On other hand, there are researchers preferred to propose a novel attack detection instead of identifying threats. Whereas others focused on a specific device such as a smart plug or home gateway to analyze the vulnerabilities threatening them and find the proper mitigation. Likewise, a group of researchers was motivated to examine certain attacks on smart homes practically and find an approach to control them.

Analysis of Research Question 2

The second research question finds the threat categorized in the selected prime studies. As stated in RQ1 the majority of the researchers motivated to investigate attacks related to the network layer, this is reflected in the threats classification. There are 24 articles from the collected 35 classified threats under the network layer only. Only two articles classified attacks under the software layer. Some articles used the CIA triad to classify attacks by knowing which factor of the CIA triad violated in this kind of attack. The rest of the articles concerned about finding challenges in general used variations of IoT architecture layers to classify attacks. We infer there is a variant in categorizes, because of the absence of security standardization in this field. In addition to the variation of IoT architectures used.

Analysis of Research Question 3

After finding threat categorizing in RQ2, we need to find what kind of countermeasures are recommended for these attacks to answer RQ3. Since researchers are motivated to find solutions for network layer attacks, the majority of solutions focused on how to secure communication and authenticate devices. Since smart home systems provide remote access capabilities, some researchers suggested using blockchain technology to overcome traditional centralized approach power limitation security issues. Blockchain provides a decentralized solution to prevent the predication of households. On other hand, instead of focusing on a particular vulnerability, researchers decided to construct attacks detection schemes. Utilizing artificial intelligence, malicious behavior can be predicted to raise the security level at smart homes and prevent as much as possible damage.

Analysis of Research Question 4

As mentioned previously in the conducted pilot research no SLR was found in our domain. The collected 35 prime studies used different methodologies to analyze security aspects. From the selected studies 28 articles conducted surveyed existing literature, which means the found threats identified by previous researchers or from real-life scenarios. Likewise, the article studies specific attacks based on real-life incidents. In previous approaches, the researchers waited for risk to take a place. Risk must be identified beforehand to reduce the damage as much as possible. There is an article that used the reverse engineering method to examine possible attacks on the device. This method is likely to find potential attacks on specific devices not the whole system. Another used approach is to identify the assets in smart home systems, then anticipate potential attacks. This approach might miss risks in the system that does not target certain assets, it targets the entire system. For example, DoS or DDoS attacks which jam the system or use the system components as an attacking center.

Analysis of Research Question 5

With exponential growth in IoT-enabled smart home devices, the attack surface will expand, and new threats will emerge to the surface. This is because the manufacturers still do not take into consideration these devices' security into consideration in the design phase due to current limitations in hardware. However, the collected studies did not expect future risk because the study focused on the current s vulnerabilities encountered.

6. SURVEY

In order to enhance our research work, we conducted a survey. A survey is a research methodology that depends on collecting data from a group of participants in standardized method to avoid any biased data. A survey was conducted to collect a large amount of data in a short time. Surveys aid with collecting information in a particular field or topic from experts in the field. In our case, eliciting information from experts in the field will be through a questionnaire. The questionnaire will be deployed online using google survey in form of a set of unstructured questions which allow the respondents to answer the questions in their own words. It was hard to find experts in the IoT field especially in academia, but we managed to find 12 professors and experts with help of professors in Kuwait University.

The rationale of the questionnaire improves the research results by obtaining information from experts in the current time in the field of the internet of things and security. The contacted experts have no less than 10 years of experience in the field of IoT, artificial intelligent, control, wireless communication information, and cybersecurity. Also, they have no less than 4 publications in the field.
The following asked in the questionaries:

Q1. What are the advantages of using IoT in smart homes?
Q2. What are the risks in using IoT-based smart home devices?
Q3. What are the security techniques used to prevent attacks on smart home systems?
Q4. What are the threats expected in smart homes automation?
Q5. How do we handle the excepted security risks in a smart home?
Q6. What are the advantages of using SLR in your opinion?
Q7. Any other opinions about smart homes?

