Journal of Theoretical and Applied Information Technology
15th September 2018. Vol.96. No 17

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SECURITY REQUIREMENTS AND TECHNOLOGIES FOR THE INTERNET OF THINGS (IOT) APPLICATIONS: A SYSTEMATIC LITERATURE REVIEW

[1]ASMA ASDAYANA IBRAHIM, [2]MASSILA KAMALRUDIN

[1] Faculty of Information and Communication Technology,
Universiti Teknikal Malaysia Melaka, 76100, Malaysia
[2] Innovative Software System and Service Group,
Universiti Teknikal Malaysia Melaka, 76100, Malaysia
E-mail: [1]asmaasdayana@gmail.com, [2]massila@utem.edu.my

ABSTRACT

Security requirement is one of the most important intangible requirements which could be taken as a burden on the smooth functioning of the system or application. Requirements engineers without expertise in security are at risk of overlooking security requirement, which frequently leads to the act of misuse. This study plans to identify the security requirements and technologies being used in IoT applications. We conducted a systematic literature review in order to identify and analyse related literature on elicitation of security requirements for IoT applications. We found that the most used technologies for IoT applications are sensors, mobility networks, RFID systems, WiFi, Bluetooth and Zigbee and the security requirements that are relevant for IoT applications are authentication, confidentiality, integrity, authorization, access control and availability. Finally, the characteristics and properties of the security requirements and technologies were also discussed. It can be concluded that the primary challenge of security requirements is to identify the most appropriate security requirements. Furthermore, requirement engineers should consider challenges posed by security requirements such as to analyse and develop security requirements for IoT applications. In addition, right security requirements for IoT applications should be recognized at the early phase of IoT applications development.

Keywords: *Internet Of Things, Systematic Literature Review, Security Requirements, Internet Of Things, Iot Technologies*

1 INTRODUCTION

The internet of thing (IoT) is a system that is expected to interconnect compelled devices; for instance, sensors, actuators, RFID from the physical world to the Internet. The IoT is considered as an empowering innovation for few applications like healthcare, assembling and overwhelming industry, finance and banking, transportation and smart environments. It is expected that 50 billion devices will be interconnected by 2020, and this number is expected to achieve trillion [1]. Nowadays, IoT can provide a more propelled services to people, which connects variety of devices, applications, and systems. However, it covers variety of devices, protocols and application, which makes it much more complex. Recently, IoT technologies are applied in various areas. The large-scale implementation of IoT devices promises to transform many aspects of the way we live. For consumers, new IoT products like Internet-enabled appliances, home automation components, and energy management devices are moving us toward a vision of the smart city, offering more security and energy-efficiency. Other personal IoT devices like wearable fitness and health monitoring devices and network-enabled medical devices are transforming the way healthcare services are delivered. The IoT will demand a wide range of new technologies and skills, including new hardware platforms, networks, operating systems, high-volume data processing, cloud services, endpoint management tools, as well as standards and ecosystems.

Atzori et. al [2] have surveyed the most important aspects of IoT with emphasis on what is being done and what are the issues that require further research. It is undeniable that current technologies make the IoT concept feasible but it does not fit well with the scalability and efficiency requirements that they will face. On the other hand, Borgohain et. al [3] have conducted a general survey of all the security issues existing in the Internet of Things (IoT) along with an analysis of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the privacy issues that an end-user may face as a consequence of the spread of IoT. Majority of the survey is focused on the security loopholes arising from the information exchange technologies used in Internet of Things. However, no security requirements in IoT application has been analysed in the paper. Furthermore, Zhou et. al [4] introduced the architecture and unique security and privacy requirements for the next generation mobile technologies on a cloud-based IoT. This work also identifying the inappropriateness of most existing work, and addressing the challenging issues of secured packet forwarding and efficient privacy. All of this work preserving authentication by proposing new efficient privacy preserving data aggregation without public key homomorphic encryption.

Another work by [5] provides an overview about the security and privacy challenges of IoT applications in smart grids. Furthermore, they highlight and analyze some solutions and practices being used in coping with security and privacy requirements for IoT on deployment and management of smart grid. They address three types of challenge domains; customer domain, information and communication domain and the grid domain. They represent a comprehensive survey of the most recent contributions on security and privacy aspects of IoT applications in smart grid and identify some of the remaining challenges and vulnerabilities related to security and privacy. Even though the benefits of smart grid are evident and are widely acknowledged by utility companies, cyber-attacks will be more innovative than ever. The insights and recommendations outlined in all of the reviewed research works can help utilities to be in a strong position in preventing these potential threats although it is impossible to completely neutralize the likelihood of destructive cyber intrusions. Privacy and security requirements in IoT based smart grids is only partially researched and there is a wide space of research aspects to be investigated further in order to build well-defined and more secured standards for communication and protection. There are also some IoT-specific characteristics like power consumption and low computing power and this leads to existing ICT technologies to be restricted. Therefore, security requirements for IoT devices and technologies are necessary.

Based on the findings, we have identified that the most used attributes/key technologies for IoT applications are sensors, mobility networks, RFID systems, WiFi, Bluetooth, and Zigbee. The results also show that sensors have become the most frequently-used technology in IoT applications. We have discovered the important security requirements for IoT applications, namely; authentication, confidentiality, integrity, authorization, access control, and availability were applied to IoT applications. The result also shows that authentication is the most important properties needed for IoT based applications. This paper is organized in five sections. After the introduction section, we present the three phase of methodology which are planning, conducting the review and reporting the review in the second section. This is followed by the third section which described the review results of this study. The fourth section summarizes the findings of this study. Lastly, this paper will end with a section on the conclusion.

2 REVIEW METHOD

This review has to be attempted as Systematic Literature Review (SLR) in light of the first rule as proposed by [6]. The SLR consists of three phases which are Planning, Conducting the Review and Reporting the Review. Figure 1 demonstrates the systematic literature review process.

Figure 1: Systematic Literature Review Process

2.1 Planning the Review

2.1.1 The Research Question (s)

To keep the review focused, Research Question (RQ) were formulated by Kitchenham [7] using the Population, Intervention, Comparison, Outcomes and Context (PICOC) criteria in structuring the research questions. Table 1 shows summary of PICOC in arranging the research questions.

Table 1: Summary of PICOC

PICOC	Criteria
Population	IoT technologies, IoT application, security requirements, security properties
Intervention	IoT technologies, IoT attributes, security requirements properties

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Comparison	Existing technologies, properties, attributes
Outcomes	Prediction of accuracy of IoT technologies, security requirements of IoT application
Context	Empirical studies in academia and industry

Specifying the research question is the most important part of any systematic review. During the planning of SLR, the following questions were designed for the purpose of data extractions as shown in Table 2. The SLR was conducted in addressing the objectives which are to identify the most used technologies for the Internet of Things (IoT) applications and to identify the important security requirements needed for the Internet of Things (IoT) based applications.

Table 2: Research Questions

ID	Research Question	Motivation
RQ1	What are the most used technologies for Internet of Things (IoT) applications?	Identify the most used technologies for Internet of Things (IoT) applications?
RQ2	What are the important security requirements needed for Internet of Things (IoT) applications?	Identify the important security requirements needed for Internet of Things (IoT) applications.

2.1.2 Developing a Review Protocol

A review protocol indicates the methods that will be used to undertake a specific systematic review. The aim of this review is to thoroughly examine the empirical on validating security requirements of IoT applications development. The strategy that will be used to search for primary studies will include search terms and resources to be searched. Recourses include digital libraries, specific journals, and conference proceedings.

