IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 6, 2020, accepted June 28, 2020, date of publication July 1, 2020, date of current version July 13, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3006358

Security Analysis of IoT Devices by Using Mobile Computing: A Systematic Literature Review

BIN LIAO[1], YASIR ALI[2], SHAH NAZIR[2], LONG HE[1], AND HABIB ULLAH KHAN[3]

[1]Office of Cyber Security and Informatization, Fuzhou University, Fuzhou 350108, China
[2]Department of Computer Science, University of Swabi, Swabi 23430, Pakistan
[3]Department of Accounting and Information System, College of Business and Economics, Qatar University, Doha 2713, Qatar

Corresponding authors: Long He (helong@fzu.edu.cn) and Yasir Ali (yasiuop007@gmail.com)

ABSTRACT Internet of Things (IoT) devices are operating in various domains like healthcare environment, smart cities, smart homes, transportation, and smart grid system. These devices transmit a bulk of data through various sensors, actuators, transceivers, or other wearable devices. Data in the IoT environment is susceptible to many threats, attacks, and risks. Therefore, a robust security mechanism is indispensable to cope with attacks, vulnerabilities, security, and privacy challenges related to IoT. In this research, a systematic literature review has been conducted to analyze the security of IoT devices and to provide the counter-measures in response to security problems and challenges by using mobile computing. A comprehensive and in-depth security analysis of IoT devices has been made in light of mobile computing, which is a novel approach. Mobile computing's technological infrastructures such as smartphones, services, policies, strategies, and applications are employed to tackle and mitigate these potential security threats. In this paper, the security challenges and problems of IoT devices are identified by a systematic literature review. Then, mobile computing has been used to address these challenges by providing potential security measures and solutions. Hardware and software-based solutions furnished by mobile computing towards the IoT security challenges have been elaborated. To the best of our knowledge, this is the first attempt to analyze the security issues and challenges of IoT in light of mobile computing and it will open a gateway towards future research.

INDEX TERMS Internet of Things devices, security, mobile computing, mobile applications, smartphone.

I. INTRODUCTION

The security and privacy in the internet of things (IoT) has been remained a serious concern due to the heterogeneous nature of large scale devices and its vulnerability in the operating environment. The numbers of IoT devices are drastically increasing, according to [1], the number of devices in 2017 are 8.4 billion with an increase 31% is expected to rise to 33% by the end of 2018. But, on other hand, the applications of IoT devices are encompassing the various domains from smaller scales to larger ones such as from smart Gird to smart City. However, this popularity of IoT devices is delimited by the cyber-attacks and security threats. According to HP analysis several common IoT devices experience an average of 25% vulnerabilities per device. This trend in IoT led to provide the serious security solutions. IoT devices suffer from computational processing, low power and limited memory [2]. IoT system is composed of three components such as a sensing unit having large number of sensors, actuators and mobile terminals to detect the physical environments [3]. This fragile and simple structure of IoT makes it more vulnerable to the threats related to security of IoT. Besides, IoT devices suffer from other various security issues and challenges. These security issues and challenges were addressed by various approaches by different authors. But, we systematically reviewed the analysis of IoT based devices by using the concepts of mobile computing. To address the security issues after analysing all the major threats, we integrated the mobile computing in IoT system. Mobile computing not only provides hardware but also provides software based solutions affiliated with the security of IoT devices. The communication among the IoT devices is machine to machine (M2M) without the involvement of human but mobile computing is more intelligent due the human to machine interaction. In hardware based solutions, the mobile computing provides more intelligent devices such as computers, Persona digital

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

assistants PDAs, smart phones, notebooks, handheld computers etc. unlike IoT based system, where only sensors, actuators and processors are used. Security procedures and policies within smartphone, laptop, palmtop etc. is more robust and efficient. These devices can be connected with IoT devices to secure them like smartphone can be used as controller home automation system and IoT devices can be authenticated by using smart phone as QR-code authenticator [4], [5]. The mobile devices can also be used as IoT middleware that is designed specifically for low powered resource constrained to process data easily from sensors [6].

Similarly, mobile computing through various applications, services or other infrastructure could affect the IoT devices security. In this regard, the mobile applications and IoT will be the most disruptive class of technologies in the next 10 years [7]. The mobile applications in context of IoT management can play a vital role. The IoT devices vulnerability could be easily compromised, the IoT mobile apps can be reckoned as helpful to disintegrate this vulnerability but the development of such apps could be challenging task as such apps are not like mobile applications because they contain web, mobile and networking components.. The IoT has many applications and thus it is needed to collect personal information, IoT is experiencing some more serious privacy security risks [8]. Similarly, the current IoT devices available in market with lousy security, leading to vulnerabilities that will ''affect flesh and blood'' [9]. We need some solutions to address these security and privacy risks. In this paper, our focus will be to highlight and analyse the threat, vulnerabilities, attacks of IoT devices and then to provide reasonable security and privacy measures and defence techniques in light of mobile computing. In this paper, we present a systematic approach to highlight these threats, attacks, vulnerabilities and then provide approaches based upon mobile computing, which could answer the questions raise on the privacy and security of IoT.

II. MOTIVATION

The main motivation that led to pursue this research was due to the ubiquitous and pervasive nature of IoT devices. Strong security is the dire need to the rapid rise in IoT devices and cyber-attacks [10]. The motivation behind research work awakened due to the many factors but the most prominent reasons are:

- **i.** The exiting research made on IoT did not provide any security measures based on mobile computing, so, there exists a huge gap of pursuing research in IoT based on mobile computing thus the security through mobile computing will enhance the underlying security mechanisms and will open a new gateway for research in future.
- **ii.** Security of IoT is intriguing field of research for the last ten years in field of wireless communication and mobile computing. Exorbitant researches have been made in IoT to address the security issues of IoT.
- **iii.** Similarly the rapid development of IoT supporting technologies, the security problems are becoming serious which has grabbed the people's attentions [8]. The IoT has wide range of applications in various application domains from smart city to the smart grid.

This motivation comes as the IoT security have never been worked before through mobile computing. So, this will become a future research trend to evaluate the security of IoT system based upon the concepts of mobile computing.

The remaining research paper is divided into five sections. In section III, related work has been discussed, in section IV, SLR protocol has been discussed along with steps, in section V, overview of selected studies and results are elaborated. In section VI, Threat to validity are discussed, in section VII limitations and section VIII conclusion is highlighted.

III. RELATED WORK

IoT devices are pervasive and ubiquitous in nature as per predication the number of IoT devices to be 50 billion by 2020 [11]. With rise of this mammoth elevation in number, security has become burning issue and has grabbed a great deal of attention in last few years. Security is important from device to device as it deals with the end-to end communication between individual devices [12]. The strong security is the dire need of IoT due to the rapid rise in IoT devices and cyber-attacks [10]. In this regard, various reviews have suggested mechanisms to cope with the security problems and challenges of IoT. Security analysis of IoT by using systematic approach has been performed by different authors with different aspects but the main focus of this research work is to analyse the security of IoT by using the concepts of mobile computing. The security analysis of IoT by using mobile computing is novel approach and it is the first attempt to analyse the security of IoT devices in light of mobile computing.

Systematic approaches for security analysis of IoT are discussed like Mohammadi *et al.* [13] performed SLR and presented trust based IoT recommendation techniques. Bhandari and Gupta [14] performed a systematic review based upon fault analysis of IoT. Fazal *et al.* [15] analysed the security of IoT through systematic approach and they focused upon highlighting and classifying the security challenges at three different aspects such that hardware, network and cloud server. Aly *et al.* [16] systematically analysed the security issues pertaining to IoT based upon different layers. Macedo *et al.* [17] conducted SLR to analyse the security based upon four security aspects such as trust, access control, data protection, and authentication. Martínez *et al.* [18] highlighted threats, attacks, challenges and countermeasures related to security of IoT. Similarly, Witti and Konstantas [19] evaluated the existing security and privacy issues by systematic mapping study. Sultan *et al.* [20] analysed the security issues and provided the solution by using block chain technology. The current literature about the security analysis of IoT devices is categorized as depicted in Table 1.

TABLE 1. Techniques wise literature categorization.

Ref. No	Techniques/ Research method	Year	Domain	Description
[21]	Research article	2017	IoT	Focuses upon requirement based security analysis of IoT
[22]	Review article	2015	IoT	Analysed the IoT security challenges, issues and open problems
[23]	Survey	2018	IoT	Discusses the layer based security analysis of IoT
[24]	Survey	2018	IoT	Architecture based analysis in light of security requirements
[25]	Security model	2019	IoT	Risk assessment model for addressing the security issues in IoT ecosystem
[26]	Framework	2018	IoT	Discusses the problem analysis of IoT layers and provided proposed solution
[10]	Review	2018	IoT	Threat and attack based analysis of IoT
[9]	Survey	2018	IoT	Analysis of all security areas in IoT
[27]	Review	2015	IoT	Discusses security aims, goals and vulnerabilities for IoT
[28]	Survey	2019	IoT	Threats and attack based analysis of IoT
[29]	Survey	2016	IoT/Mobile computing	Security issues and challenges of IoT and mobile computing
[30]	Research article	2018	Mobile computing	Security analysis of mobile device to device network using Android operating system
[31]	Research article	2018	IoT/Mobile computing	Security analysis of Mobile health applications for testing functionality.
[32]	Survey	2016	IoT/Mobile computing	Security analysis of smart phone in IoT
[11]	Review	2016	IoT	Analysis of identification of application, Threats and impacts in IoT
[4]	Review	2018	IoT/Mobile computing	Study of existing and proposed countermeasures in IoT based system
[1]	Review	2018	IoT	Study of current security advances and protecting methods in IoT
[33]	Review	2018	IoT	A study of vulnerability, privacy and security concern for IoT
[34]	Tool/Research	2017	IoT/Mobile computing	Proposed a mobile application tool for analysis of IoT threats.
[35]	Tool/Research	2017	IoT	Presented a threat categorization based on security dimensions like integrity, confidentiality, etc
[36]	Classification Model	2017	IoT	Proposed a classification model to analyse the relation between potential risk and potential vulnerabilities in home automation devices
[37]	OWASP framework	2018	IoT	Performed complete analysis of relevant IoT attack surfaces and vulnerabilities from IoT OWASP framework
[38]	Survey	2018	IoT	Discusses the threat classification and vulnerabilities of IoT
[13]	SLR	2019	IoT	Studies trust based IoT recommendation techniques in IoT environment
[39]	Low-power and Lossy network (RPL) protocol	2018	IoT	Used a protocol for assessment of vulnerabilities in IoT network

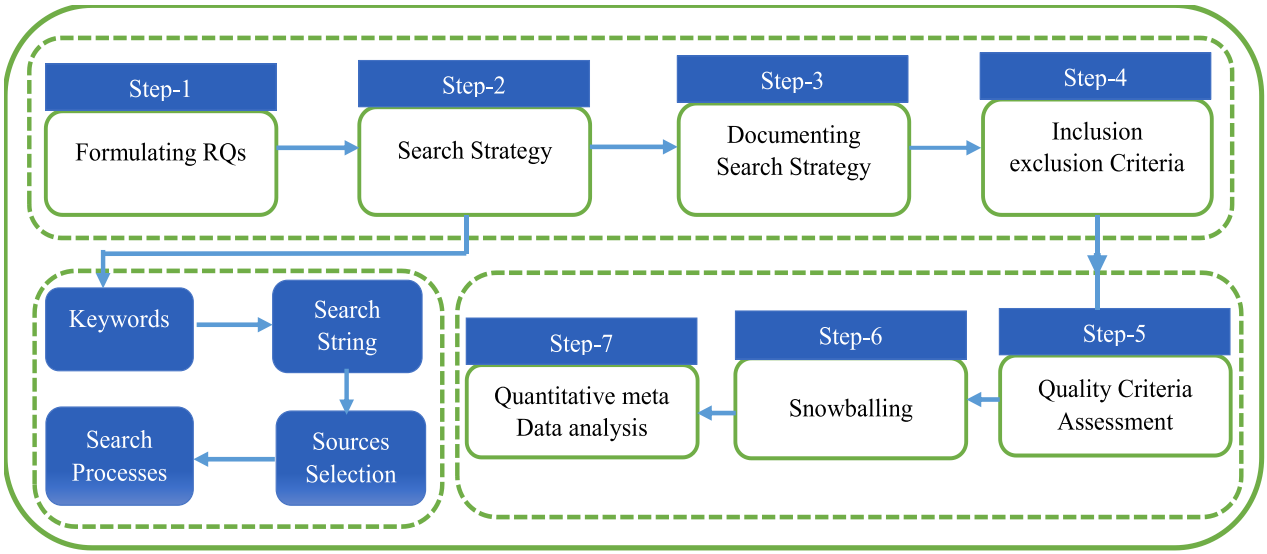


FIGURE 1. SLR design.

TABLE 2. Research questions, description and motivation.