In summary of survey, question one enhances our statement in the introduction in terms of smart home systems making daily life routines easier and enhancing home security in general. Question 2 conforms to the vulnerabilities extracted from prime studies in Table and the reason for these vulnerabilities is the lack of security standardization. Whereas question three regarding the suggested countermeasures, all suggested security techniques included in answering research question 3 from the systematic review, except for strong password and biometric authentication methods. Because the strong password is related to the human factor

and not related to IoT limitations, and biometric authentications require a high computational process. In question 4 the experts anticipated that will increase demand on smart home devices the attack surface will widen, and more untrustworthy devices will be produced. In question 5 the proper mitigations to handle smart homes risk suggested two-factors authentication which only can be used devices with high computational power in the system such as the connecting hub. Another suggested way to handle risk is to conduct an awareness program for users. Security standardization was suggested, but not feasible because of the heterogenicity of such devices. Similarly, disasters contingency plans are hard to implement due to heterogenicity. Keeping devices up to date plays a significant role in securing smart home devices in terms of software and it was proposed in the result of the systematic review. Threat modeling is a method to identify threats by defining the vulnerable assets of the system then proposing the proper mitigation. Threat modeling will be used in section 5 to simplify the process of identifying the threats and suggested mitigations in smart homes. As for using systematic literature review in our study, the academic professors granted that SLR is an important methodology to collect and compare exiting threats and countermeasures and provide a breadth of search. Also, identify research gaps and find space for improvement. Finally, the experts emphasized the role of smart home systems in making our daily routines easier and the need of improving the security of such systems for a better quality of life.

7. CONCLUSION AND FUTURE WORKS

In conclusion, this study discussed the security challenges encountered by IoT-enabled smart homes. The systematic literature review resulted in 731 articles found from 6 scientific databases. After removing the duplication and filtration process to exclude articles not related to our purpose and research questions 70 articles were left to be examined fully. Then, of the 70 articles examined and assessed, 35 were excluded for not eligibility to be included in our research. The final step is to extract the data from the articles and analyze them quantitively and qualitatively. The quantitative analysis demonstrated that there is growth in published studies since 2015, and most published articles were very recent in 2020. This proves the spread of IoT-enabled smart homes and the published vulnerabilities attracted researchers to be active in this domain. This also explains the low articles number since this is a very young domain of research. Therefore, a roadmap is needed in this domain to guide the coming researcher as we provide in our research.

Additionally, a survey was conducted to elicit the latest challenges from experts in the field. The result was 22 unique threats were identified. As future work, we are planning to create a framework that enables the user to design a smart home system by selecting the components of the smart home system from a predefined list such as smart lock, smoke detectors, or surveillance camera. This tool identifies the threats for each component by checking the CVE database for vulnerabilities and how to mitigate them. If a threat exists for such a component, the framework enables the user to download the patch to mitigate the issue. Otherwise, the framework suggests a proper mitigation procedure to combat the threat. Also, the framework guides the user on how to configure the available features in devices to enhance security. This method adds an active layer of protection for the smart home system and enhances the overall security of the smart home system.

REFERENCES

[1] Karimi, K., & Atkinson, G, "What the Internet of Things (IoT) Needs to Become a Reality", Retrieved June 3, 2024, from https://www.mouser.cn/pdfdocs/INTOTHNGSWP.PDF, 2014.

[2] Smart Home Market Size & Share will hit $53.45 Billion by 2022. (Zion Market Research) Retrieved June 3, 2024, from https://www.globenewswire.com/news-release/2017/04/12/959610/0/en/Smart-Home-Market-Size-Share-will-hit-53-45-Billion-by-2022.html, 2022

[3] Smart home - Statistics & Facts, (Statista) Retrieved June 3, 2024, from https://www.statista.com/topics/2430/smart-homes/, 2024

[4] Liberati, A., Altman, D. G., & Tetzlaff, J, "The PRISMA Statement for Reporting Systematic Reviews and Meta-Analyses of Studies That Evaluate Health Care Interventions: Explanation and Elaboration. Annals of Internal Medicine", 873–880, 2009.

[5] Burhan, M., Rehman, R. A., Khan, B., & Kim, B.-S, "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. Sensors", 18(9), 2796-2833, 2018.

[6] Rehman, S. U., & Manickam, S., "A Study of Smart Home Environment and its Security Threats", International Journal of Reliability, Quality and Safety Engineering, 23(3), 1640005-1640014, 2015.