2.1.2.1 Study Selection Criteria

Study selection criteria are used to determine which studies are included in, or excluded from the systematic review. After the research questions is finalized, we have conducting the search process. The source of the search was digital libraries and databases using search string, and refining search string. The list of the digital databases is based on the most popular and acquainted databases to ease and develop the set of related search papers. The list of the digital databases used to search the papers in this study is shown in Table 3.

Table 3: Digital Database Library

Source	Links
IEEE Xplore	Ieeexplore.iee.org
ScienceDirect	sciencedirect.com
Google Scholar	scholar.gooogle.com
Elsevier	elsevier.com
Emerald Insight	emeralsight.com
Elvedit	elvedit.com
Springer Link	link.springer
ACM Digital Library	dl.acm.org

2.1.2.2 Study Selection Procedure

The search strings are based on the research questions and the keywords of the research field such as security requirements and IoT technologies. The searches for relevant papers were also based on the title and the author's name. Language for the search was limited to English only. The selection procedure was conducted systematically based on the following steps as shown in Figure 2. Table 4 shows the inclusion and exclusion criteria for the remaining paper studies.

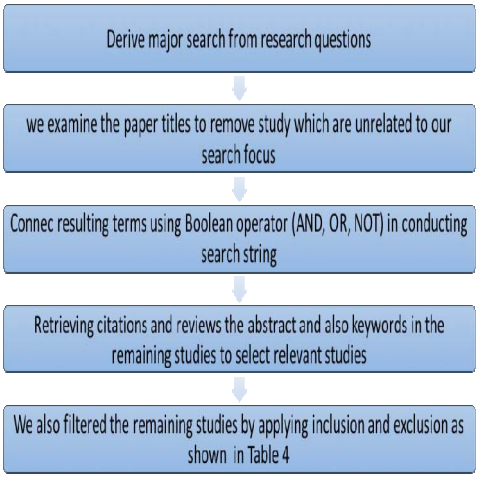

Figure 2: Selection process

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 4: Inclusion and exclusion criteria

Inclusion Criteria	Exclusion Criteria
Papers focusing on security requirements Papers describing IoT applications Papers describing IoT technologies and attributes Systematic Literature Review	Papers presented are not subjected to peer review Papers presenting results without supporting evidence Paper being studied are not related to research questions Studies unclear

2.1.2.3 Study Quality Assessment Checklist

Each SLR was evaluated using the selected items from the quality checklist provided by Kitchenham et. al [8]. The criteria are based on four quality assessment (QA) questions as shown in Table 5:

Table 5: Quality Assessment

QA1	Are the review's inclusion and exclusion criteria described and appropriate?
QA2	Is the literature search likely to have covered all relevant studies?
QA3	Did the reviewers assess the quality/validity of the relevant studies?
QA4	Were the basic data/studies adequately described?

The questions were scored as shown in Table 6. The scoring procedure was Y=1, P=0.5, N=0, or Unknown if the information is not specified. If any of the criteria was not applicable on any studies, it was included from evaluating for only that particular study. Studies that scored less than 50% in the quality assessment were excluded as they do not provide the basic information about their research methodology.

Table 6: Question Scores

QA1	Y (Yes), the inclusion criteria are explicitly defined in the study	P (Partly), the inclusion criteria are implicit	N (No), the inclusion criteria are not defined and cannot be readily inferred
QA2	Y, the authors have either searched for 4 or more digital libraries and included additional search strategies or identified and referenced all journals addressing the topic of interest	P, the authors have searched for 3 or 4 digital libraries with no extra search strategies, or searched for a defined but restricted set of journals and conference proceedings.	N, the authors have searched up to 2 digital libraries or an extremely restricted set of journals
QA3	Y, the authors have explicitly defined quality criteria and extracted them from each primary study	P, the research question involves quality issues which have been addressed by the study	N, no explicit quality assessment of individual primary studies are attempted
QA4	Y, Information is presented about each study	P, only summary information about primary studies is presented	N, the results of the individual primary studies are not specified

2.1.2.4 Data Extraction Strategy

The relevant information in answering the research questions required were extracted from selected primary studies is shown in Table 7. We used data extraction form to make sure that this task was carried out in an accurate, consistent and complete manner.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 7: Data Extraction

Search focus	Data item	Description
General	Bibliography Type of paper Study aims Study design	Author, title, year, source Article, book, conference proceeding, journals, thesis, white paper The goals of the primary study Controlled experiments/survey
RQ1	Examples	Examples of technologies for the IoT applications
RQ2	Examples	Examples of security requirements for the IoT applications

2.2 Conducting the Review

2.2.1 Identify Relevant Research and Primary Studies

Firstly, we examined title of the papers to remove any studies which are not related to the research focus. Next, we used the abstract, keywords and the conclusion to eliminate additional unrelated studies. After applying these two steps, there are 122 studies remained. We examined these 122 studies and applied the inclusion/exclusion criteria in Table 4 to select 109 papers as primary studies for this SLR. Furthermore, we applied the same selection steps to reference list of the selected 84 primary studies to find additional primary studies which are related to the research focus.

2.2.2 Data Extraction and Quality Assessments

We used data extraction from Table 7 to extract data from the primary studies. Many primary studies did not answer all of the questions in the data extraction form. We extracted important information provided by the primary studies using the data extraction form. Next, depending on the type of the study, we applied quality assessment questions in Table 5 or Table 6 to each primary study. We provided 'yes' and 'no' answer to our quality assessment questions. We used a binary scale since we were not interested in providing a quality score for the studies.

2.3 Reporting the Review

The data extracted from 84 primary papers were used to formulate answers to the two research questions. We closely followed the guidelines provided by Kitchenham et. al [8] in preparing the SLR report.

3 THE REVIEW RESULTS

In this section, we present the synthesis of evidence of our SLR, starting with the analysis of the literature. We used selected primary papers to provide answers to research questions as well. Table 8 shows the number of studies for quality assessment through the level layer of SLR. The exclusion on this paper, 11 studies were investigated and two were investigated as redundancy during this study. After quality assessment of 109 studies, 84 of them were identified for the synthesis of evidence.

Table 8: Paper Study for Quality Assessment

Criteria	Paper study
Before Quality Assessment	122
Duplicate	2
Exclusion	11
After Quality Assessment	109
Accepted	84
Rejected	25

3.1 Quality Assurances

The table shows details based on the quality assessments conducted during the process of searching. The calculation result of this quality assessment identified above than 0.5 were considered accepted, while below or than 0.5 was rejected. Table 9 shows the final result which is 84 studies were accepted and 25 primary studies were rejected.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 9: Quality Assurances