Research Question	Description and Motivation
RQ1. What are the security problems and challenges faced by IoT devices inside a network?	The question focuses upon to get a deep sight into the security concerns and challenges of IoT devices in network without the involvement or support from mobile computing
RQ2. How mobile computing provides security options to enhance the security of IoT devices?	This questions is aimed to provide a security solutions towards the IoT security of IoT by using technological features of mobile computing
RQ3. What are the available security techniques employed for IoT device and mobile phone? What are drawbacks and accuracy of mobile phone techniques?	A comparative analysis of security techniques, frameworks, or tools of both IoT device and smart phone have been discussed. How smart phone is more reliable in terms of handling threats and risks affiliated with malwares and attacks. The susceptibility IoT device is investigated in this question.
RQ4. What are the software based security solutions (Apps) provided by mobile computing for IoT devices?	The main idea is to understand that how mobile applications can be used as a security option for IoT devices in the network

IV. RESEARCH METHOD

Our systematic literature review inspired by [40]. This systematic literature review was performed in order to address the formulated questions carefully in concrete manner. A deep analysis was performed based upon the collection of studies and the most relevant studies, addressing the formulated questions were documented. The whole focus of this SLR is to obtain the most relevant papers from the primary sources. These papers were interpreted and evaluated for the purpose of capturing the best results. The main theme of SLR is to define a protocol is free from biasness [41]. We made same efforts to minimize the element of biasness to bring the objectivity. Our SLR design is composed of series of steps as shown in Figure 1.

The steps included in SLR protocol in sequential fashion are as: defining research questions, designing search strategy, documenting search strategy, inclusion and exclusion criteria, quality criteria assessment and quantitative meta-data analysis. All these steps are discussed in next section.

A. RESEARCH QUESTIONS

The prime purpose of this systematic literature review is to define questions which could encompass the security and to provide answers to the questions in concrete manner. The research questions laid the foundation of discussion about the privacy and security measures that could be adopted to analyse the IoT environment by using the concept of mobile computing. In this research work, four research questions were formulated and they were answered based upon our collated studies. The motivation and descriptive detail about these questions have been listed in Table 2.

B. SEARCH STRATEGY

The search strategy plays an important role in any research so our focus was to organize our search strategy well. In this step of SLR protocol, the first step was to form a search string from the keywords. Only keywords are not enough for searching papers, it has to be combined in different combinations to form a string for different Journals and digital libraries [42]. Our search strategy was inspired by [43]. Search strategy was composed of four steps i.e. defining keywords, forming search string, selection of sources and search process.

1) DEFINING KEYWORDS

Keywords were defined for individual questions to get the most relevant results of papers. The list of all various keywords made for searching purposes are shown in Table 3.

TABLE 3. RQs with keywords.

Research Questions	Keywords
What are the security problems and challenges faced by IoT devices in the network?	"Security Problems*" OR Security Difficulties" OR Security Challenges" AND "IoT OR Internet of Things*"
How mobile computing provides security options to enhance the security of IoT devices?	"IoT OR Internet of Things*" AND "*Security Options OR "Security features *" Security opportunities" AND "Mobile computing*" OR" Nomadic Computing"
What are the available security techniques employed for IoT device and mobile phone? What are drawbacks and accuracy of mobile phone techniques?	"Security Techniques" Security Frameworks" OR "Security Models" OR "Security Schemes" OR "Security Tools" AND "IoT OR Internet of Things*" AND "Mobile phone" OR "smart phone" AND "Drawbacks OR "Shortcomings" AND "Accuracy"
What are the software based security solutions (Apps) provided by mobile computing for IoT devices?	"Softwares*" OR "Applications*" OR "Apps*" AND "Mobile computing" OR "Nomadic Computing" AND "IoT" OR "Internet of Things*"

Search string for the main topic was formed by using the keywords of individual questions. Formulated questions were also searched by using these keywords in order to obtain the most relevant data about our topic.

2) FORMING SEARCH STRING

A search string was formed based on the keywords for individual questions. This was validated by experts in the field of IoT and wireless networking. The search string was checked on the searching sources and it was modified till the best relevant results. Search string was formed by following [44].

(a) Derivation of major terms from topic and research questions

(b) Identification of alternating spellings or synonyms for major terms

(c) Keywords identifications

(d) Use of Boolean operator OR for synonyms or alternating spellings

(e) Linkage of major terms with Boolean AND operator

As a result of above procedure the following search string was created.

(Security OR Protection OR safety) AND (Internet of Things OR IoT) AND (Mobile computing OR Nomadic computing) AND (Assessment OR Evaluation OR Analysis).

Pilot searches were conducted for the purpose of producing the best results and refining our search. Our search string is composed of two parts on focuses upon the security of IoT and second part describes the mobile computing.

3) SELECTION OF SOURCES

The following libraries and data base sources were used for the purpose of collecting data. These libraries are the most relevant and cover the many aspects about the area of our discussion. These libraries provide easy to use and powerful search engines and are more suitable for automatic search [45]. The list of these libraries is given in the Table 4.

4) SEARCH PROCESS

Our search query was performed in September, 2019. In order to find the relevant primary studies both automatic and manual searches were performed. According to [44], automatic research is better than manual research. A manual search was performed to validate the search string. The above mentioned search string was run on all of databases listed in Table 4. This search string retrieved 1651 search results on Science Direct, ACM digital library returned 3137 search results, Springer produced 197,602 results, IEE Xplore digital library fetched 276 results, Hindawi returned 171 search results.

TABLE 4. Online data sources.

Database Source	Link or Website
ACM	http://dl.acm.org
Science Direct	http://www.sciencedirect.com
Springer	http://link.springer.com
IEE Xplore	http://ieeexplore.ieee.org
Wiley/Hindawi	http://Hindawi.com
Taylor and Francis	https://www.tandfonline.com

C. DOCUMENTING SEARCH STRATEGY

Our search strategy documentation inspired by [46]. In this step a document was prepared which consisted of all details about our search strategy. The list of included and excluded papers was also documented and its detail has been shown in Table 5.

The details about search strategy based upon the defined search string were also noted like date of search, name of online libraries, number of records retrieved. The output of this step is a report that contains all detail about search strategy. This documentation helps in assessment of search

TABLE 5. Included and excluded studies detail.

Journal Name	Included	Excluded	Total
ACM	19	50	69
IEEE	34	105	139
Science Direct	26	93	119
Springer	24	29	53
Taylor and Francis	6	30	36
Wiley	3	12	15
Hindawi	3	32	35
Other	2	23	25
Total	**117**	**374**	**491**

TABLE 6. Document of search strategy.

Source	Date Accessed	# of results retrieved without filter	# of results with filter (by years)
ACM	7.9.2019	9,342	5,779
Science Direct	3.9.2019	7,119	6,029
Springer	30.8.2019	97,714	7,333
IEEE Xplore	7.9.2019	470	430
Hindawi	8.9.2019	171	171
Wiley	10.9.2019	20	05

TABLE 7. Inclusion and exclusion criteria.

Inclusion Criteria
Research papers published in English language were included
Primary studies i.e. original research papers were selected
Research papers, book chapters or magazines relevant to our main topic were selected
Research papers ranges in years from 2011 to 2019 were included for the studies
Exclusion Criteria
Papers written other than English language are not included
Papers did not answer research questions or did not define the topic properly were excluded
Gray papers were excluded
Elimination of duplicated papers
Research papers with less than three pages were removed

and allows to keep track of search. The complete detail of documenting search has been depicted in Table 6.

D. INCLUSION AND EXCLUSION CRITERIA

The details of inclusion and exclusion criteria have been explained in Table 7.

The selection of included papers were scrutinized by applying above inclusion and exclusion criteria. In first attempt, redundant papers were removed and then each paper was checked against the defined keywords and formulated research questions. Those papers were excluded, which failed to provide meticulous answers to the questions. Then, each paper was considered based upon title, abstract and then by full reading by applying inclusion-exclusion criteria. Studies from peer-reviewed journal, conference proceedings, book chapters, editorial and magazines were selected for including studies. In case of multiple copies of the same paper, the latest, complete, and updated one is selected for including studies and other copies were excluded. Biasness was avoided by conflict analysis through every stage of selection.

E. QUALITY ASSESSMENT CRITERIA

The quality assessment criteria is important for any research. In our research quality assessment was applied after the study selection. The focus of this process is to improve the criteria for selection. The quality assessment questions (QAs) checklist was created, against which each paper was checked in order to select the more relevant studies so that majority of them will furnish answers to our RQs. The quality assessment procedure was based upon [41]. Each study was marked with

TABLE 8. Quality assessment questions.

Q.ID	Quality assessment questions
QA1	Are the aims of research clearly stated?
QA2	Is any security of IoT device or mobile computing reported?
QA3	Any solution provided towards the formulated RQs?
QA4	Does it answer to security of IoT device in light of mobile computing?
QA5	Is the security techniques related to IoT and mobile phone contributes towards this research?

''Yes'', if it was answering the quality assessment checklist, and it was marked ''No'', if it did not answer all questions in quality assessment. Some research papers were found partially answering the QA questions. For this purpose, scores or values has been assigned to each research paper based upon the answering the QA questions. Each question has only possible three answers and scoring is done is such way that ''Yes''=1, ''No''=0 and ''Partial''=0.5. Each paper was evaluated against the QA questions and at the end quality sum was calculated for each research paper. In our quality assessment, based upon quality score 67 papers were rejected. The checklist of quality assessment questions have been listed in Table 8.

In first step QA questions were defined then scale was defined for assigning ranks to the papers based upon QA questions checklist. The aggregate value (A.V) was obtained after summing up the all weightages awarded based upon QA questions. A threshold was defined such as if the A.V was greater than 2.5 then paper was accepted for inclusion and it was less than 2.5 then paper was rejected. The work flow of quality assessment procedure is shown in Figure 2.

Those studies having A.V greater than 2.5 were 117 and they are finally included papers for our studies. All detail of quality assessment has been depicted in Figure 3.

F. SNOWBALLING

Snowballing is important for any research as it takes start from relevant studies and derives further study [44]. In our research both types of snowballing i.e. forward and backward snowballing were performed for the best relevant results. Snowball working procedure was executed in form of steps: in first step 125 papers were identified, in second step after reading titles this figure was reduced to 37, in third step after reading keywords and abstracts it became 17, in fourth

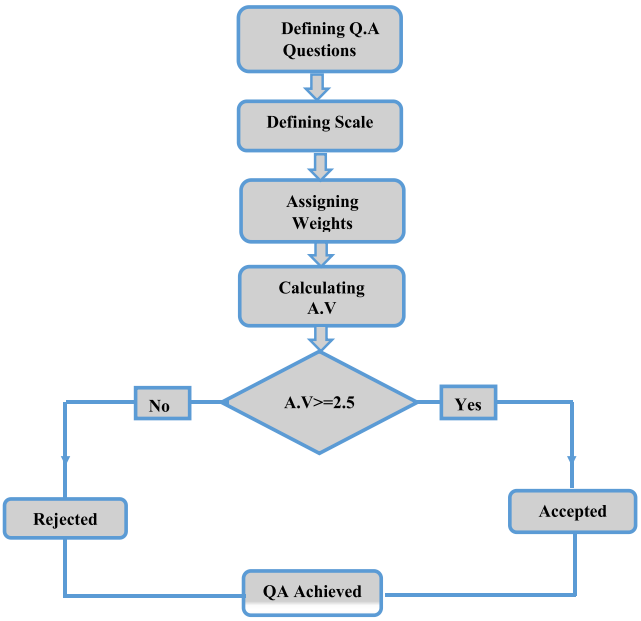


FIGURE 2. Quality Assessment flow chart.

step after reading complete papers, 6 papers were obtained and final step is end of iteration. This iteration continued until no new papers found. Steps involved in snowballing and paper selection procedure for our SLR are depicted in more clear and detailed fashion in Figure 4.

G. QUANTITATIVE META-DATA ANALYSIS

The quantitative meta-data analysis is important to be included in our SLR as it gives the statistical analysis of data about research studies. The literature on quantitative meta-analysis also typically recommends establishing research quality criteria for inclusion decisions [47]. The beauty of this research work is to analyse the data from different perspectives and parameters in order to completely understand the nature and trend about our research area. In quantitative meta-data analysis step, we made in-depth analysis of our collated studies from different perspectives such the detail about the type of document and year of publication in referenced wise fashion is given in Figure 5.

This was also important to understand the research trend about our research area. The number of relevant research papers selected for our research work in term of years has been displayed in Figure 6.

Similarly the distribution of our collated studies in terms of sources has been shown in Figure 7.

The details of all online data bases along with selection criteria of our collated studies have been depicted in figure 8.

The year wise break up of our collated studies has been displayed in Table 9.

V. OVERVIEW OF SELECTED STUDIES

In this section, the research questions answered in detail to meet the research questions objectives precisely clear. The research questions are RQ1, RQ2, RQ3, and RQ4.