[7] Kitchenham, B. Procedures for Performing Systematic Reviews. Keele University, 7, 1-26, 2004.

[8] Davis, J., Mengersen, K., Bennett, S., & Mazerolle, L. "Viewing systematic reviews and meta-analysis in social research through different lenses", SpringerPlus, 511-520, 2014.

[9] Aly, M., Khomh, F., Haoues, M., & Quintero, A., "Enforcing security in Internet of Things frameworks: A Systematic Literature Review", Internet of Things, 6, 100050, 2019

[10] Liao, B., Ali, Y., Nazir, S., & He, L., "Security Analysis of IoT Devices by Using Mobile Computing: A Systematic Literature Review", IEEE Access, 8, 120331 – 120350, 2020.
[11] Pico-Valencia, P., & Holgado-Terriza, J. A., "Agentification of the Internet of Things: A systematic literature review", International Journal of Distributed Sensor Networks (IJDSN), 14(10), 1-20, 2018.
[12] Heartfield, R., Loukas, G., Budimir, S., & Bezemskij, A., "A taxonomy of cyber-physical threats and impact in the smart home", Computers & Security, 78, 398-428, 2018.
[13] Anwar, M. N., Nazir, M., & Mustafa, K., "Security threats taxonomy: Smart-home perspective", International Conference on Advances in Computing, Communication & Automation. Dehradun, India, 2017.
[14] Okoli, C., "A Guide to Conducting a Standalone Systematic Literature Review", Communications of the Association for Information Systems, 37(43), 879-910., 2015.
[15] Macedo, E. L., Oliveira, E. A., & Silva, F. H., "On the security aspects of Internet of Things: A systematic literature review", Journal of Communications and Networks, 21(5), 444 – 457, 2019.
[16] Zhang, Y., Huang, X., Chen, X., & Zhang, L. Y., "A Hybrid Key Agreement Scheme for Smart Homes Using the Merkle Puzzle", IEEE Internet of Things Journal, 7(2), 1061 – 1071, 2020.
[17] Majumder, A. J., Veilleux, C. B., & Miller, J. D., "A Cyber-Physical System to Detect IoT Security Threats of a Smart Home Heterogeneous Wireless Sensor Node", IEEE Access, 8, 205989 – 206002, 2020.
[18] Batalla, J. M., & Gonciarz, F., "Deployment of smart home management system at the edge: mechanisms and protocols", Neural Computing and Applications , 1301–1315, 2019.
[19] Arif, S., Khan, M. A., Rehman, S. U., & Kabir, M. A., "Investigating Smart Home Security: Is Blockchain the Answer?", IEEE Access, 8, 117802 – 117816, 2020.
[20] Huang, Z., Zhang, L., Meng, X., & Choo, K.-K. R., "Key-Free Authentication Protocol Against Subverted Indoor Smart Devices for Smart Home", IEEE Internet of Things Journal, 7(2), 1039 – 1047, 2019
[21] Dey, S., & Hossain, A., "Session-Key Establishment and Authentication in a Smart Home Network Using Public Key Cryptography", IEEE Sensors Letters, 3(4), 1-4, 2019.
[22] Ji, X., Li, C., & Zhou, X., "Authenticating Smart Home Devices via Home Limited Channels. Transactions on Internet of Things", 1(4), 1-24, 2020.
[23] Liu, Q., Zhang, W., Ding, S., & Li, H., "Novel secure group data exchange protocol in smart home with physical layer network coding", Sensors, 20(4), 1138-2245, 2020.
[24] Lin, H., & Bergmann, N. W., "IoT privacy and security challenges for smart home environments. Information", 7(33), 44-59, 2016.
[25] Xiao, Y., Jia, Y., Liu, C., Alrawais, A., & Rekik, M., "HomeShield: A Credential-Less Authentication Framework for Smart Home Systems", IEEE Internet of Things Journal, 7(9), 7903 – 7918, 2020.
[26] Lu, Y., & Xu, L. D., "Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics", IEEE Internet of Things Journal, 6(2), 2103 – 2115, 2019.
[27] Banerjee, S., Odelu, V., & Das, A. K., "An efficient, anonymous and robust authentication scheme for smart home environments. Sensors", 20(4), 1215-1234,2020.
[28] Lee, Y., Rathore, S., Park, J. H., & Park, J. H., "A blockchain-based smart home gateway architecture for preventing data forgery", Human-centric Computing and Information Sciences, 10(9), 9-23, 2020.
[29] Bogdan-CosminChifor, Bicaa, I., & Victor-ValeriuPatriciua, "A security authorization scheme for smart home Internet of Things devices", Future Generation Computer Systems, 86, 740-749, 2018.
[30] Shuaia, M., Yu, N., & Wang, H., "Anonymous authentication scheme for smart home environment with provable security", Computers & Security, 86, 132-146, 2019.
[31] Hong, N., Kim, M., Jun, M.-S., & Kang, J., "A study on a JWT-based user authentication and API assessment scheme using IMEI in a smart home environment", Sustainability, 9(7), 1099-2118, 2017.
[32] Davis, B. D., Mason, J. C., & Anwar, M., "Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study", IEEE Internet of Things Journal, 7(10), 10102 – 10110, 2020.
[33] Batalla, J. M., Vasilakos, A. V., & Gajewski, M., "Secure Smart Homes: Opportunities and Challenges", ACM Computing Surveys, 50(5), 1-32, 2017.
[34] Awad, A., & Ali, B., "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes", Sensors, 18(3), 817, 2018.
[35] Sicato, J. C., Sharma, P. K., & Loia, V., "VPNFilter Malware Analysis on Cyber Threat in Smart Home Network", Applied Science, 9(13), 2763, 2019.
[36] Ling, Z., Luo, J., Xu, Y., Gao, C., & Wu, K., "Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System", IEEE Internet of Things Journal, 4(6), 1899 – 1909, 2017.
[37] Lee, J., Yu, S., & K. P., "Secure Three-Factor Authentication Protocol for Multi-Gateway IoT Environments Sensors", 19(10), 2358-2383, 2019.
[38] Kang, W. M., Moon, S. Y., & Park, J. H., "An enhanced security framework for home appliances in smart home Human-centric Computing and Information Sciences", 7(6), 1-12, 2017.