Paper Study	Author	QA1	QA2	QA3	QA4	Result	Status
PS1	Segura et al. (2016) [9]	0.5	0.5	1	1	0.75	Accepted
PS2	Rahimi et al. (2016) [10]	1	1	1	1	1	Accepted
PS3	Li et al. (2016) [11]	0.5	0.5	1	1	0.75	Accepted
PS4	Malina et al. (2016) [12]	0.5	1	1	1	0.875	Accepted
PS5	Lau et al. (2016) [13]	0.5	1	1	1	0.875	Accepted
PS6	Scuotto et al. (2016) [14]	0.5	1	1	1	0.875	Accepted
PS7	Sruthi & Geethakumari (2016) [15]	0.5	0	1	1	0.625	Accepted
PS8	Kim (2015) [16]	0.5	1	0.5	0.5	0.625	Accepted
PS9	Asplund & Nadjm-Tehrani (2016) [17]	0.5	0.5	0.5	1	0.625	Accepted
PS10	Rullo et al. (2016) [18]	0.5	0	1	1	0.625	Accepted
PS11	Mori et al. (2016) [19]	0	0	1	1	0.5	Rejected
PS12	Ando & Kayashima (2016) [20]	1	0	1	1	0.75	Accepted
PS13	Oualha & Thuat Nguyen (2016) [21]	0.5	0.5	1	1	0.75	Accepted
PS14	Oualha & Thuat Nguyen (2016) [22]	0.5	1	1	0.5	0.75	Accepted
PS15	Marktscheffel et al. (2016) [23]	1	1	1	0.5	0.875	Accepted
PS16	Gope & Hwang (2016) [24]	1	1	1	1	1	Accepted
PS17	Skarmeta (2016) [25]	1	0.5	1	1	0.875	Accepted
PS18	Fotouhi et al. (2016) [26]	1	1	1	0.5	0.875	Accepted
PS19	Ometov et al. (2016) [27]	1	0	0.5	1	0.625	Accepted
PS20	W. Lee et al. (2016) [28]	1	0.5	1	0	0.625	Accepted
PS21	Aldosari (2015) [29]	0.5	1	1	0	0.625	Accepted
PS22	Tran & Ha (2015) [30]	1	0.5	1	1	0.875	Accepted
PS23	Khanna & Anand (2016) [31]	1	0.5	1	1	0.875	Accepted
PS24	Vučinić et al. (2015) [32]	1	0	1	1	0.75	Accepted
PS25	Sicari et al. (2015) [33]	0.5	1	0.5	0.5	0.625	Accepted
PS26	Neisse et al. (2015) [34]	1	1	1	1	1	Accepted
PS27	Islam et al. (2015) [35]	1	1	1	1	1	Accepted
PS28	Moosavi et al. (2015) [36]	1	1	1	0.5	0.875	Accepted
PS29	(Singh et al. (2015) [37]	1	0.5	1	1	0.875	Accepted
PS30	Wu et al. (2015) [38]	0.5	1	1	0	0.625	Accepted
PS31	Granjal et al. (2015) [39]	1	0.5	1	1	0.875	Accepted
PS32	He & Zeadally (2015) [40]	1	1	1	1	1	Accepted
PS33	Ouaddah et al. (2015) [41]	1	0	1	1	0.75	Accepted
PS34	Nguyen & Iacono (2015) [42]	0.5	0.5	1	1	0.75	Accepted
PS35	Zhang & Zhang (2015) [43]	1	0	1	1	0.75	Accepted
PS36	Mu et al. (2015) [44]	0.5	1	1	0	0.625	Accepted
PS37	Alqassem & Svetinovic (2014) [45]	1	0.5	1	0.5	0.75	Accepted
PS38	Shin (2014) [46]	1	1	1	0.5	0.875	Accepted
PS39	Razzak (2012) [47]	0.5	0	1	1	0.625	Accepted
PS40	Zolanvari (2010) [48]	1	1	1	0.5	0.875	Accepted
PS41	Weber (2010) [49]	0.5	0.5	1	0.5	0.625	Accepted
PS42	Babar et al. (2010) [50]	0.5	1	1	1	0.875	Accepted
PS43	Niemeyer et al. (2010) [51]	1	1	0.5	0.5	0.75	Accepted
PS44	G. Rosado et al. (2006) [52]	0	1	0	0	0.25	Rejected
PS45	Al-Mawee (2012) [53]	0	0	1	1	0.5	Rejected
PS46	Gershenfeld et al. (2004) [54]	0	0.5	0.5	0.5	0.375	Rejected
PS47	Yang & Fang (2011) [55]	1	0.5	1	0	0.625	Accepted
PS48	Weber (2011) [56]	0	1	0	0	0.25	Rejected
PS49	Blowers & Iribarne [57]	0	1	0	0	0.25	Rejected
PS50	Roman et al. (2011) [58]	0	0.5	0	0	0.125	Rejected
PS51	Kim et al. (2016) [59]	0.5	1	1	0	0.625	Accepted
PS52	Mineraud et al. (2015) [60]	0	1	0.5	0	0.375	Rejected
PS53	Alsaadi & Tubaishat (2015) [61]	0	0.5	0.5	0	0.25	Rejected
PS54	Ukil et al. (2014) [62]	1	1	1	1	1	Accepted
PS55	Borgia (2014) [63]	0	1	0.5	0	0.375	Rejected
PS56	Lee & Kim (2015) [64]	0	0.5	0	0	0.125	Rejected
PS57	Aggarwal & Lal Das (2012) [65]	0.5	0.5	1	1	0.75	Rejected
PS58	Kanuparthi et al. (2013) [66]	1	0.5	1	0.5	0.75	Accepted
PS59	Lea & Blackstock (2014) [67]	0.5	0	1	1	0.625	Accepted

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Paper Study	Author	QA1	QA2	QA3	QA4	Result	Status
PS60	Ferati et al. (2016) [68]	0.5	0.5	1	0.5	0.625	Accepted
PS61	Tank et al. (2016) [69]	0.5	1	1	0	0.625	Accepted
PS62	Alqassem (2014) [70]	1	1	0.5	0.5	0.75	Accepted
PS63	Riliskis et al. (2015) [71]	0.5	1	1	0	0.625	Accepted
PS64	Banu et al. (2016) [72]	0.5	1	1	0	0.625	Accepted
PS65	C. Lee et al. (2016) [73]	1	1	1	0	0.75	Accepted
PS66	Lee & Lee (2016) [74]	0.5	1	1	0.5	0.75	Accepted
PS67	Tsang et al. (2016) [75]	1	1	1	0.5	0.875	Accepted
PS68	Fink et al. (2015) [76]	0.5	0.5	1	0.5	0.625	Accepted
PS69	Hussien et al. (2016) [77]	1	1	0.5	0	0.625	Accepted
PS70	Idoga et al. (2016) [78]	1	1	0.5	0	0.625	Accepted
PS71	Huang et al. (2016) [79]	0.5	0.5	1	1	0.75	Accepted
PS72	Kamalrudin et al. (2011) [80]	0	0.5	0.5	0.5	0.375	Rejected
PS73	Hibshi et al. (2015) [81]	0	0.5	1	0.5	0.5	Rejected
PS74	Mumtaz et al. (2016) [82]	1	0.5	0.5	0.5	0.625	Accepted
PS75	Islam & Mukhopadhyay (2016) [83]	0	0	0.5	0.5	0.25	Rejected
PS76	Abraham et al. (2017) [84]	0.5	0	1	1	0.625	Accepted
PS77	Maleh et al. (2016) [85]	0	0.5	0	0.5	0.25	Rejected
PS78	C. Lee et al. (2016) [73]	0.5	0	0	0	0.125	Rejected
PS79	Wang et al. (2012) [86]	1	1	0	0.5	0.625	Accepted
PS80	Kowkutla & Ravi (2017) [87]	0.5	0.5	1	1	0.75	Accepted
PS81	Zhou et al. (2017) [4]	1	0	1	0.5	0.625	Accepted
PS82	Muvuna et al. (2016) [88]	1	0.5	1	1	0.875	Accepted
PS83	Gabriel et al. (2017) [89]	1	0.5	1	0.5	0.75	Accepted
PS84	Dalipi & Yayilgan (2016) [5]	1	1	0.5	0	0.625	Accepted
PS85	Pradeep et al. (2016) [90]	0.5	1	1	0	0.625	Accepted
PS86	Ribeiro et al. (2016) [91]	1	1	1	0	0.75	Accepted
PS87	Reddy et al. (2017) [92]	1	0	1	0.5	0.625	Accepted
PS88	Kamalakannan & Tamilselvan (2017) [93]	0.5	0.5	1	1	0.75	Accepted
PS89	Kishore & Sharma (2016) [94]	1	0.5	0.5	0.5	0.625	Accepted
PS90	Dhillon & Kalra (2017) [95]	0.5	1	1	0.5	0.75	Accepted
PS91	Oltsik (2014) [96]	0	1	0	0	0.25	Rejected
PS92	David & Sarah (2014) [97]	0.5	1	1	0	0.625	Accepted
PS93	Dhariwal & Mehta (2017) [98]	0	1	0	0	0.25	Rejected
PS94	Selinger et al. (2013) [99]	0	0.5	0	0	0.125	Rejected
PS95	Russell et al. (2015) [100]	0.5	1	0.5	0.5	0.625	Rejected
PS96	Rose et al. (2015) [101]	0	0	0.5	0	0.125	Rejected
PS97	Peter & K.Gopal (2016) [102]	1	0.5	1	0.5	0.75	Accepted
PS98	Ukil et al. (2015) [103]	0.5	1	0.5	0.5	0.625	Accepted
PS99	Mattern & Floerkemeier (2010) [104]	0.5	0.5	1	0.5	0.625	Accepted
PS100	Tankard (2015) [105]	0	0.5	0.5	0	0.25	Rejected
PS101	Gubbi et al. (2013) [106]	0	0	0.5	0.5	0.25	Rejected
PS102	Borgohain et al. (2015) [3]	0.5	1	0.5	1	0.75	Accepted
PS103	Liu et al. (2016) [107]	0	1	0.5	1	0.625	Accepted
PS104	Das et al. (2016) [108]	0	1	1	0.5	0.625	Accepted
PS105	Nolin & Olson (2016) [109]	0	1	0.5	0	0.375	Rejected
PS106	Thatmann et al. (2015) [110]	0	0.5	1	0.5	0.5	Rejected
PS107	Summerville et al. (2015) [111]	0	0	1	1	0.5	Rejected
PS108	Vasilomanolakis (2015) [112]	0.5	1	1	0	0.625	Accepted
PS109	Bouij-pasquier et al. (2015) [113]	0.5	1	1	1	0.875	Accepted