A. RQ1. WHAT ARE THE SECURITY PROBLEMS AND CHALLENGES FACED BY IOT DEVICES INSIDE A NETWORK?

This question is intended to provide solution towards the open problems and security challenges confronted by IoT devices. These devices face a lot of security open-problems and challenges. These security problems exist in the form attacks, threats and various sort of vulnerabilities. Security related to the communication and connectivity of these devices is the major security threat and a paramount concern [33]. IoT devices are always vulnerable due the environment in which operating and non-involvement of human. Some of these interconnected IoT devices are mobile devices and could lose connectivity due to vulnerability of wireless outages. Some of them could also run out of the battery life time to operate. Since the nature opened wireless communications are the basic communication way in IoT, which are extremely susceptible to eavesdropping by nature and whose ubiquitous deployment makes security a crucial issue for IoT [80]. IoT devices have many applications in smart home, smart health and smart city but still enormous vulnerabilities are associated with it [11]. The impact of vulnerabilities can by assessed by different ways such as one is the vulnerability assessment of OF of RPL protocol [39]. Other methods like game-theory-based vulnerability quantification method is also used for inspecting the security vulnerability of network over legacy methods [105]. Similarly, the vulnerability can also be assessed by using vulnerability scoring like Common Vulnerability Scoring System (CVSS), which is based on scoring from 0 to 10 [106]. The vulnerabilities of IoT network can also be investigated by using multi-attacker multi-target graphical model [25]. These devices have shown multiple attacks in the past and the reasons of the failures not the availability of requirement of sufficient password length and complexity, not proper encryption of data and vulenrabe interface and firmware [78]. According to this analysis, the IoT devices vulnerabilities in terms of percentages and reasons have shown Figure 9.

IoT devices suffer from enormous security threats due to low cost and power unlike traditional desktop and mobile devices. According to HP report, 70% of the most commonly used IoT devices contain serious vulnerabilities The vulnerabilities in IoT devices arise due to lack of transport encryption, insecure Web interfaces, inadequate software protection, and insufficient authorization [62]. The malware can replicates itself by compromising the connection that links IoT devices [100]. According to [11], [16], [100], the most common IoT vulnerabilities identified have been depicted in Figure 10.

B. RQ2. HOW MOBILE COMPUTING PROVIDES SECURITY OPTIONS TO ENHANCE THE SECURITY OF IOT DEVICES?

IoT devices are not smart enough to cope with security challenges solitarily. These devices need some strong security

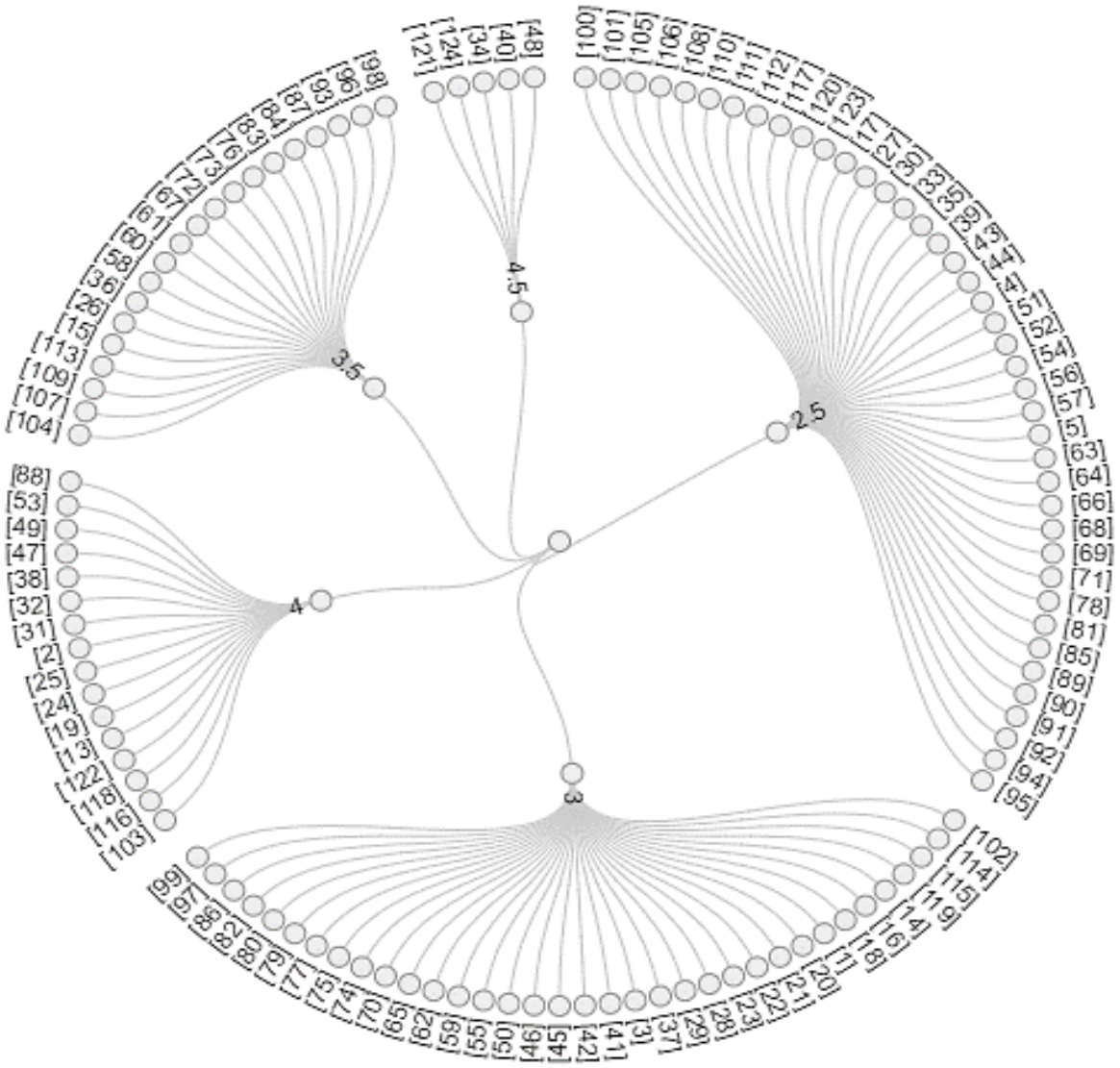


FIGURE 3. Quality assessment detail.

mechanism to cope with vulnerabilities and security challenges. These devices are having small memory to store the security apps or services. The structure of these devices is simple as they are embedded with small processing chip, sensors, actuators and transceivers. Due to this vulnerable and fragile structure, DDOS can be launched which leads to halting of devices and spawns a lot of problems in network. Mobile based technologies are continuously and rapidly increasing due to their ubiquitous and pervasive nature. IoT devices when interact with mobile computing then it is important to address the security issues like unauthorized access to the shared resources. Solution can be tackled by Yaler: software provides a relay infrastructures for secure access to embedded system [29]. In IoT network smartphone phone is important constituent due to collecting a huge amount of data from IoT devices and sending receiving it, if it is hacked then it will halt sending data or it will result in transmission of fake data [32]. The mobile base computing contributes to the IoT in different ways but more importantly the multi sensors embedded in smartphone helps in reducing the barriers associated with mobile computing in context of IoT. The smartphone functions in IoT environment cannot be neglected due to its multi-purpose uses. From security perspective, the mobile computing plays crucial role such as smartphones acts like IoT device controller in IoT environment. These device controllers have sensors to serve a variety of applications that deal with human biometric information, because some of these sensors collect and manage fingerprint, voice, iris, signature, and even behaviour patterns [4]. Sensors integrated in smartphone have advanced capabilities such as measuring proximity, acceleration and location or record audio/noise, sense electromagnetism or capture images and videos [29]. IoT devices lack According to [5], the smart phone can be employed as authentication factor and it facilitates the authentication of each device based on QR-based authentication framework in a user friendly manner. In the

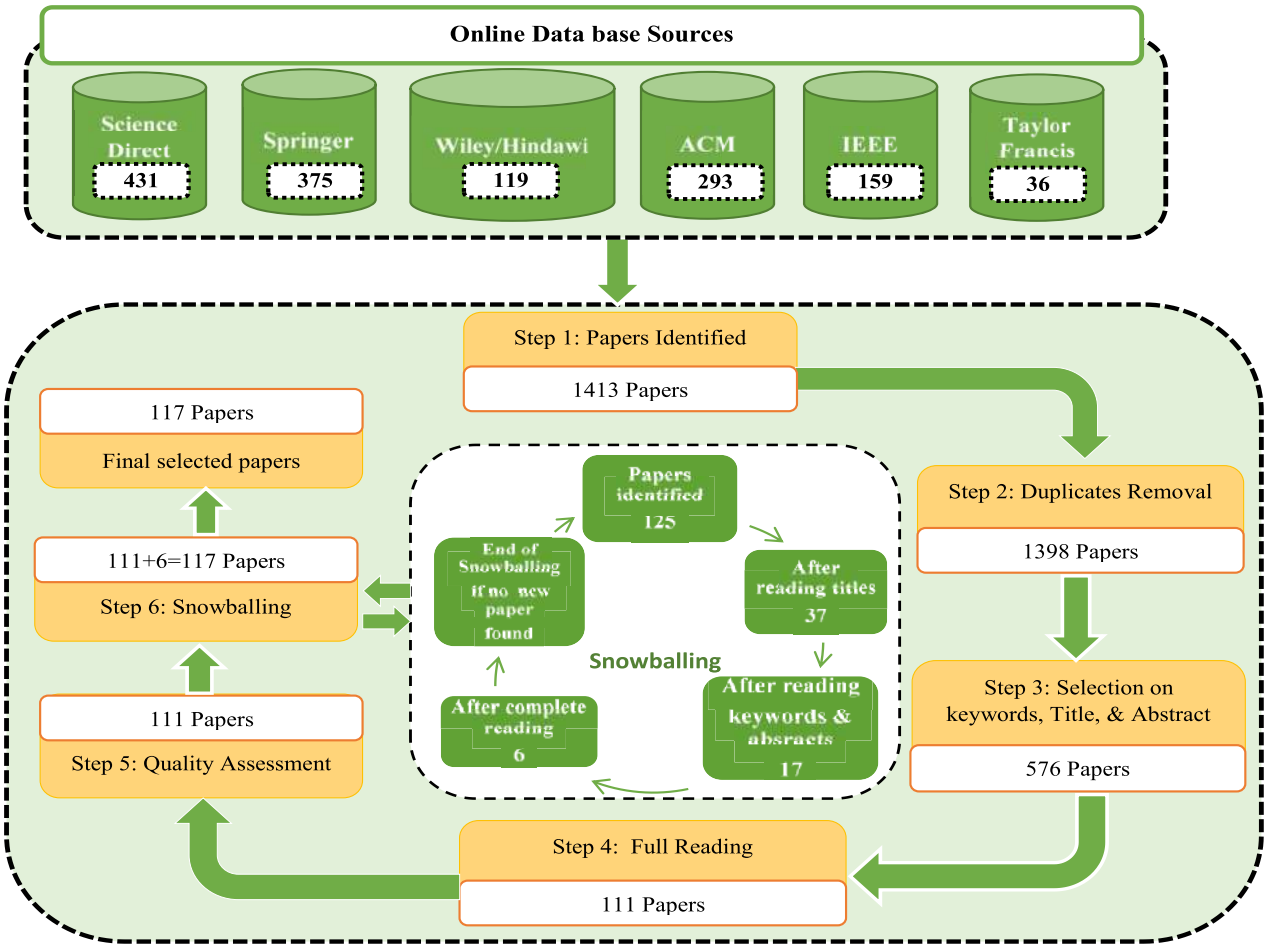


FIGURE 4. Paper selection processes.

FlexRFID middleware IoT architecture, smartphone could be used as an automatic identification and sensing device at the level of the sensing/auto-tracking layer and as a backend device at the level of the application layer, where various users accessing different applications could get the required services [86].

The most low-power IoT devices cannot transmit the collected the data directly to such servers due the limited transmission power and range. Thus, third party devices such as smart mobile phones are used as a relay to establish the communication link between IoT devices and the cloud server. Smart phone can provide a mobile-based relay assistance solution for secure end-to-end connectivity between low-power IoT sensors and cloud servers by using Bluetooth Low Energy (BLE) technology [111].

In modern world mobile devices are indispensable in our everyday life, as their applications are exorbitant. Performing biometric authentication through mobile devices can provide a stronger mechanism for identity verification as the two authentication factors, ''something you have'' and ''something you are,'' are combined [133]. The smartphone ecosystem can be built based on existing ecosystem that allows to define and enforce custom security policies which are necessary for IoT devices and ecosystem [64].

C. RQ3. WHAT ARE THE AVAILABLE SECURITY TECHNIQUES EMPLOYED FOR IOT DEVICES AND MOBILE PHONES? WHAT ARE DRAWBACKS AND ACCURACY OF MOBILE PHONE SECURITY TECHNIQUES?