[39] Anthi, E., Ahmad, S., & Rana, O., "EclipseIoT: A secure and adaptive hub for the Internet of Things", Computers & Security, 78, 477-490, 2018.
[40] Pecorella, T., & Pierucci, L., "Network Sentiment Framework to improve security and privacy for smart home", Future Internet, 10(12), 125-139, 2018.
[41] Anthi, E., Williams, L., Słowińska, M., & Theodorakopoulos, G., "A Supervised Intrusion Detection System for Smart Home IoT Devices", IEEE Internet of Things Journal, 6(5), 9042 – 9053, 2019.
[42] Zainab, A., Refaat, S. S., & Bouhali, O., "Ensemble-based spam detection in smart home IOT devices time series data using machine learning techniques", Information, 11(7), 344-359, 2020.
[43] Gajewskia, M., & Batallaab, J. M., "Two-tier anomaly detection based on traffic profiling of the home automation system", Computer Networks, 158, 46-60, 2019.
[44] Beyer, S. M., Mullins, B. E., Graham, S. R., & Bindewald, J. M., "Pattern-of-Life Modeling in Smart Homes", IEEE Internet of Things Journal , 5(6), 5317 – 5325, 2018.
[45] Park, M., Oh, H., & Lee, K., "Security Risk Measurement for Information Leakage in IoT-Based Smart Homes from a Situational Awareness Perspective. Sensors", 19(9), 2148-2172, 2019.
[46] Procopiou, A., Komninos, N., & Douligeris, C., "ForChaos: Real time application DDoS detection using forecasting and chaos theory in smart home IoT network", Wireless Communications and Mobile Computing, 1(14), 1-14, 2019.
[47] Baruah, B., & Dhal, S., "A two-factor authentication scheme against FDM attack in IFTTT based Smart Home System", Computers & Security, 77, 21-35, 2018.
[48] Lin, C., He, D., Kumar, N., & Huang, X., "HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes", IEEE Internet of Things Journal, 7(2), 818 – 829, 2020.
[49] ACM Digital Library . (n.d.). Retrieved from https://dl.acm.org/search/advanced
[50] IEEE Xplore Advacned Search. (n.d.). Retrieved from https://ieeexplore.ieee.org/search/advanced
[51] Internet of Things (IoT). (n.d.). (ENISA), from https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot , Retrieved June 3, 2024.
[52] Internet of Things: What Is IoT? IoT Security. (n.d.). (Kaspersky) Retrieved June 3, 2024, from https://www.kaspersky.com/resource-center/definitions/what-is-iot
[53] IoT security an overview. (n.d.). (Microsoft), from https://azure.microsoft.com/en-us/overview/internet-of-things-iot/iot-security-cybersecurity/, Retrieved June 17, 2024
[54] MDPI Advanced Search. (n.d.). Retrieved from https://www.mdpi.com/about/journals
[55] Publications, R. G. (n.d.). Retrieved from https://www.researchgate.net/search/publication
[56] ScienceDirect Advanced Search. (n.d.). Retrieved from https://www.sciencedirect.com/search
[57] Scopus Document Search. (n.d.). Retrieved from https://www-scopus-com.kulibrary.vdiscovery.org/search/form.uri?display=basic
[58] SpringerLink Avanced Search. (n.d.). Retrieved from https://link.springer.com/advanced-search
[59] The 18 Most Popular IoT Devices, (Software Testing Help) Retrieved June 3, 2024, from https://www.softwaretestinghelp.com/iot-devices/, April 16, 2024.
[60] Jacobsson, A., Boldt, M., & Carlsson, B., "A risk analysis of a smart home automation system", Future Generation Computer Systems, 56, 719-733, 2016.
[61] Mocrii, D., & Chen, Y., "IoT-based smart homes: A review of system architecture, software, communications, privacy and security", Internet of Things, 1(2), 81-98, 2018.
[62] Okoli, C., & Schabram, K., "A Guide to Conducting a Systematic Literature Review of Information Systems Research", SSRN, 26(10), 1-51, 2010.
[63] Stellios, I., Kotzanikolaou, P., & Psarakis, M., "A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services", IEEE Communications Surveys & Tutorials, 20(4), 3453 – 3495, 2018.