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.2 Quality Extractions

According to Table 10, we sorted the accepted 84 paper studies which are related to research questions. We identified several studies which are appointed to single and multiple studies. Based on Table 11, we found that IEEE Xplore provided 33 relevant studies to our study, followed by Elsevier with 12 studies and Google Scholar with 10 studies. Table 12 shows types of papers which are investigated based on their effectiveness for our study. Journal articles and Conference Proceedings were found to be the highest with 52 and 41 studies. Furthermore, this study also includes seven articles, three white papers, two books and a thesis.

Table 10: Quality Extractions

Paper Study	Title	RQ1	RQ2
PS1	Towards Industrial Internet of Things: Crankshaft Monitoring, Traceability and Tracking using RFID	√	√
PS2	End-to-end Security Scheme For Mobility Enabled Healthcare Internet	√	√
PS3	The Internet of Things: A Security Point of View		√
PS4	On Perspective of Security and Privacy-preserving Solutions In The Internet of Things		√
PS5	An Intelligent Tracking System Based on Internet of Things for The Cold Chain	√	√
PS6	Internet of Things Applications and Challenges in Smart Cities: A Case Study of IBM Smart City Projects	√	√
PS7	An Efficient Secure Data Aggregation Technique for Internet of Things Network: An Integrated Approach using DB-MAC and Multi-Path Topology	√	√
PS8	Requirement of Security for IoT Application based on Gateway System		√
PS9	Attitudes and Perceptions of IoT Security in Critical Societal Services		√
PS10	Strategic Security Resource Allocation for Internet of Things		√
PS12	A Proposal of Security Requirements Definition Methodology in Connected Car Systems by CVSS v3	√	√
PS13	Lightweight Attribute-based Encryption for Internet of Things	√	√
PS14	On the Authentication of Devices in the Internet of Things	√	√
PS15	QR Code Based Mutual Authentication for Internet of Things	√	√
PS16	BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network	√	√
PS17	ARMY: Architecture for a Secure and Privacy-aware Lifecycle of Smart Objects in The Internet of Things		√
PS18	Communication and Security in Health Monitoring Systems – A Review	√	√
PS19	Feasibility Characterization of Cryptographic Primitives for Constrained (Wearable) IoT Devices		√
PS20	A Gateway based Fog Computing Architecture for Wireless Sensors and Actuator Networks		√
PS21	A Proposed Security Layer for the Internet of Things Communication Reference Model		√
PS22	Dependable Control System with Internet of Things	√	√
PS23	IoT based Smart Parking System	√	
PS24	OSCAR: Object Security Architecture for the Internet of Things	√	√
PS25	Security, Privacy, and Trust in Internet of Things: The Road Ahead		√
PS26	SecKit: A Model-based Security Toolkit for the Internet of Things		√
PS27	The Internet of Things for Health Care: A Comprehensive Survey	√	√
PS28	Session Resumption End-to-End Security for Healthcare Internet of Things	√	√
PS29	Secure MQTT for Internet of Things (IoT)		√
PS30	Security and Privacy in the Internet of Vehicles	√	
PS31	Security for Internet of Things: A Survey of Existing Protocols and Open Research Issues		√
PS32	Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography)	√	√
PS33	Security Analysis and Proposal of New Access Control Model in The Internet of Things	√	√
PS34	REST-ful CoAP Message Authentication		√
PS35	Short Paper: 'A Peer to Peer Security Protocol for the Internet of Thing'		√
PS36	Requirement Semi-formalization Methodology for SoC Design		√
PS37	A Socio-technical framework for Internet of Things Design: A Human-centered design for the Internet of Things		√
PS38	A Taxonomy of Security and Privacy Requirements for Internet of Things (IoT)	√	√
PS39	Spamming the Internet of Things: A Possibility and its Probable Solution	√	√
PS40	The Internet of Things: A Survey		√
PS41	Internet of Things – New Security and Privacy Challenges		√
PS42	Proposed Security Model and Threat Taxonomy for The Internet of Things (IOT)		√
PS43	Security Requirements of IoT-based Smart Building using RESTful Web Services		√
PS47	Security Model and Key Technologies for Internet of Things		√