This question is to explore the various security techniques and frameworks for the security of IoT device and smart phone. In first part of this question, security techniques/frameworks for IoT devices are identified, used for securing IoT devices. Then, security techniques for mobile phones are identified. Mobile phone is considered as integral part of mobile computing. Mobile phone can be used in IoT environment as option to mitigate the impact of threats by providing security options like QR-code and biometric authentication factor, a relay, or as controller (as discussed in previous question) but still there are some malware attacks that can be launched to comprise its security. But, as compared to IoT devices, which are more fragile and vulnerable due to machine to machine interaction. The security risks in IoT devices are very high due to nature of highly dynamics, mobility and not defined perimeters heterogeneity [78].

Both IoT and smart phone devices use sensors and transmit a bulk amount of data over wireless network such as Wifi, RFID, and Blutooth. Security is vital for both devices to send

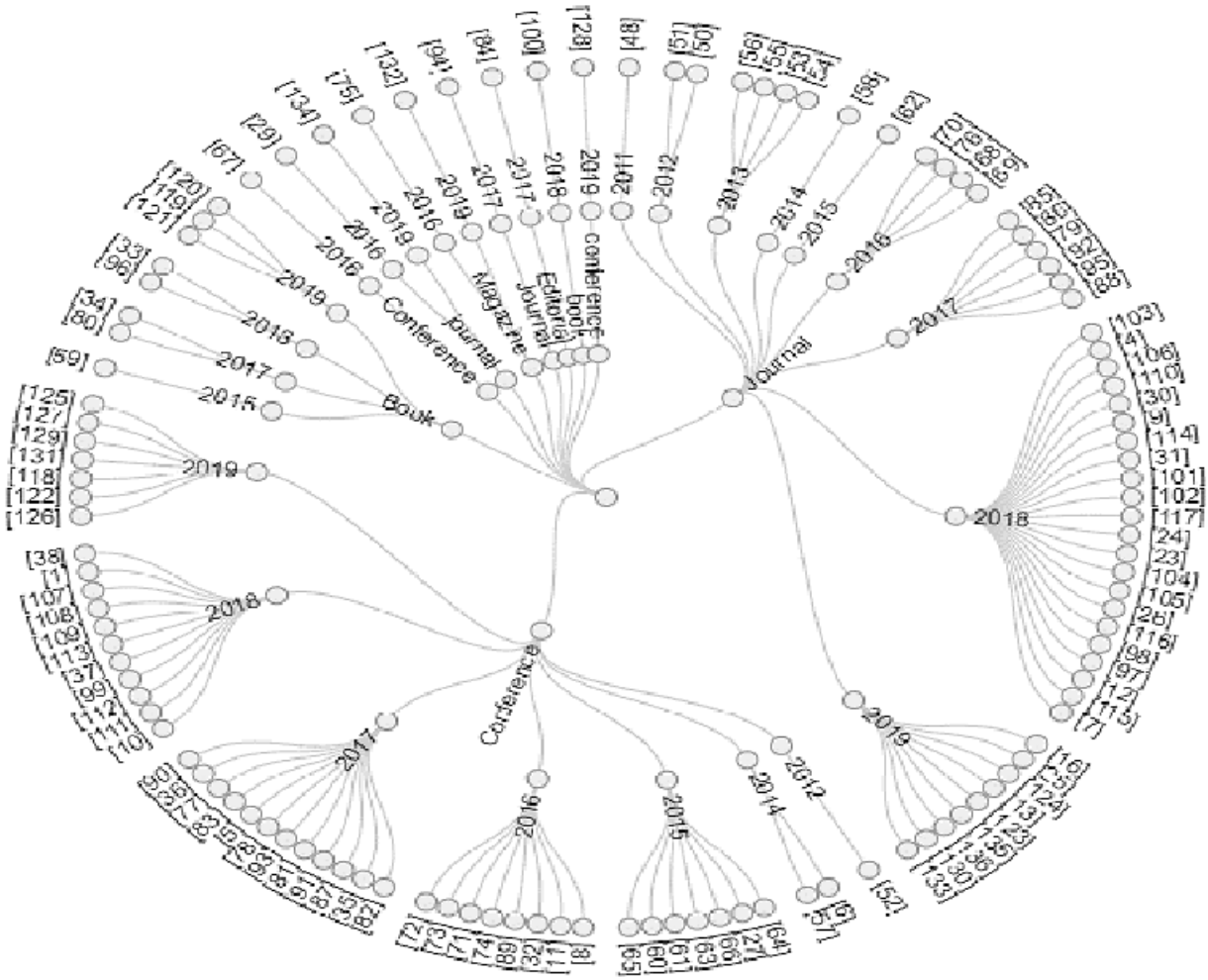


FIGURE 5. Detail of selected study.

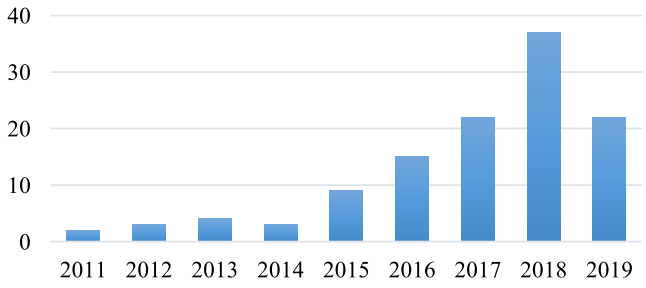


FIGURE 6. Research trends.

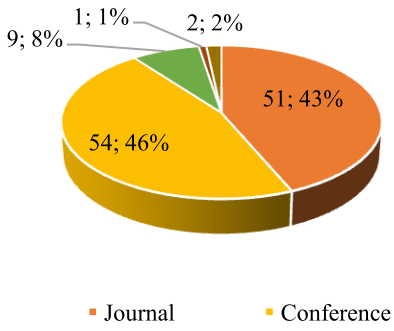


FIGURE 7. Source distribution.

data and any breach will compromise the device and network where they are operating. For this purpose, various security architectures and schemes have been proposed [57]. Problem related to the security of IoT device is that these devices are not designed with updated protection. For hardware-based system, the security components are often not connected to the network to protect them from attacks. Updating these kinds of systems would require a technician to come to update them, or the system would need to be replaced [12]. Similarly, the Intrusion Detection System (IDS) designed for IoT does not support anomaly detection capabilities [78]. The security and privacy issues in IoT ranges from simple password to insecure mobile apps and web interface [77]. Cyber criminals can easily attack IoT devices due to the default software configuration, irregular updates of software installed, a long gap between patch release and it installation [10]. Due to the fragile nature of IoT devices, it is important to provide a secure and reliable framework to IoT devices to operate. One solution to the security issues is the implementation of block chain technology. The block chain technology is

TABLE 9. Year-wise break up.

2011	2012	2013	2014	2015	2016	2017	2018	2019
[48]	[50]	[53]	[57]	[59]	[67]	[77]	[96]	[118]
[49]	[51]	[54]	[6]	[60]	[68]	[34]	[97]	[119]
	[52]	[55]	[58]	[61]	[69]	[36]	[38]	[120]
		[56]		[62]	[70]	[78]	[37]	[121]
				[63]	[71]	[79]	[33]	[13]
				[64]	[72]	[80]	[98]	[122]
				[65]	[73]	[81]	[99]	[123]
				[66]	[74]	[82]	[100]	[124]
				[27]	[8]	[35]	[101]	[25]
					[11]	[5]	[102]	[16]
					[29]	[83]	[103]	[125]
					[75]	[84]	[24]	[126]
					[32]	[85]	[23]	[127]
					[76]	[86]	[104]	[128]
						[87]	[105]	[129]
						[88]	[26]	[130]
						[89]	[1]	[131]
						[90]	[106]	[132]
						[91]	[107]	[133]
						[92]	[108]	[134]
						[93]	[109]	[135]
						[94]	[110]	[136]
						[95]	[30]	
							[10]	
							[111]	
							[112]	
							[9]	
							[113]	
							[114]	
							[31]	
							[115]	
							[12]	
							[116]	
							[4]	
							[7]	
							[117]	

beneficial for IoT system by providing management access control, symmetric and asymmetric key management and trustworthy and authorized identity registration [23]. The blockchain provides its own trust mechanism with the support first distributed recording system. Blockchain technology uses decentralized architecture which can track billions of IoT devices [83]. The decentralized approach eliminates the risk of single point failure and creates more secure environment for the IoT devices. It builds a reliable architecture for decentralized control through multi-node information redundancy. The blockchain technology is also helpful to solve the problem of IoT information sharing security [123]. For the security of IoT, various techniques, architectures and frameworks have been depicted Table 10.

Mobile computing provides answers towards the security of IoT devices by hardware infrastructure such as smart phone. It can acts as controller or it can be used as authentication option for security purposes. Unlike IoT, smart phones are smart devices and they provide better security but these phones are vulnerable to malware attacks. In order to address these attack various detection techniques have been used. The main focus of such techniques is to identify the malware attacks and provide robust security against the external interference. The detail about these various malware techniques has been discussed in Table 11.

These techniques need to be more reliable and accurate to minimize the impacts of malwares. According to our collated studies, among 10 malware detection techniques are identified, among them 9 techniques are from 2017 and one was presented in 2018. The accuracy in terms of percentage for each malware detection technique based has been shown in Figure 11.

Smart phones not only vulnerable to malwares but they are also under the siege of various risks such congestion in network, phishing attacks, spoofing attacks and many other attacks. According to [32] the smart phones experience various risks as depicted in Figure 12.

Apart from suffering such threats and malware attacks, the smartphone is still an option can be used as security for enabling the IoT device in context of security. The security techniques for protecting smart phone against malicious threats are much stronger as compared to IoT. Due to the specific characteristics of IoT conventional privacy techniques are not adequately enough for IoT. IoT devices are vulnerable to physical attacks due to large deployment. The significance application of smart phone is in IoT environment where all devices are fully connected via device controller, called smartphone [4]. The mobile phone act as smart controller can be used as a security control element for smart-home modules, because it can communicate with both the cloud component and the embedded devices, being able to run an IoT network protocol stack [5]. The security of mobile phone is important one due to many perspectives as it connects IoT devices and it provides a platform that enables to

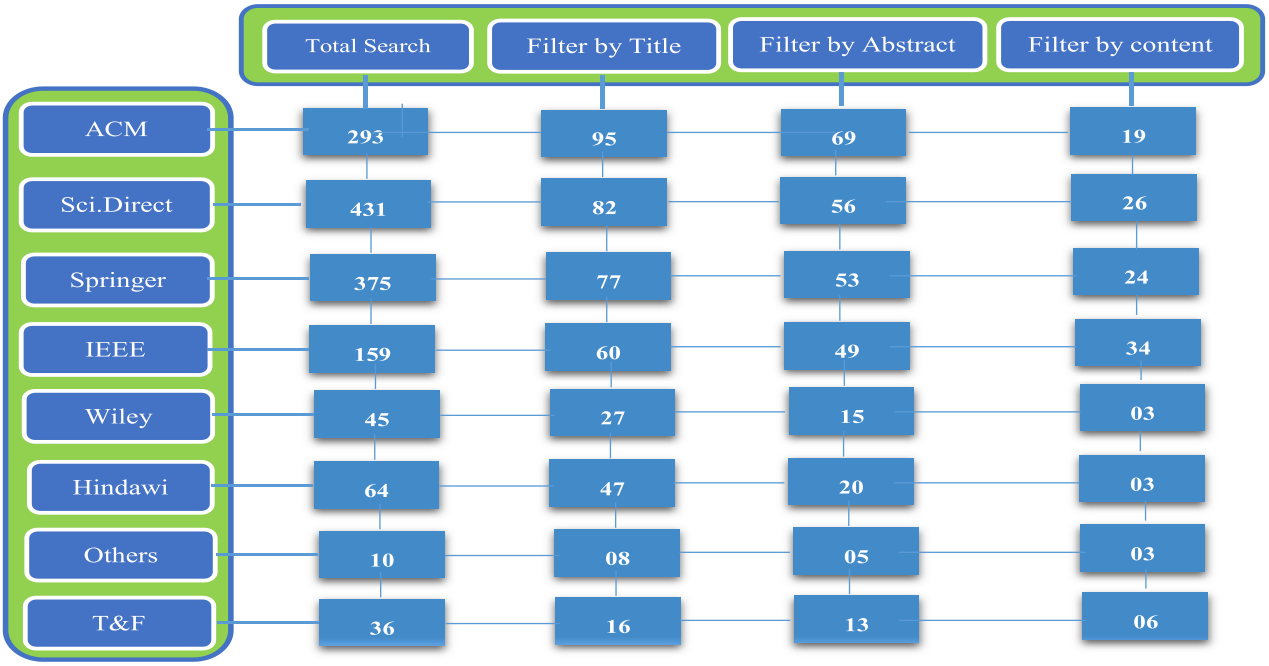


FIGURE 8. Selection detail.