BIOGRAPHY OF AUTHORS

Abdullah Ali Ben-Nakhi is an Associate Computer Engineer at State Audit Bureau of Kuwait. (September 2015 – Present) where he completed lot of computing security projects; Servers and virtual machine administrator, Disasters recovery planning, Access control and managing users' permissions on different level of systems, Harden operating systems security, Harden operating webservers security, Prototyping and designing mobile application, Maintaining electronic archiving system and etc. Mr. Adullah graduated in 2014 from Portland State University, Portland, Oregon, USA. He also completed his master in Computing Information Systems in 2022 and his email: bennakhi1@gmail.com

Mostafa Abd-El-Barr received his PhD degree from the Department of Electrical and Computer Engineering, University of Toronto, Canada in 1986. He was with the Department of Information Science, College of Computing Sciences and Engineering (CCSE), Kuwait University 2003-2020. He was also an Adjunct Professor with the ECE Department, University of Victoria (UVic), BC, Canada 2009-2020. He is now the Chairman of the Electrical Engineering Department, Badr University in Egypt. His research interests include Information Security, Design and Analysis of Reliable & Fault-Tolerant Computer Systems, Computer Networks Optimization, Parallel Processing/Algorithms, Multiple-Valued Logic (MVL) Design & Analysis, VLSI System Design, and Digital Systems Testing. He is the author and/or co-author of more than 185 scientific papers published in journals and conference proceedings/symposia. He has three books published (two are translated to the Chinese Language).

Kalim Qureshi is an Associate Professor of the Information Science Department at Kuwait University, Kuwait. His research interests include network parallel distributed computing, thread programming, concurrent algorithms designing, task scheduling, performance measurement and medical imaging. Dr. Qureshi receive his Ph.D and MS degrees from Muroran Institute of Technology, Hokkaido, Japan in (2000, 1997). He published more than 70 journal papers in reputed journals. His email address: kalimuddin.qureshi@ku.edu.kw.