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Paper Study	Title	RQ1	RQ2
PS51	A Study on Device Security in IoT Convergence		√
PS54	Lightweight Security Scheme for IoT Application using CoAP	√	√
PS57	RFID Security in The Context of "Internet of Things"	√	√
PS58	Hardware and Embedded Security in the Context of Internet of Things	√	√
PS59	Smart Cities: An IoT-centric Approach	√	√
PS60	Augmenting Requirements Gathering for People with Need using IoT: A Position Paper		√
PS61	A Survey on IoT Privacy Issues and Mitigation Techniques		√
PS62	Privacy and Security Requirements Framework for the Internet of Things	√	√
PS63	POSTER: Computations on Encrypted Data in the Internet of Things Applications		√
PS64	A Review on Biologically Inspired Approaches to Security for Internet of Things (IoT)		√
PS65	A Resource-Efficient System Architecture for Processing Various Sensor Data in Smart Home Environment	√	√
PS66	An User Authentication Scheme Based on The ECC and OpenID Techniques in The Internet of Things		√
PS67	An IoT-based Occupational Safety Management System in Cold Storage Facilities	√	√
PS68	Security and Privacy Grand Challenges for the Internet of Things		√
PS69	Secure and Efficient E-health Scheme Based on the Internet of Things	√	√
PS70	Review of Security Issues in E-Healthcare and Solutions		√
PS71	Lightweight Authentication Scheme with Dynamic Group Members in IoT Environments		√
PS74	Strong Authentication Protocol based on Java Crypto Chip as Secure Element	√	√
PS75	Smart Sensors and Internet of Things: A Postgraduate Paper	√	
PS76	Garmdroid: IoT Potential Security Threats Analysis Through the Inference of Android Applications Hardware Features Requirements	√	√
PS79	Research on Application and Security Protection on Internet of Things in Smart Grid	√	√
PS80	Chapter 12 Security Standard for Embedded Devices and Systems	√	
PS81	Security and Privacy for Cloud-Based IoT: Challenges, Countermeasures and Future Directions	√	√
PS82	System Engineering Approach to Design and Modelling of Smart Cities		√
PS83	Security analysis of a proposed internet of things middleware		√
PS84	Security and Privacy Considerations for IoT Application on Smart Grids: Survey and Research Challenge		√
PS85	IoT and Its Connectivity Challenges in Smart Home		√
PS86	Providing Security and Privacy in Smart House Through Mobile Cloud Computing		√
PS87	Building Smart Cities Based on Web Architecture and using IoT	√	√
PS88	Design of Secured and Intelligent Architecture for Security in Perceptual Layer of the Internet of Things		√
PS89	Evolution of Wireless Sensor Networks as the Framework of Internet of Things - A Review	√	
PS90	A lightweight biometrics based remote user authentication scheme for IoT services		√
PS92	Lack of Security in Internet of Things devices		√
PS97	Multi-level Authentication System for Smart Home Security Analysis and Implementation		√
PS98	Embedded security for internet of things		√
PS99	From the Internet of Computers to the Internet of Things		√
PS102	Survey of Security and Privacy Issues of Internet of Things		√
PS103	On Emerging Family of Elliptic Curves to Secure Internet of Things: ECC Comes of Age	√	
PS104	Context-Sensitive Policy Based Security in Internet of Things	√	
PS108	On the Security and Privacy of Internet of Things Architectures and Systems		√
PS109	SmartOrBAC: Security and Privacy in the Internet of Things		√

Table 11: Digital library of Paper Study

Database Library	No. Paper Study	Paper Study
ACM DL	9	PS57, PS58, PS59, PS60, PS61, PS62, PS63, PS71, PS72
Atlantis Press	1	PS67
Elsevier	12	PS1, PS2, PS4, PS5, PS24, PS25, PS37, PS39, PS40, PS90, PS101
Elvedit	1	PS53
Emerald Insight	5	PS3, PS6, PS44, PS54, PS105
Google Scholar	10	PS8, PS17, PS23, PS43, PS65, PS66, PS85, PS87, PS88, PS102
IEEE Access	3	PS9, PS11, PS75
IEEE Xplore	35	PS7, PS10, PS12, PS13, P14, PS15, PS16, PS18, PS19, PS20, PS27, PS28, PS29, PS30, PS31, PS32, P33, PS34,PS35, PS36, PS38, PS51, PS64, PS68, PS69, PS70, PS77, PS78, PS82, PS84, PS86, PS97, PS98, PS106, PS107
ScienceDirect	8	PS21, PS26, PS41, PS47, PS48, PS49, PS52, PS55
Springer Link	3	PS42, PS56, PS99

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 12: Type of Paper Study

Type study	Quantity	Paper Study
Article	7	PS17, PS50, PS81, PS92, PS93, PS100
Book	2	PS46, PS80
Conference proceeding	41	PS7, PS10, PS13, PS14, PS15, PS18, PS20, PS28, PS30, PS33, PS34, PS35, PS36, PS38, PS51, PS57, PS58, PS59, PS60, PS61, PS62, PS63, PS64, PS67, PS68, PS69, PS70, PS71, PS72, PS75, PS76, PS77, PS79, PS82, PS84, PS86, PS97, PS98, PS104, PS106, PS107
Journal article	52	PS1, PS2, PS3, PS4, PS5, PS6, PS8, PS9, PS11, PS12, PS16, PS19, PS21, PS22, PS23, PS24, PS25, PS26, PS27, PS31, PS32, PS37, PS39, PS40, PS41, PS42, PS43, PS44, PS47, PS48, PS49, PS52, PS53, PS54, PS55, PS56, PS65, PS66, PS73, PS74, PS78, PS83, PS85, PS88, PS89, PS90, PS99, PS101, PS103, PS105
Thesis	1	PS45
White paper	3	PS91, PS95, PS96

3.3 RQ1: What are the most used technologies in Internet of Things (IoT) applications?

Figure 3 shows the technologies involves in IoT applications. IoT is fascinating and it connects everyday devices to the internet. It can be hard to wrap the head around at times. However, with all the technologies, everyone is moving forward to a future where devices are smarter and we will be able to leverage technology to create more efficient, intelligent machines. This study identifies 20 technologies which are being used in IoT applications. Based on the list of the most used technologies in Table 13, we found that sensors are the most used technology for IoT, which accounts for 23 studies. This is followed by mobility networks with 15 studies, RFID systems with 12 studies, WiFi with 9 studies, Bluetooth and Zigbee with 8 studies.

Figure 3: IoT Technologies (www.postscapes.com)

a) Sensors

They are currently used in various fields like healthcare, military, and industry. Each sensor network consists of a large number of sensing nodes, in addition to a special node called sink, where the sink node is used to collect sensing results reported by other nodes in the network [45]. Because such networks can cooperate with RFID systems to enhance objects tracking, sensor networks have a significant role in the IoT development.

b) Mobility networks

Mobility is referred as the capacity to maintain connections and service no matter where user's data are located. The location data must be transparent and used only by the system to protect users' privacy [114]. loT environment can be characterized by a high level of mobility. Other than that, smart mobility generally involves efficient transportation systems which make use of time and energy efficiently. It also involves transportation systems which use renewable energy rather than relying on fossil fuel as well as encouraging and promoting non-motorised transportation [88].

c) RFID Systems

The full deployment of IoT relies on the widespread use of Radio-Frequency Identification (RFID) tags in identifying everyday objects. This enables the tracking ability of objects through space and time in a sustainable manner [45]. Most RFID systems have a generic architecture comprises of three main components [9]. Firstly, RFID readers

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

or reading points are located throughout the production line configured to read/write data from/to RFID tags affixed to parts, where in each RFID tag uniquely identifies a part. Next, a data processing system is configured to process the data collected by the RFID reader and a service application is developed to provide tracking and traceable information to the end users. RFID is considered as an enabling technology and it has a wide range of beneficial applications such as electronic toll collection systems, access management systems, airport baggage tracking logistics and other applications.

d) WiFi

Wi-Fi is a technology that allows electronic devices to exchange data wirelessly (using radio waves) over a computer network, including high-speed Internet connections. WiFi enables communication between electronic devices such as smartphones, tablets, and others [90]. The Wi-Fi Alliance defines Wi-Fi as any wireless local area network (WLAN) products which are based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards. Variation of wireless network protocols are being applied in smart home applications, like IEEE 802.11 (Wi-Fi), Bluetooth LE (Low Energy), cellular, ZigBee (a low- power wireless technology), Z-Wave and Thread.

e) Bluetooth

Bluetooth is a wireless technology standard for exchanging data over short distances from fixed and mobile devices, creating personal area networks (PANs) with high levels of security. Bluetooth is a technology intended at being a secured and a tawdry means of connecting and transmitting data between supported devices. Bluetooth has the frequency radio bands from 2.4 to 2.485 GHz [90]. It importantly reduces power consumption of Bluetooth devices and enables long term operation using coin cell batteries. Bluetooth offers an infrastructure of direct connection from smartphones and tablets, leaving users to control household appliances from their mobile devices.