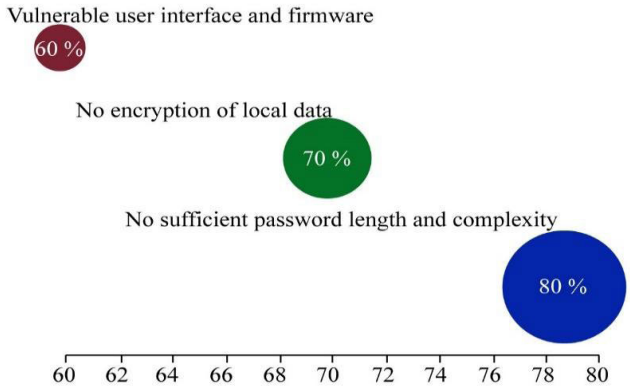


FIGURE 9. Percentage of vulnerabilities of IoT.

manage the IoT device. The IoT devices suffers more from authentication problems as there still exists some issues by using multiple digital signatures approach for authentication [137], [138]. IoT devices are susceptible to many cyber-attacks such as Man In Middle, eavesdropping, replay attacks, phishing, Denial of Service (DoS), spoofing, phishing, privacy breach and many others [139], [140]. Unlike smart phone, tablet the IoT devices have limited capabilities and resources, it leads to the confidentiality that remains a serious concern. Similarly, other issues are pertaining to privacy, physical threats and integrity [141].

D. RQ4. WHAT ARE THE SOFTWARE BASED SECURITY SOLUTIONS (APPS) PROVIDED BY MOBILE COMPUTING FOR IOT DEVICES?

In early ages, the mobile phones were used for making phone calls but now they can be used for variety of functions like installing various apps and strong operating systems, that enable mobile phones to do multiple options and computing abilities. The number of mobile subscribers are increasing exponentially and it has ultimately led to the millions of apps installed on the tablet devices and smart phones [70]. The mobile applications not only can affect the IoT by affecting power and processing abilities of network but they can also be used a security options like providing QR decoders, geo-features tagging and authentication mechanisms. But, using smartphone app without testing can lead towards the serious security problems. Mobile applications are rapidly affecting the world of IoT in terms of providing critical services and proving to be a good management tools. The mobile apps provide powerful features to IoT and it acts like a hub of IoT by leveraging its working and features. Apart from influencing the IoT, the mobile apps also have some major effects on the security of IoT. Modern IoT devices are complex in nature due the reason that they operate on powerful hardware with full blown software stack unlike traditional IoT devices residing on the primitive hardware with few KBs of memory running on microcontroller. Smart phone allows the installation of these apps, which controls the IoT devices. Third party apps provide number of roles in IoT ecosystem. These apps can be used to control IoT devices and such apps also receive notifications from devices such as a Samsung SmartThings allows the user to control the IoT devices [142].

The security of IoT devices has always been remained an issue due to its susceptibility and environment, where do they operate. Some IoT devices may share the data with third parties to be used for marketing purposes [77]. Information sent to the servers should be encrypted and authenticated. These mobile apps can also have impacts on IoT devices

TABLE 10. Summary of Security framework/techniques of IoT device.

S.No	Ref. No	Techniques/Architecture /Framework for IoT Security	Author Name	Year
1	[33]	• Message Queue Telemetry Transport (MQTT) • Advanced Message Queuing Protocol (AMQP)	Girma, Anteneh	2018
2	[130]	Heterogeneous IoT With Multiple Access Mobile Edge Computing	Wang, Dong et al	2019
3	[24]	• SmartThings • AWS IoT • Calvin • Brillo/Weave, • Kura • ARM Mbed • HomeKit • Azure IoT	Mahmud Ammar et. al	2018
4	[123] , [23]	Blockchain Technology	Haiping Si et al	2019
5	[37]	OWASP IoT framework	Lally, Gurjan et al	2018
6	[35]	Security Test Suite	Loi, Franco et al	2017
7	[58]	Mobile-ipv6-enabled RFID Tags	Sandra Dominikus Stefan Kraxberger	2011
8	[111]	Mobile Relay Architecture using BLE	Manzoor, Ahsan et.al	2018
9	[58]	• Hash functions • Cryptographically Secure Pseudo Random Number Generators (CSPRNGs)	Dominikus Sandra et al	2014
10	[113]	• EPSAKA • SEAKA • ECAKA & EC-AKA2	Quaissa, Mariya et al	2018
11	[55]	SVELTE	Shahid Raza et al	2018
12	[49]	Privacy Preservation of Analysis Hierarchy model	Jun, Wu Lei et al	2011
13	[124]	Random Coefficient Selection and Mean Modification Approach (RCSMMA) scheme	Hurrah, Nasir et al	2019
14	[133]	Authentication and Authorization for mobile IoT devices using Biofeatures	Ferrag, Amine et al	2019
15	[115]	Security Information and Event Management (SIEM) system	Diaz lopez, Daniel et.al	2018
16	[81]	Cloud-Based Vulnerability Mitigation Framework	Hadar, Noy et al	2017

in the context of security. As the portability and size of the smart phone has replaced the general pc and laptops, the malware developers have also targeted these IoT applications and the smart phones [102]. The Smart phone users require reliable sensing of information, thus they can publish their information from the phone on the protection layer like the social networking and install the Saas application on their devices which can help to register their data on the cloud and process without any malicious attacks [66]. According to [61] a proposed app store named as Ubibazar can also be used in context of IoT.

Mobile applications in the context of IoT are deployed in various fields but its significance in the healthcare environment is notice worthy. In healthcare the nature of data is more fragile so much security is required for making the data safe from malicious and unauthorized access. In healthcare various mobile health apps (M-health) are used and these apps have gained momentum and currently they are widely spread among cell phone users but due to not following the security policies, lack of encryption, unencrypted traffic and embedded advertisement have resulted in jeopardized the security of patients [31]. The security and privacy of

TABLE 11. Malware detection techniques for mobile phones.

S.No	Ref. No	Description	Author	Year	Drawback
1	[87]	Uses four ways to detect malwares. It divides the applications into four types like malicious, benign, aggressive and risky applications.	Shankar et al	2017	Time consuming in analysing malware
2	[88]	Detects the malware by using AOT compiler that changes byte code into machine code form.	Shahid alam et al	2017	Requires to enhance the run time through parallelization
3	[89]	It uses the machine learning algorithm which was presented by Waikato environment for knowledge analysis (WEKA).	Divya bansal et al	2017	Only aggressive applications and no classification of risky and benign applications
4	[90]	Detects application features and decides whether is malicious or not.	Dongfanghi et al	2017	Accuracy is less
5	[91]	Detects malware by using ensemble classifier for malware detection	Fariba ghaffari et al	2017	Only zero day malware detection and more false alarm with less accuracy
6	[92]	Woks based upon comparing malicious pattern and normal pattern set and then detects malicious and benign applications	Fie tong and Zhen Yen	2017	Not compatible with every OS
7	[93]	Uses ADA GRAD optimize algorithm for detecting malware pattern without manual intervention.	Hangliang Liang et al	2017	Less accuracy rate in detecting malware
8	[94]	Uses machine learning method for android malware detection	Paolo palumbo et al	2017	Protection only against ransomware attacks
9	[95]	Andro analysis techniques for evaluating the effectiveness of Andrio intense	Ali feizollah et al[	2017	Less accuracy
10	[117]	Uses Multiflow detection algorithm based upon information flow analysis	Feng shen et al	2018	Limited attributes to detect malware

IoT in healthcare can also be achieved by IoT application market (IAM), only the trusted applications can be used with the help of interactive vectors [56]. The smart phone applications provide the authentication to the IoT device in the context of smart home system. According to [5], the smart phone application provides the security solution to authenticate and authorize the IoT appliance after scanning and then sends this data to the QR authentication server. The mobile applications can also be used to provide a secret anonymity, protecting geo-location privacy and creation of virtual secret communities [72].

VI. THREATS TO VALIDITY

Validity threats affected data extraction and quality assessment of our selected studies in SLR protocol. Threats to validity of our SLR protocol were divided into internal validity, construct validity, external validity and conclusion validity [44]. These threats are explained as:

- **Internal validity**

This category describes the implementation of SLR protocol like search terms, data extraction, research method, quality assessment. Search terms were validated by using different databases and results obtained from search results were compared with the sample of papers that were collected through manual search. In order to mitigate the various versions of search strings were formed and tested on online data sources. Quality assessment was performed to bring the most relevant primary studies for SLR protocol. Quality assessment questions were defined for quality assessment criteria and then a suitable scale was created. Every paper was checked against the quality assessment average value and if it was less than certain value (2.5) then those papers were rejected and if quality assessment average score was more than defined value then paper was accepted for the inclusion list of primary studies. After quality assessment procedure, those papers were obtained which answered the RQs.

- **Construct validity**

In this category, threat related to construction of search string, formulation of questions, selection of online sources, inclusion-exclusion criteria and selection of primary studies. We formed search string and research questions very carefully and comprehensively. To refine the search string and questions, we performed a pilot study. Finally, we reached to finalise the research questions and search terms. It is no

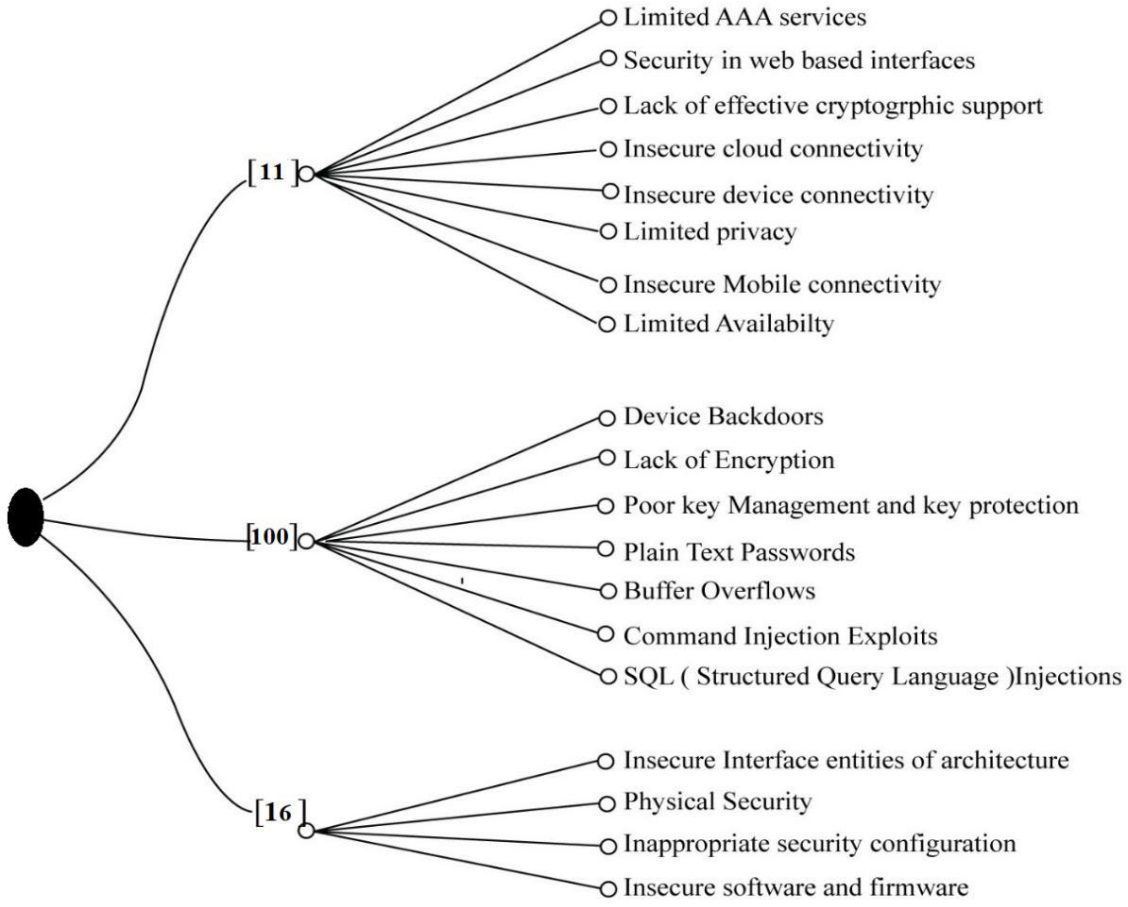


FIGURE 10. IoT vulnerabilities.

sure that the search string answered the questions completely but it still furnished the primary studies pertaining to SLR protocol. Selected online data sources are the most trusted, authentic and well-reputed sources. Snowballing and pilot study were performed to mitigate the threat related to construct validity.

- **External validity**

It is about generalization of finding results over primary studies and finding out to which degree the SLR results are representing the review topic. Threat related to external validity was mitigated by repeating the research procedure. After searching 117 primary studies were selected to answer the research questions. Subjective errors during the search phases were diminished by using multiple sources for searching. Duplicated and outdated papers were deleted to avoid the ambiguity.

- **Conclusion validity**

It is not possible at all that all relevant studies will be included in SLR protocol to address the research questions, there is probability that some relevant papers can be missed. Personal bias and subjectivity errors were mitigated by carefully designing and discussing the inclusion-exclusion criteria with the research experts to avoid the exclusion of relevant and important papers.

VII. LIMITATIONS

This research was carried upon a few selected online databases however, these databases are more referenced, having a high quality of research papers and are globally accepted. Some online data sources were skipped. The mobile malware detection techniques described in answering one of the questions are not exact in terms of figures, it could be even more. These techniques were only to support the arguments relevant to the security in smartphones. The search for this paper was performed by using a limited set of keywords so there is a chance that some papers might have been left which might be implicitly describing the security of IoT with the support of mobile computing. The list of all papers included in this research are not analysed properly but the analysis is limited to the IoT devices security in light of mobile computing. In this regard, every possible effort has been made to analyse all those papers that answer amply to research questions and having a high quality so readers can take benefits from it.

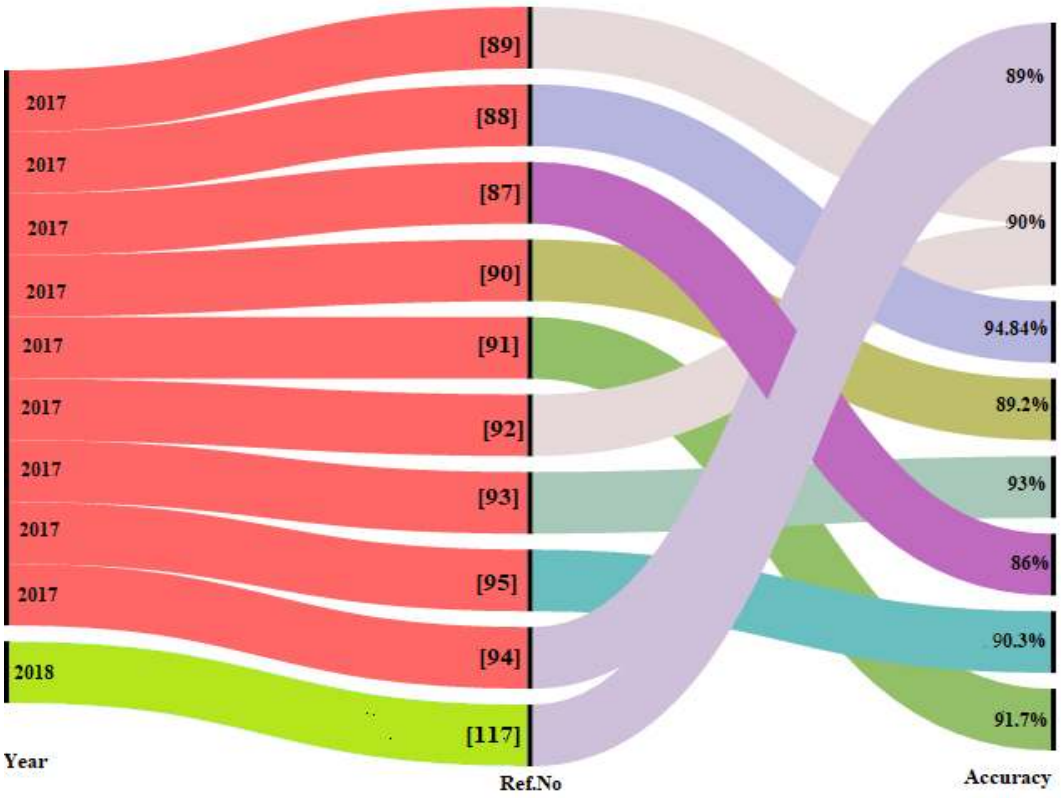


FIGURE 11. Accuracy of malware detection techniques.

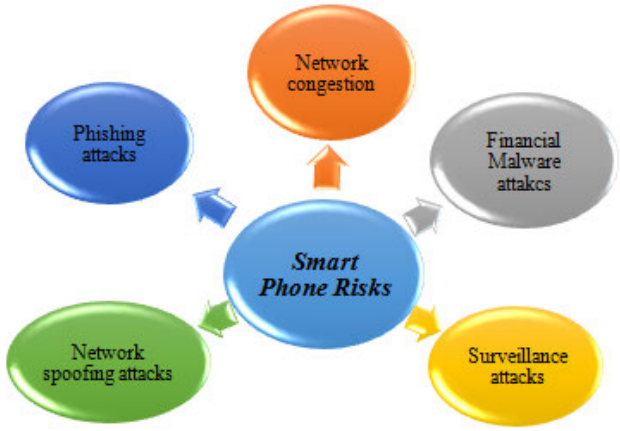


FIGURE 12. Smart phone risks.

VIII. CONCLUSION

In this paper, the security of IoT devices analysed comprehensively in order to understand the existing work and to provide a gateway to the future work for enhancing the existing security with the support of mobile computing. The IoT devices suffer from various vulnerabilities and threats due to their pervasive and ubiquitous nature. A strong security mechanism is required in a bid to enhance the existing security works. This can be achieved more handsomely through mobile computing which provides both hardware and software-based security solutions. The software-based solution encompasses various apps, services, and the modern apps embed biometric security features, while hardware-based solution includes smartphone physical devices. Similarly, mobile devices can be used as a controller of IoT devices. The security of IoT devices has been the most rising trend in the modern world but securing IoT with mobile computing is more intriguing and it will open a door for the researcher to enhance the existing security in light of mobile computing.

ACKNOWLEDGEMENT

Education and Scientific research project for young and middle-aged teachers in Fujian Province (2019), Project No.: jat191916, Project Name: Analysis and practice of artificial intelligence campus scene.

CONFLICT OF INTEREST

The authors declare no conflict of interest regarding this paper.

REFERENCES

[1] A. Dean and M. O. Agyeman, "A study of the advances in IoT security," in *Proc. 2nd Int. Symp. Comput. Sci. Intell. Control*, 2018, p. 15.
[2] C.-T. Li, C.-C. Lee, C.-Y. Weng, and C.-M. Chen, "Towards secure authenticating of cache in the reader for RFID-based IoT systems," *Peer-Peer Netw. Appl.*, vol. 11, no. 1, pp. 198–208, Jan. 2018.
[3] C.-T. Li, T.-Y. Wu, C.-L. Chen, C.-C. Lee, and C.-M. Chen, "An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system," *Sensors*, vol. 17, no. 7, p. 1482, Jun. 2017.

[4] X. Su, Z. Wang, X. Liu, C. Choi, and D. Choi, "Study to improve security for IoT smart device controller: Drawbacks and countermeasures," *Secur. Commun. Netw.*, vol. 2018, pp. 1–14, May 2018.

[5] M. Togan, B.-C. Chifor, I. Florea, and G. Gugulea, "A smart-phone based privacy-preserving security framework for IoT devices," in *Proc. 9th Int. Conf. Electron., Comput. Artif. Intell. (ECAI)*, Jun. 2017, pp. 1–7.

[6] C. Perera, P. P. Jayaraman, A. Zaslavsky, D. Georgakopoulos, and P. Christen, "MOSDEN: An Internet of Things middleware for resource constrained mobile devices," in *Proc. 47th Hawaii Int. Conf. Syst. Sci.*, Jan. 2014, pp. 1053–1062.

[7] F. Alshahwan, "Adaptive security framework in Internet of Things (IoT) for providing mobile cloud computing," in *Mobile Computing—Technology and Applications*. London, U.K.: IntechOpen, 2018.

[8] W. Xi and L. Ling, "Research on IoT privacy security risks," in *Proc. Int. Conf. Ind. Informat.-Comput. Technol., Intell. Technol., Ind. Inf. Integr. (ICIICII)*, Dec. 2016, pp. 259–262.

[9] R. Román-Castro, J. López, and S. Gritzalis, "Evolution and trends in IoT security," *Computer*, vol. 51, no. 7, pp. 16–25, 2018.

[10] R. Gurunath, M. Agarwal, A. Nandi, and D. Samanta, "An overview: Security issue in IoT network," in *Proc. 2nd Int. Conf. IoT Social, Mobile, Anal. Cloud (I-SMAC)*, Aug. 2018, pp. 104–107.

[11] J. Ahamed and A. V. Rajan, "Internet of Things (IoT): Application systems and security vulnerabilities," in *Proc. 5th Int. Conf. Electron. Devices, Syst. Appl. (ICEDSA)*, Dec. 2016, pp. 1–5.

[12] E. Buenrostro, D. Cyrus, T. Le, and V. Emamian, "Security of IoT devices," *J. Cyber Secur. Technol.*, vol. 2, no. 1, pp. 1–13, 2018.

[13] V. Mohammadi, A. M. Rahmani, A. M. Darwesh, and A. Sahafi, "Trust-based recommendation systems in Internet of Things: A systematic literature review," *Hum.-Centric Comput. Inf. Sci.*, vol. 9, no. 1, p. 21, Dec. 2019.

[14] G. P. Bhandari and R. Gupta, "A systematic literature review in fault analysis for IoT," *Int. J. Web Sci.*, vol. 3, no. 2, pp. 130–147, 2019.

[15] K. Fazal, H. Shehzad, A. Tasneem, A. Dawood, and Z. Ahmed, "A systematic literature review on the security challenges of Internet of Things and their classification," *Int. J. Technol. Res.*, vol. 5, no. 2, pp. 40–48, 2017.

[16] M. Aly, F. Khomh, M. Haoues, A. Quintero, and S. Yacout, "Enforcing security in Internet of Things frameworks: A systematic literature review," *Internet Things*, vol. 6, Jun. 2019, Art. no. 100050.

[17] E. L. C. Macedo, E. A. R. de Oliveira, F. H. Silva, R. R. Mello, F. M. G. Franca, F. C. Delicato, J. F. de Rezende, and L. F. M. de Moraes, "On the security aspects of Internet of Things: A systematic literature review," *J. Commun. Netw.*, vol. 21, no. 5, pp. 444–457, Oct. 2019.

[18] J. Martínez, J. Mejía, and M. Muñoz, "Security analysis of the Internet of Things: A systematic literature review," in *Proc. Int. Conf. Softw. Process Improvement (CIMPS)*, Oct. 2016, pp. 1–6.

[19] M. Witti and D. Konstantas, "IOT and security-privacy concerns: A systematic mapping study," *Int. J. Netw. Secur. Appl.*, vol. 10, no. 6, pp. 25–33, Nov. 2018.

[20] A. Sultan, M. S. Arshad Malik, and A. Mushtaq, "Internet of Things security issues and their solutions with blockchain technology characteristics: A systematic literature review," *Amer. J. Comput. Sci. Inf. Technol.*, vol. 6, no. 3, p. 27, 2018.

[21] S.-R. Oh and Y.-G. Kim, "Security requirements analysis for the IoT," in *Proc. Int. Conf. Platform Technol. Service (PlatCon)*, Feb. 2017, pp. 1–6.

[22] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the Internet of Things," in *Proc. IEEE World Congr. Services*, Jun. 2015, pp. 21–28.

[23] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[24] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, Feb. 2018.

[25] G. George and S. M. Thampi, "Vulnerability-based risk assessment and mitigation strategies for edge devices in the Internet of Things," *Pervas. Mobile Comput.*, vol. 59, Oct. 2019, Art. no. 101068.

[26] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," *Future Gener. Comput. Syst.*, vol. 108, pp. 909–920, Jul. 2020.

[27] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2015, pp. 180–187.

[28] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8182–8201, Oct. 2019.

[29] A. Kamilaris and A. Pitsillides, "Mobile phone computing and the Internet of Things: A survey," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 885–898, Dec. 2016.

[30] K. Liu, W. Shen, Y. Cheng, L. X. Cai, Q. Li, S. Zhou, and Z. Niu, "Security analysis of mobile Device-to-Device network applications," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2922–2932, Apr. 2019.

[31] A. Papageorgiou, M. Strigkos, E. Politou, E. Alepis, A. Solanas, and C. Patsakis, "Security and privacy analysis of mobile health applications: The alarming state of practice," *IEEE Access*, vol. 6, pp. 9390–9403, 2018.

[32] M. H. Khan and M. Ali Shah, "Survey on security threats of smartphones in Internet of Things," in *Proc. 22nd Int. Conf. Autom. Comput. (ICAC)*, Sep. 2016, pp. 560–566.

[33] A. Girma, "Analysis of security vulnerability and analytics of Internet of Things (IOT) platform," in *Information Technology—New Generations*. Cham, Switzerland: Springer, 2018, pp. 101–104.

[34] A. Rodríguez-Mota, P. J. Escamilla-Ambrosio, J. Happa, and E. Aguirre-Anaya, "GARMDROID: IoT potential security threats analysis through the inference of Android applications hardware features requirements," in *Applications for Future Internet*. Cham, Switzerland: Springer, 2017, pp. 63–74.

[35] F. Loi, A. Sivanathan, H. H. Gharakheili, A. Radford, and V. Sivaraman, "Systematically evaluating security and privacy for consumer IoT devices," in *Proc. Workshop Internet Things Secur. Privacy (IoTS&P)*, 2017, pp. 1–6.

[36] M. Capellupo, J. Liranzo, M. Z. A. Bhuiyan, T. Hayajneh, and G. Wang, "Security and attack vector analysis of IoT devices," in *Proc. Int. Conf. Secur., Privacy Anonymity Comput., Commun. Storage*, 2017, pp. 593–606.