Table 13: IoT Technologies

Types Selection	Quantity	Paper Study
Actuators	6	PS20, PS22, PS33, PS58, PS107, PS40
Bluetooth	8	PS12, PS18, PS23, PS27, PS33, PS69, PS85, PS86
Cloud	5	PS6, PS18, PS81, PS86, PS87
Embedded system	3	PS2, PS19, PS27
Ethernet	1	PS20
GPRS	2	PS16, PS69
GPS	5	PS5, PS23, PS54, PS79, PS40
IEEE 802.11/ 802.15/802.16	5	PS4, PS18, PS28, PS31, PS85
IPv6	4	PS27, PS28, PS31, PS85
Mobility networks (GSM/3G/LTE/GPRS)	15	PS5, PS6, PS14, PS16, PS18, PS20, PS23, PS27, PS30, PS54, PS69, PS74, PS79, PS86, PS40
QR Code	1	PS15
RFID Systems	12	PS1, PS5, PS14, PS23, PS27, PS32, PS39, PS40, PS57, PS62, PS67, PS74
Sensors	23	PS76, PS2, PS5, PS13, PS16, PS18, PS19, PS20, PS65, PS69, PS75, PS104, PS23, PS27, PS28, PS30, PS33, PS38, PS54, PS59, PS62, PS58, PS40
Smart gateways	1	PS2
WiFi	9	PS18, PS28, PS33, PS67, PS69, PS85, PS86, PS79, PS40
WiMAX	1	PS19
Wireless sensor network	7	PS7, PS23, PS27, PS30, PS31, PS33, PS40
Z-Wave	1	PS85
Zigbee	8	PS5, PS18, PS20, PS23, PS33, PS80, PS85, PS79
2D Barcode	1	PS39

3.4 RQ2: What are the important security requirements needed for Internet of Things (IoT) applications?

There are 83 security requirements altogether identified from the total of 84 studies which are related to security properties involved in security requirements on IoT applications. IoT has huge potential to develop new intelligent applications in nearly every field. The various applications can be grouped into three major domains [63] as shown in Figure 4. They are industrial domain, smart city domain and health well-being domain. Each domain is not isolated from others but it is partially overlapped since some applications are shared.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 14 shows all security requirements needed for IoT applications and Table 15 shows security requirements according to IoT applications.

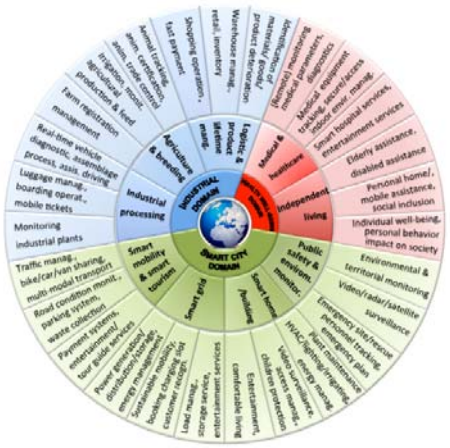

Figure 4: IoT Application Domain and Related Applications [63]

Table 14: Security Requirements

Types Selection	Quantity	Paper Study
Access control	12	PS2, PS7, PS13, PS71, PS21, PS25, PS26, PS33, PS109, PS68, PS38, PS41
Anonymization	6	PS16, PS26, PS31, PS32, PS33, PS108
Assurance	1	PS21
Attack resistance	2	PS90, PS32
Authentication	36	PS81, PS83, PS7, PS8, PS14, PS15, PS16, PS17, PS64, PS66, PS69, PS70, PS71, PS84, PS86, PS97, PS21, PS22, PS24, PS25, PS27, PS31, PS34, PS108, PS68, PS95, PS102, PS38, PS54, PS39, S79, PS47, PS98, PS40, PS42, PS43
Authorization	15	PS17, PS64, PS69, PS70, PS86, PS24, PS26, PS27, PS35, PS108, PS95, PS38, PS92, PS42, PS43
Availability	11	PS90, PS21, PS27, PS30, PS31, PS32, PS108, PS68, PS102, PS47, PS98
Client privacy	1	PS41
Communication Security	1	PS51
Confidentiality	20	PS83, PS90, PS3, PS12, PS61, PS7, PS74, PS84, PS21, PS25, PS26, PS27, PS31, PS32, PS108, PS68, PS54, PS47, PS98, PS42
Contextual	2	PS109, PS38
Cryptographic	7	PS88, PS13, PS51, PS71, PS24, PS29, PS39
Cryptographic Primitive	1	PS19
Data access	1	PS18
Data authentication	3	PS3, PS18, PS41
Data confidentiality	6	PS2, PS18, PS69, PS97, PS28, PS95
Data Encryption	1	PS4
Data freshness	3	PS16, PS18, PS27
Data integrity	8	PS2, PS16, PS18, PS21, PS28, PS95, PS38, PS47
Data Privacy	1	PS108
Data protection	1	PS51
Data provenance	1	PS58
Data retention	1	PS26
Denial of Services (DoS)	2	PS2, PS28
Dynamic Information Sensing	1	PS37
Embedding	1	PS39
Encryption Algorithm	6	PS88, PS13, PS29, PS35, PS63, PS42
Encryption key	5	PS81, PS88, PS24, PS92, PS79
End-to-end security	2	PS2, PS28
Enforcement	1	PS25
Fault Tolerance	4	PS2, PS97, PS27, PS99
Forward security	3	PS90, PS28, PS32
Functionality	1	PS62
Group Authentication	1	PS3
Hash Functions	3	PS4, PS69, PS71
High mobility	1	PS30
Identification	6	PS51, PS70, PS37, PS79, PS40, PS42
Identity management	2	PS108, PS58
Information security	2	PS8, PS23
Information Transmission	1	PS37
Integrity	19	PS83, PS3, S12, PS61, PS64, PS70, PS74, PS84, PS97, PS24, PS31, PS10, PS68, PS102, PS38, S54, PS58, PS39, PS79
Interoperability	1	PS99
Key Protection	1	PS3
Key distribution	1	PS30
Lightweight solutions	7	PS81, PS2, PS51, PS71, PS29, PS33, PS109
Local security	1	PS23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Types Selection	Quantity	Paper Study
Low computational	1	PS54
Low error tolerance	1	PS30
Manageability	1	PS20
Middleware	1	PS25
Mutual authentication	8	PS90, PS2, PS69, PS71, PS97, PS28, PS32, PS54
Mutual authorization	3	PS2, PS28, PS57
Network security	1	PS7
Network Transmission	2	PS8, PS23
Non-repudiation	9	PS3, PS18, PS70, PS74, PS84, PS21, PS26, PS31, PS98
Notarization/Signature	1	PS21
Physical protection	1	PS51
Privacy	7	PS81, PS83, PS7, PS25, PS38, PS92, PS42
Privacy Preservation	1	PS97
Privacy Protection	1	PS3
Pseudonymity	1	PS108
Public key cryptography	1	PS39
Reliability	3	PS28, PS62, PS47
Resiliency	3	PS27, PS31, PS108
Resistance to relay attacks	1	PS57
Resistance to disclosure attacks	1	PS57
Resistance to desynchronization attacks	1	PS57
Robustness	1	PS108
Scalability	8	PS87, PS90, PS20, PS28, PS32, PS33, PS109, PS99
Secure Localization	1	PS16
Security of Keys	1	PS3
Self-healing	1	PS27
Semi-formalization	1	PS36
Sensor spoofing	1	PS2
Service Authentication	1	PS3
Smart gateway	1	PS2
Support security	1	PS38
Trust	4	PS25, PS31, PS108, PS42
Trust management	2	PS26, PS58
Unlink ability	1	PS33, PS38, PS62
Usability	3	PS33, PS38, PS108
User content	1	PS26
Verification	3	PS34, PS39, PS43