[37] G. Lally and D. Sgandurra, "Towards a framework for testing the security of IoT devices consistently," in *Proc. Int. Workshop Emerg. Technol. Authorization Authentication*, 2018, pp. 88–102.

[38] I. Sahmi, T. Mazri, and N. Hmina, "Security study of different threats in Internet of Things," in *Proc. 3rd Int. Conf. Smart City Appl.*, 2018, pp. 785–791.

[39] F. Semedo, N. Moradpoor, and M. Rafiq, "Vulnerability assessment of objective function of RPL protocol for Internet of Things," in *Proc. 11th Int. Conf. Secur. Inf. Netw.*, 2018, pp. 1–6.

[40] S. Nazir, S. Shahzad, and N. Mukhtar, "Software birthmark design and estimation: A systematic literature review," *Arabian J. for Sci. Eng.*, vol. 44, no. 4, pp. 3905–3927, Apr. 2019.

[41] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," Tech. Rep. EBSE-2007-01, 2007.

[42] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *J. Syst. Softw.*, vol. 80, no. 4, pp. 571–583, Apr. 2007.

[43] P. Achimugu, A. Selamat, R. Ibrahim, and M. N. Mahrin, "A systematic literature review of software requirements prioritization research," *Inf. Softw. Technol.*, vol. 56, no. 6, pp. 568–585, Jun. 2014.

[44] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proc. 18th Int. Conf. Eval. Assessment Softw. Eng.*, 2014, p. 38.

[45] S. Mahdavi-Hezavehi, V. H. S. Durelli, D. Weyns, and P. Avgeriou, "A systematic literature review on methods that handle multiple quality attributes in architecture-based self-adaptive systems," *Inf. Softw. Technol.*, vol. 90, pp. 1–26, Oct. 2017.

[46] A. K. Kable, J. Pich, and S. E. Maslin-Prothero, "A structured approach to documenting a search strategy for publication: A 12 step guideline for authors," *Nurse Educ. Today*, vol. 32, no. 8, pp. 878–886, Nov. 2012.

[47] J. M. Norris and L. Ortega, "Effectiveness of l2 instruction: A research synthesis and quantitative meta-analysis," *Lang. Learn.*, vol. 50, no. 3, pp. 417–528, Sep. 2000.

[48] J.-C. Yang and B.-X. Fang, "Security model and key technologies for the Internet of Things," *J. China Univ. Posts Telecommun.*, vol. 18, pp. 109–112, Dec. 2011.

[49] W. Jun, M. Lei, and Z. Luo, "Data security mechanism based on hierarchy analysis for Internet of Things," in *Proc. Int. Conf. Innov. Comput. Cloud Comput.*, 2011, pp. 68–70.
[50] C. Du and S. Zhu, "Research on urban public safety emergency management early warning system based on technologies for the Internet of Things," *Procedia Eng.*, vol. 45, pp. 748–754, Jan. 2012.
[51] T. S. Hjorth and R. Torbensen, "Trusted domain: A security platform for home automation," *Comput. Secur.*, vol. 31, no. 8, pp. 940–955, Nov. 2012.
[52] W. Zhu, J. Yu, and T. Wang, "A security and privacy model for mobile RFID systems in the Internet of Things," in *Proc. IEEE 14th Int. Conf. Commun. Technol.*, Nov. 2012, pp. 726–732.
[53] D. Kyriazis and T. Varvarigou, "Smart, autonomous and reliable Internet of Things," *Procedia Comput. Sci.*, vol. 21, pp. 442–448, Jan. 2013.
[54] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, Jul. 2013.
[55] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad Hoc Netw.*, vol. 11, no. 8, pp. 2661–2674, Nov. 2013.
[56] K. Kang, Z.-B. Pang, and C. Wang, "Security and privacy mechanism for health Internet of Things," *J. China Univ. Posts Telecommun.*, vol. 20, no. 2, pp. 64–68, Dec. 2013.
[57] I. D. Addo, S. I. Ahamed, S. S. Yau, and A. Buduru, "A reference architecture for improving security and privacy in Internet of Things applications," in *Proc. IEEE Int. Conf. Mobile Services*, Jun. 2014, pp. 108–115.
[58] S. Dominikus and S. Kraxberger, "Secure communication with RFID tags in the Internet of Things," *Secur. Commun. Netw.*, vol. 7, no. 12, pp. 2639–2653, Dec. 2014.
[59] M. Yoon and J. Baek, "A study on framework for developing secure IoT service," in *Advances in Computer Science and Ubiquitous Computing*. Singapore: Springer, 2015, pp. 289–294.
[60] M. N. Johnstone, Z. Baig, P. Hannay, C. Carpene, and M. Feroze, "Controlled Android application execution for the IoT infrastructure," in *Proc. Int. Internet Things Summit*, 2015, pp. 16–26.
[61] S. Stastny, B. A. Farshchian, and T. Vilarinho, "Designing an application store for the Internet of Things: Requirements and challenges," in *Proc. Eur. Conf. Ambient Intell.*, 2015, pp. 313–327.
[62] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Bus. Horizons*, vol. 58, no. 4, pp. 431–440, Jul. 2015.
[63] M. Pistoia, O. Tripp, P. Ferrara, and P. Centonze, "Automatic detection, correction, and visualization of security vulnerabilities in mobile apps," in *Proc. 3rd Int. Workshop Mobile Develop. Lifecycle*, 2015, pp. 35–36.
[64] W. Ahmad, J. Sunshine, C. Kaestner, and A. Wynne, "Enforcing fine-grained security and privacy policies in an ecosystem within an ecosystem," in *Proc. 3rd Int. Workshop Mobile Develop. Lifecycle*, 2015, pp. 28–34.
[65] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, "Network-level security and privacy control for smart-home IoT devices," in *Proc. IEEE 11th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2015, pp. 163–167.
[66] R. Gupta and R. Garg, "Mobile applications modelling and security handling in cloud-centric Internet of Things," in *Proc. 2nd Int. Conf. Adv. Comput. Commun. Eng.*, May 2015, pp. 285–290.
[67] T. Kubitza, "Apps for environments: Running interoperable apps in smart environments with the meSchup IoT platform," in *Proc. Int. Workshop Interoperability Open-Source Solutions*, 2016, pp. 158–172.
[68] D. Seo, Y.-B. Jeon, S.-H. Lee, and K.-H. Lee, "Cloud computing for ubiquitous computing on M2M and IoT environment mobile application," *Cluster Comput.*, vol. 19, no. 2, pp. 1001–1013, Jun. 2016.
[69] E. P. Morera, I. de la Torre Díez, B. Garcia-Zapirain, M. López-Coronado, and J. Arambarri, "Security recommendations for mHealth apps: Elaboration of a developer's guide," *J. Med. Syst.*, vol. 40, no. 6, p. 152, 2016.
[70] T. Wang, T. D. Duong, and C. C. Chen, "Intention to disclose personal information via mobile applications: A privacy calculus perspective," *Int. J. Inf. Manage.*, vol. 36, no. 4, pp. 531–542, Aug. 2016.
[71] M. Medwed, "IoT security challenges and ways forward," in *Proc. 6th Int. Workshop Trustworthy Embedded Devices*, 2016, p. 55.
[72] Y. Michalevsky, S. Nath, and J. Liu, "MASHaBLE: Mobile applications of secret handshakes over Bluetooth LE," in *Proc. 22nd Annu. Int. Conf. Mobile Comput. Netw.*, 2016, pp. 387–400.
[73] R. Herbster, S. DellaTorre, P. Druschel, and B. Bhattacharjee, "Privacy capsules: Preventing information leaks by mobile apps," in *Proc. 14th Annu. Int. Conf. Mobile Syst., Appl., Services*, 2016, pp. 399–411.
[74] H. C. Chen, M. A. Al Faruque, and P. H. Chou, "Security and privacy challenges in IoT-based machine-to-machine collaborative scenarios," in *Proc. Int. Conf. Hardw./Softw. Codesign Syst. Synth. (CODES+ISSS)*, 2016, pp. 1–2.
[75] X. Sun and N. Ansari, "EdgeIoT: Mobile edge computing for the Internet of Things," *IEEE Commun. Mag.*, vol. 54, no. 12, pp. 22–29, Dec. 2016.
[76] A. Chaudhuri, "Cyber threat mitigation of wireless sensor nodes for secured, trustworthy IoT services," *EDPACS*, vol. 54, no. 1, pp. 1–14, Jul. 2016.
[77] A. Tekeoglu and A. Tosun, "An experimental framework for investigating security and privacy of IoT devices," in *Proc. Int. Conf. Intell., Secure, Dependable Syst. Distrib. Cloud Environ.*, 2017, pp. 63–83.
[78] E. Bertino, "Security and privacy in the IoT," in *Proc. Int. Conf. Inf. Secur. Cryptol.*, 2017, pp. 3–10.
[79] S. Sahmim and H. Gharsellaoui, "Privacy and security in Internet-based computing: Cloud computing, Internet of Things, cloud of things: A review," *Procedia Comput. Sci.*, vol. 112, pp. 1516–1522, Jan. 2017.
[80] S. Li and L. Da Xu, *Securing the Internet of Things*. Syngress, 2017.
[81] N. Hadar, S. Siboni, and Y. Elovici, "A lightweight vulnerability mitigation framework for IoT devices," in *Proc. Workshop Internet Things Secur. Privacy (IoTS P)*, 2017, pp. 71–75.
[82] M. N. Aman, K. C. Chua, and B. Sikdar, "Secure data provenance for the Internet of Things," in *Proc. 3rd ACM Int. Workshop IoT Privacy, Trust, Secur.*, 2017, pp. 11–14.
[83] G. Varshney and H. Gupta, "A security framework for IOT devices against wireless threats," in *Proc. 2nd Int. Conf. Telecommun. Netw. (TEL-NET)*, Aug. 2017, pp. 1–6.
[84] A. Roy, S. Sengupta, K.-K. Wong, V. Raychoudhury, K. Govindan, and S. Singh, *5G Wireless With Cognitive Radio and Massive IoT*. New York, NY, USA: Taylor & Francis, 2017.
[85] C. Maple, "Security and privacy in the Internet of Things," *J. Cyber Policy*, vol. 2, pp. 155–184, Jan. 2017.
[86] M. A. El Khaddar and M. Boulmalf, "Smartphone: The ultimate IoT and IoE device," in *Proc. Smartphones Appl. Res. Perspective*, 2017, p. 137.
[87] V. G. Shankar, G. Somani, M. S. Gaur, V. Laxmi, and M. Conti, "AndroTaint: An efficient Android malware detection framework using dynamic taint analysis," in *Proc. ISEA Asia Secur. Privacy (ISEASP)*, Jan. 2017, pp. 1–13.
[88] S. Alam, Z. Qu, R. Riley, Y. Chen, and V. Rastogi, "DroidNative: Automating and optimizing detection of Android native code malware variants," *Comput. Secur.*, vol. 65, pp. 230–246, Mar. 2017.
[89] E. Gandotra, D. Bansal, and S. Sofat, "Zero-day malware detection," in *Proc. 6th Int. Symp. Embedded Comput. Syst. Design (ISED)*, Dec. 2016, pp. 171–175.
[90] D. Li, Z. Wang, L. Li, Z. Wang, Y. Wang, and Y. Xue, "FgDetector: Fine-grained Android malware detection," in *Proc. IEEE 2nd Int. Conf. Data Sci. Cyberspace (DSC)*, Jun. 2017, pp. 311–318.
[91] F. Ghaffari, M. Abadi, and A. Tajoddin, "AMD-EC: Anomaly-based Android malware detection using ensemble classifiers," in *Proc. Iranian Conf. Electr. Eng. (ICEE)*, May 2017, pp. 2247–2252.
[92] F. Tong and Z. Yan, "A hybrid approach of mobile malware detection in Android," *J. Parallel Distrib. Comput.*, vol. 103, pp. 22–31, May 2017.
[93] H. Liang, Y. Song, and D. Xiao, "An end-to-end model for Android malware detection," in *Proc. IEEE Int. Conf. Intell. Secur. Informat. (ISI)*, Jul. 2017, pp. 140–142.
[94] P. Palumbo, L. Sayfullina, D. Komashinskiy, E. Eirola, and J. Karhunen, "A pragmatic Android malware detection procedure," *Comput. Secur.*, vol. 70, pp. 689–701, Sep. 2017.
[95] A. Feizollah, N. B. Anuar, R. Salleh, G. Suarez-Tangil, and S. Furnell, "AndroDialysis: Analysis of Android intent effectiveness in malware detection," *Comput. Secur.*, vol. 65, pp. 121–134, Mar. 2017.
[96] A. Mondal, P. Rao, and S. K. Madria, "Mobile computing, IoT and big data for urban informatics: Challenges and opportunities," in *Handbook Smart Cities*. Springer, 2018, pp. 81–113.
[97] H.-C. Hsieh, C.-S. Lee, and J.-L. Chen, "Mobile edge computing platform with container-based virtualization technology for IoT applications," *Wireless Pers. Commun.*, vol. 102, no. 1, pp. 527–542, Sep. 2018.
[98] K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray, and Y. Jin, "Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice," *J. Hardw. Syst. Secur.*, vol. 2, no. 2, pp. 97–110, Jun. 2018.

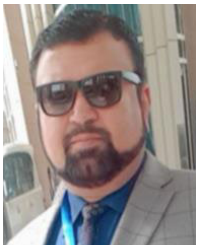
[99] C. Liu and W. Xiong, "Research on Internet of Things vulnerability based on complex network attack model," in *Proc. Int. Conf. Space Inf. Netw.*, 2018, pp. 21–29.
[100] C. Hosmer, "IoT vulnerabilities," in *Defending IoT Infrastructures With the Raspberry Pi: Monitoring and Detecting Nefarious Behavior in Real Time*. Berkeley, CA, USA: Apress, 2018, pp. 1–15.
[101] M. Hussain, A. Al-Haiqi, A. A. Zaidan, B. B. Zaidan, M. Kiah, S. Iqbal, S. Iqbal, and M. Abdulnabi, "A security framework for mHealth apps on Android platform," *Comput. Secur.*, vol. 75, pp. 191–217, Jun. 2018.
[102] J. Abawajy, S. Huda, S. Sharmeen, M. M. Hassan, and A. Almogren, "Identifying cyber threats to mobile-IoT applications in edge computing paradigm," *Future Gener. Comput. Syst.*, vol. 89, pp. 525–538, Dec. 2018.
[103] H. Elazhary, "Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions," *J. Netw. Comput. Appl.*, vol. 128, pp. 105–140, Feb. 2019.
[104] N. P. Owoh and M. Mahinderjit Singh, "Security analysis of mobile crowd sensing applications," *Appl. Comput. Informat.*, to be published. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2210832718302473
[105] S. Lee, S. Kim, K. Choi, and T. Shon, "Game theory-based security vulnerability quantification for social Internet of Things," *Future Gener. Comput. Syst.*, vol. 82, pp. 752–760, May 2018.
[106] M. Lei, Y. Yang, N. Ma, H. Sun, C. Zhou, and M. Ma, "Dynamically enabled defense effectiveness evaluation of a home Internet based on vulnerability analysis and attack layer measurement," *Pers. Ubiquitous Comput.*, vol. 22, no. 1, pp. 153–162, Feb. 2018.
[107] I. Bastys, M. Balliu, and A. Sabelfeld, "If this then what?: Controlling flows in IoT apps," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Jan. 2018, pp. 1102–1119.
[108] P. Adina, R. H. Venkatnarayan, and M. Shahzad, "Impacts & detection of network layer attacks on IoT networks," in *Proc. 1st ACM MobiHoc Workshop Mobile IoT Sens., Secur., Privacy*, 2018, p. 2.
[109] E. Ruiz, R. Avelar, and X. Wang, "Protecting remote controlling apps of smart-home-oriented IOT devices," in *Proc. 40th Int. Conf. Softw. Eng., Companion*, May 2018, pp. 212–213.
[110] J. Li, X. Li, J. Yuan, R. Zhang, and B. Fang, "Fog computing-assisted trustworthy forwarding scheme in mobile Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2778–2796, Apr. 2019.
[111] A. Manzoor, P. Porambage, M. Liyanage, M. Ylianttila, and A. Gurtov, "DEMO: Mobile relay architecture for low-power IoT devices," in *Proc. IEEE 19th Int. Symp. 'World Wireless, Mobile Multimedia Netw.' (WoWMoM)*, Jun. 2018, pp. 14–16.
[112] S. Chaudhry, "An encryption-based secure framework for data transmission in IoT," in *Proc. 7th Int. Conf. Rel., Infocom Technol. Optim. (Trends Future Directions) (ICRITO)*, Aug. 2018, pp. 743–747.
[113] M. Ouaissa, A. Rhattoy, and I. Chana, "New security level of authentication and key agreement protocol for the IoT on LTE mobile networks," in *Proc. 6th Int. Conf. Wireless Netw. Mobile Commun. (WINCOM)*, Oct. 2018, pp. 1–6.
[114] E. Novak, Z. Tang, and Q. Li, "Ultrasound proximity networking on smart mobile devices for IoT applications," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 399–409, Feb. 2019.
[115] D. D. López, M. B. Uribe, C. S. Cely, A. V. Torres, N. M. Guataquira, S. M. Castro, P. Nespoli, and F. G. Mármol, "Shielding IoT against cyber-attacks: An event-based approach using SIEM," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–18, Oct. 2018.
[116] M. G. Samaila, M. Neto, D. A. B. Fernandes, M. M. Freire, and P. R. M. Inácio, "Challenges of securing Internet of Things devices: A survey," *Secur. Privacy*, vol. 1, no. 2, p. e20, Mar. 2018.
[117] F. Shen, J. D. Vecchio, A. Mohaisen, S. Y. Ko, and L. Ziarek, "Android malware detection using complex-flows," *IEEE Trans. Mobile Comput.*, vol. 18, no. 6, pp. 1231–1245, Jun. 2019.
[118] S. Batool, N. A. Saqib, M. K. Khattack, and A. Hassan, "Identification of remote IoT users using sensor data analytics," in *Proc. Future Inf. Commun. Conf.*, 2019, pp. 328–337.
[119] I. Damaj and S. Kasbah, "Integrated mobile solutions in an Internet-of-Things development model," in *Mobile Solutions Their Usefulness Everyday Life*. Cham, Switzerland: Springer, 2019, pp. 3–31.
[120] H. F. Atlam and G. B. Wills, "IoT security, privacy, safety and ethics," in *Digital Twin Technologies and Smart Cities*. Springer, 2020, pp. 123–149.
[121] S. Ziegler, C. Crettaz, E. Kim, A. Skarmeta, J. B. Bernabe, R. Trapero, and S. Bianchi, "Privacy and security threats on the Internet of Things," in *Internet of Things Security and Data Protection*. Cham, Switzerland: Springer, 2019, pp. 9–43.
[122] S. Malempati and V. Padminivalli, "Work-in-progress: Challenges in IoT security," in *Proc. Int. Conf. Remote Eng. Virtual Instrum.*, 2019, pp. 357–364.
[123] H. Si, C. Sun, Y. Li, H. Qiao, and L. Shi, "IoT information sharing security mechanism based on blockchain technology," *Future Gener. Comput. Syst.*, vol. 101, pp. 1028–1040, Dec. 2019.
[124] N. N. Hurrah, S. A. Parah, J. A. Sheikh, F. Al-Turjman, and K. Muhammad, "Secure data transmission framework for confidentiality in IoTs," *Ad Hoc Netw.*, vol. 95, Dec. 2019, Art. no. 101989.
[125] N. Klingensmith, Y. Kim, and S. Banerjee, "A hypervisor-based privacy agent for mobile and IoT systems," in *Proc. 20th Int. Workshop Mobile Comput. Syst. Appl.*, Feb. 2019, pp. 21–26.
[126] A. Nakajima, T. Watanabe, E. Shioji, M. Akiyama, and M. Woo, "A pilot study on consumer IoT device vulnerability disclosure and patch release in Japan and the United States," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, Jul. 2019, pp. 485–492.
[127] S. Aljawarneh, V. Radhakrishna, and G. R. Kumar, "A recent survey on challenges in security and privacy in Internet of Things," in *Proc. 5th Int. Conf. Eng. MIS*, 2019, p. 25.
[128] M. J. C. Samonte, E. P. E. Signo, R. J. M. Gayomali, W. P. Rey, and E. A. Serrano, "PHYTO: An IoT urban gardening mobile app," in *Proc. 2nd Int. Conf. Inf. Sci. Syst.*, 2019, pp. 135–139.
[129] N. A. Gunathilake, W. J. Buchanan, and R. Asif, "Next generation lightweight cryptography for smart IoT devices: Implementation, challenges and applications," in *Proc. IEEE 5th World Forum Internet Things (WF-IoT)*, Apr. 2019, pp. 707–710.
[130] D. Wang, B. Bai, K. Lei, W. Zhao, Y. Yang, and Z. Han, "Enhancing information security via physical layer approaches in heterogeneous IoT with multiple access mobile edge computing in smart city," *IEEE Access*, vol. 7, pp. 54508–54521, 2019.
[131] Y. Fukushima and V. P. Kafle, "Hide-and-disclose: On-site information sharing for privacy-aware mobile IoT communications," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2019, pp. 352–354.
[132] J. Ni, X. Lin, and X. S. Shen, "Toward edge-assisted Internet of Things: From security and efficiency perspectives," *IEEE Netw.*, vol. 33, no. 2, pp. 50–57, Mar. 2019.
[133] M. A. Ferrag, L. Maglaras, and A. Derhab, "Authentication and authorization for mobile IoT devices using biofeatures: Recent advances and future trends," *Secur. Commun. Netw.*, vol. 2019, pp. 1–20, May 2019.
[134] C. Kolias, W. Meng, G. Kambourakis, and J. Chen, "Security, privacy, and trust on Internet of Things," *Wireless Commun. Mobile Comput.*, vol. 2019, Feb. 2019, Art. no. 6452157 .
[135] G. Kalyani and S. Chaudhari, "An efficient approach for enhancing security in Internet of Things using the optimum authentication key," *Int. J. Comput. Appl.*, vol. 42, no. 3, pp. 306–314, 2019.
[136] V. Malik and S. Singh, "Security risk management in IoT environment," *J. Discrete Math. Sci. Cryptogr.*, vol. 22, no. 4, pp. 697–709, May 2019.
[137] M.-S. Hwang and C.-C. Lee, "Research issues and challenges for multiple digital signatures," *IJ Netw. Secur.*, vol. 1, no. 1, pp. 1–7, 2005.
[138] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, and K. Salah, "A user authentication scheme of IoT devices using blockchain-enabled fog nodes," in *Proc. IEEE/ACS 15th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Oct. 2018, pp. 1–8.
[139] A. W. Atamli and A. Martin, "Threat-based security analysis for the Internet of Things," in *Proc. Int. Workshop Secure Internet Things*, Sep. 2014, pp. 35–43.
[140] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-service detection in 6LoWPAN based Internet of Things," in *Proc. IEEE 9th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2013, pp. 600–607.
[141] X. Liu, M. Zhao, S. Li, F. Zhang, and W. Trappe, "A security framework for the Internet of Things in the future Internet architecture," *Future Internet*, vol. 9, no. 3, p. 27, Jun. 2017.
[142] N. Zhang, S. Demetriou, X. Mi, W. Diao, K. Yuan, P. Zong, F. Qian, X. Wang, K. Chen, Y. Tian, C. A. Gunter, K. Zhang, P. Tague, and Y.-H. Lin, "Understanding IoT security through the data crystal ball: Where we are now and where we are going to be," 2017, *arXiv:1703.09809*. [Online]. Available: http://arxiv.org/abs/1703.09809

BIN LIAO was born in Fujian, China, in 1984. He received the B.E. degree in software engineer specialty and the M.E. degree in computer application specialty from Fuzhou University, Fuzhou, China, in 2007 and 2010, respectively. From 2010 to 2013, he was an Assistant Engineer with the Fujian Supercomputer Center, Fujian. Since 2010, he has been an Engineer with the Office of Cyber Security and Informatization, Fuzhou University. He is the author of more than ten articles. His research interests include the Internet of Things, cybersecurity, information systems, and smart campus.

YASIR ALI received the M.Sc. degree in computer science from the University of Peshawar. He is currently pursuing the M.S. degree in computer science with the Department of Computer Science, University of Swabi. He is working as a Lecturer at the Government Postgraduate College Swabi. His research interests include the Internet of Things and security evaluation.

SHAH NAZIR received the Ph.D. degree in computer science with a specialization in software engineering. He has several research publications in well-reputed international journals and conference proceedings. He is a reviewer for several journals and conferences. He is currently an Assistant Professor and the Head of the Department of Computer Science, University of Swabi. He worked at the University of Peshawar. His research interests include component-based software engineering, software birthmark, systematic literature review, and decision-making.

LONG HE was born in Fujian, China, in 1971. He received the B.S. degree in chemistry specialty from Jilin University, Jilin, China, in 1994, and the M.E. degree in computer application specialty from Fuzhou University, Fuzhou, China, in 2003. From 1994 to 2006, he was a Senior Engineer with the Environmental Information, Fujian, China. Since 2006, he has been a Senior Engineer with the Office of Cyber security and Informatization, Fuzhou University. He is the author of more than ten articles. He research interests include artificial intelligence, network technique, big data analysis, and the Internet of Things.



HABIB ULLAH KHAN received the Ph.D. degree in management information systems from Leeds Beckett University, U.K. He is currently an Associate Professor of management information systems with the Department of Accounting and Information Systems, College of Business and Economics, Qatar University, Qatar. He has nearly 20 years of industry, teaching, and research experience. His research interests include IT adoption, social media, the Internet addiction, mobile commerce, computer mediated communication, IT outsourcing, big data, and IT security.