Based on the list of IoT applications and its security requirements in Table 14, we found that authentication is the most commonly investigated property which accounts for 36 studies. This is followed by confidentiality with 20 studies, integrity with 19 studies, authorization with 15 studies, access control with 12 studies and availability with 11 studies.

a) Authentication

One of the important security requirements found in this study is authentication. Authentication enables an IoT device to ensure the identity of the peer that it communicates [35]. Authentication is essential to create trustable services. IoT is a network in which billions of entities are connected. Managing identity is a major challenge. The edges are equipped with the computational capability and can communicate with any other edge without external intervention [15]. Hence, authentication logic is required in every entity. Interactions are very dynamic and a user might not know whom he will have to interact with in a particular event. This means that even in a network of users whose information is gathered, users are not encouraged to trust others except for the base station offering the service.

b) Confidentiality

Most of the studies focus on confidentiality. Confidentiality ensures private information will not be accessible for unauthorized users. In addition, confidential messages will not reveal their content to eavesdroppers. This requirement means that secret information must be transmitted securely during all communications between communicating parties. For that reason, communicating parties must exchange all information in an encrypted form in order to ensure confidentiality. [95].

c) Integrity

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data will not be altered by unauthorized people (for example, in a breach of confidentiality). These measures include

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

file permissions and user access controls. Backups or redundancies must be available to restore the affected data to its correct state. Furthermore, integrity ensures that important data received will not be altered in transit by an adversary. In addition, the integrity of stored data and content should not be compromised [35].

d) Authorization

Authorization ensures that only authorized nodes are accessible for network services or recourses. Authorization is granting a right or permission to a system or application entity in accessing system resources. This function determines who can be trusted for a given purpose. In addition, security authorization is the process in which a senior management official and the authorizing official reviews security-related information describing the current security posture of an information system. Then the information is used to determine whether or not the mission/business risk of operating a system is acceptable and if it is, explicitly accepts the risk [115].

e) Access control

Access control is prevention of unauthorized use of a resource, including prevention of the use of a resource in an unauthorized manner. Several studies choose access control that verifies user's identity in each and every step of the request similar to the point-to-point access control scheme. Access control refers to permission in the usage of the resources, assigned to differentiate actors of wide IoT network [33].

f) Availability

Availability enforces the check on the server or the nodes so that it is continuously available for the user to access information or to send commands to the nodes when required. Availability as the ability to make information and related physical and logical resources accessible as needed, when they are needed and where they are needed [115]. In IoT healthcare services, an availability ensures survival of IoT healthcare services (either local or global/cloud services) to authorized parties when needed even under denial-of-services attacks [77].

As a conclusion, although authentication is the most concerned property identified in this study, the weight of applying the security properties is different. It shows all six security requirements which are confidentiality, integrity, authorization, access control, and availability have gained more attention in IoT applications.

Table 15: IoT Based Applications and Security Requirements

IoT Applications		Security Requirements	Quantity	Paper Study
Industrial domain	Logistic and product lifetime management	Authentication	2	PS8, PS40
		Identification	2	PS37, PS40,
		Dynamic Information Sensing	1	PS37
		Information Transmission	1	PS37
		Information security	1	PS8
		Network Transmission	1	PS8
		Cryptographic Primitive	1	PS19
	Agriculture and breeding	Authentication	1	PS40
		Identification	1	PS40
Smart city domain	Smart mobility and smart tourism	Authentication	7	PS21, PS24, PS31, PS39, PS54, PS81 PS83
		Cryptographic	3	PS24, PS29, PS39
		Embedding	1	PS39
		Integrity	8	PS12, PS24, PS31, PS39, PS54, PS58, PS74, PS83
		Public key cryptography	1	PS39
		Verification	1	PS39
		Data provenance	1	PS58
		Identity management	1	PS58
		Trust management	1	PS58
		Dynamic Information Sensing	1	PS37
		Identification	1	PS37
		Information Transmission	1	PS37
		Confidentiality	2	PS74, PS81
		Low computational	1	PS54

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IoT Applications	Security Requirements	Quantity	Paper Study
	Mutual authentication	1	PS54
	Access control	1	PS21
	Assurance	1	PS21
	Availability	4	PS12, PS21, PS30, PS31
	Data integrity	1	PS21
	Non-repudiation	3	PS21, PS31, PS74
	Notarization/Signature	1	PS21
	Authorization	2	PS24, PS35
	Encryption key	2	PS24, PS81
	Encryption Algorithm	2	PS29, PS35
	Lightweight solutions	2	PS29, PS81
	High mobility	1	PS30
	Key distribution	1	PS30
	Low error tolerance	1	PS30
	Anonymization	1	PS31
	Resiliency	1	PS31
	Trust	1	PS31
	Semi-formalization	1	PS36
	Privacy	2	PS81, PS83
Smart grid	Authentication	2	PS38, PS79
	Encryption key	1	PS79
	Identification	3	PS37, PS79, PS51
	Integrity	3	PS38, PS58, PS79
	Data provenance	1	PS58
	Identity management	1	PS58
	Trust management	1	PS58
	Dynamic Information Sensing	1	PS37
	Information Transmission	1	PS37
	Access control	2	PS13, PS38
	Authorization	1	PS38
	Contextual	1	PS38
	Data integrity	1	PS38
	Cryptographic Primitive	1	PS4
	Data Encryption	1	PS4
	Hash Functions	1	PS4
	Cryptographic	2	PS13, PS51
	Encryption Algorithm	1	PS13
	Manageability	1	PS20
	Scalability	1	PS20
	Communication Security	1	PS51
	Data protection	1	PS51
	Lightweight solutions	1	PS51
	Physical protection	1	PS51
Smart home/building	Authentication	6	PS8, PS15, PS40, PS43, PS84, PS97
	Authorization	2	PS26, PS43
	Encryption Algorithm	1	PS43
	Verification	1	PS43
	Identification	2	PS37, PS40
	Dynamic Information Sensing	1	PS37
	Information Transmission	1	PS37
	Access control	3	PS26, PS33, PS109
	Anonymization	2	PS26, PS33
	Confidentiality	2	PS26, PS84
	Data retention	1	PS26
	Non-repudiation	2	PS26, PS84
	Trust management	1	PS26
	User content	1	PS26
	Lightweight solutions	2	PS33, PS109
	Scalability	3	PS33, PS83, PS109
	Usability	2	PS33, PS38
	Privacy	1	PS38
	Support security	1	PS38
	Contextual	1	PS109

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IoT Applications		Security Requirements	Quantity	Paper Study
		Cryptographic Primitive	1	PS4
		Data Encryption	1	PS4
		Hash Functions	1	PS4
		Information security	1	PS8
		Network Transmission	1	PS8
		Integrity	1	PS84
		Data confidentiality	1	PS97
		Forward security	1	PS97
		Mutual authentication	1	PS97
		Privacy Preservation	1	PS97
	Public safety and environment monitoring	Authentication	1	PS40
		Identification	1	PS40
		Privacy	1	PS38
		Support security	1	PS38
		Usability	1	PS38
Health well-being domain	Medical and healthcare	Data provenance	1	PS58
		Identity management	1	PS58
		Integrity	2	PS58, PS70
		Trust management	1	PS58
		Dynamic Information Sensing	1	PS37
		Identification	2	PS37, PS70
		Information Transmission	1	PS37
		Authentication	4	PS16, PS27, PS69, PS70
		Authorization	3	PS27, PS69, PS70
		Availability	2	PS27, PS32
		Confidentiality	3	PS27, PS32, PS70
		Data freshness	3	PS16, PS18, PS27
		Fault Tolerance	1	PS27
		Resiliency	1	PS27
		Self-healing	1	PS27
		Data confidentiality	4	PS2, PS18, PS28, PS69
		Data integrity	4	PS2, PS16, PS18, PS28
		Denial of Services (DoS)	2	PS2, PS28
		End-to-end security	2	PS2, PS28
		Forward security	3	PS2, PS28, PS32
		Mutual authentication	4	PS2, PS28, PS32, PS69
		Mutual authorization	2	PS2, PS28
		Reliability	1	PS28
		Scalability	2	PS28, PS32
		Anonymization	2	PS16, PS32
		Attack resistance	1	PS32
		Privacy	1	PS38
		Support security	1	PS38
		Usability	1	PS38
		Access control	1	PS2
		Architecture scalability	1	PS2
		Lightweight solutions	1	PS2
		Sensor spoofing	1	PS2
		Smart gateway	1	PS2
		Secure Localization	1	PS16
		Data access	1	PS18
		Data authentication	1	PS18
		Non-repudiation	2	PS18, PS70
		Hash Functions	1	PS69
	Independent	Usability	1	PS60
		Acceptability	1	PS60

4 FINDINGS

The findings have addressed the following two research questions of this study:

a) QA1: What are the most used technologies for Internet of Things (IoT) applications?
b) QA2: What are the important security requirements needed for Internet of Things (IoT) applications?

The following are the summary of the main findings from the SLR. These findings are

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

considered as the challenges in the security requirements for IoT applications.

4.1 The most used technologies for the Internet of Things (IoT) Applications.

There are many technologies that enable IoT. Crucial to this field is the network used to communicate between devices of an IoT installation, a role that several wireless or wired technologies may fulfill. We have identified that the most used technologies for IoT applications are sensors, mobility networks, RFID systems, WiFi, Bluetooth, and Zigbee. Based on the result, sensors become the most technology used in IoT base applications. Sensors are now found in a wide variety of applications, such as smart mobile devices, automotive systems, industrial control, healthcare, smart city and climate monitoring. Sensors are used almost everywhere and now sensor technology is beginning to closely mimic the ultimate sensing machine which are the human being. Furthermore, in IoT, sensors are the troops of it, in which the small hardware who does all the critical work of monitoring process, taking measurements and collecting data. The first things that people think when picturing the IoT is sensors.

4.2 The important security requirements needed for the Internet of Things (IoT) applications.

We discovered important security requirements for IoT applications, namely; authentication, confidentiality, integrity, authorization, access control, and availability were applied in IoT applications. The focus of the six security requirements are to help the requirements engineer to improve security requirements relevant for IoT applications. Authentication is the most important properties needed for IoT based applications. It is the process of identifying an individual, usually based on a username and password. In IoT security, authentication is usually distinct from authorization, in which it is the process of giving individuals an access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

4.3 Strengths and weakness of SLR

The strength and weakness of SLR conducted are identified based on keyword search as well as inclusion and exclusion process. The strength of SLR is the use of a systematic approach which includes inclusion and exclusion. This SLR examined a reference list of selected primary studies in identifying any additional studies. SLR also extracts relevant information consistency while reducing biases and validity by authors. The weakness of this SLR is that it cannot ensure that the search facilities will return a set of papers similar to a search process conducted independently. Therefore, there may be other solutions provided by the IoT security methods due to the failure in capturing some of the methods proposed.

4.4 Implications for Research and Society

This study is the first SLR conducted to investigate an analysis of security requirements for IoT applications. It is also the first SLR to identify security requirements related to IoT applications development. Our research work contributes to research efforts for IoT analysis especially on security requirements for IoT applications. The security requirements discussed in this paper will help requirements engineer and client-stakeholder to analyze and identify appropriate security requirements for any IoT applications and improve the quality of security requirements. In addition, there are also advantages for IoT engineering researcher to find solution, be aware of the process and method as well as identify and approach related security requirements in solving challenges which have been identified.

5 CONCLUSION

This paper described SLR which is targeted at empirical studies in analyzing security requirements for IoT applications and total of 84 primary studies have been selected. We found that authentication, confidentiality, integrity, authorization, access control and availability are important security properties needed for IoT applications. Five methods have been used to analyse the security requirement for IoT applications. Findings also show that IoT security requirements properties are the major concern in this study. There are various methods employed to analyse security requirements for IoT applications. As a conclusion, this study shows that analyzing security requirements for IoT

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

applications are rarely employed in the development of IoT applications although it is a crucial process needed from early phase as it is highly exposed to privacy and security issues.

ACKNOWLEDGEMENTS

The authors would like to acknowledge Universiti Teknikal Malaysia Melaka (UTeM) and Ministry of Education (MoE) for its support and the funding of this FRGS research grant: FRGS/1/2016/ICT01/FTMK-CACT/F00325.

REFERENCES

[1] Cisco, "IoT Threat Environment : An Overview of the Iot Threat Lanscape with Risk-based Security Prigram Recommendations," 2015.

[2] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[3] T. Borgohain, U. Kumar, and S. Sanyal, "Survey of Security and Privacy Issues of Internet of Things," *Cryptogr. Secur.*, p. 7, 2015.

[4] J. Zhou, Z. Cao, X. Dong, and A. V Vasilakos, "Security and Privacy for Cloud-Based IoT: Challenges, Countermeasures, and Future Directions," *Impact Next-Generation Mob. Technol. IoT Cloud Converg.*, no. January, pp. 26–33, 2017.

[5] F. Dalipi and S. Y. Yayilgan, "Security and Privacy Considerations for IoT Application on Smart Grids: Survey and Research Challenges," in *2016 4th Conference on Future Internet of Things and Cloud Workshops*, 2016.

[6] 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, 2007.

[7] B. A. Kitchenham, "Guidelines for Performing Systematic Literature Reviews in Software Engineering," 2007.

[8] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering – A systematic literature review," *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, 2009.

[9] D. M. Segura, N. Kaur, W. G. Whittow, P. P. Conway, and A. A. West, "Towards industrial internet of things: Crankshaft Monitoring, Traceability and Tracking using RFID," *Robot. Comput. Integr. Manuf.*, vol. 41, pp. 66–77, 2016.

[10] S. Rahimi, T. Nguyen, and A. M. Rahmani, "End-to-end Security Scheme for Mobility Enabled Healthcare Internet of Things," *Futur. Gener. Comput. Syst.*, vol. 64, pp. 108–124, 2016.

[11] S. Li, T. Tyrfonas, and H. Li, "The Internet of Things: A Security Point of View," *Internet Res.*, vol. 26, no. 26, pp. 337–356, 2016.

[12] L. Malina, J. Hajny, R. Fujdiak, and J. Hosek, "On Perspective of Security and Privacy-preserving Solutions in The Internet of Things," *Comput. Networks*, vol. 102, pp. 83–95, 2016.

[13] H. Lau, M. Zhu, and S. Ye, "An Intelligent Tracking System Based on Internet of Things for The Cold Chain," *Internet Res.*, vol. 26, no. 2, pp. 435–445, 2016.

[14] V. Scuotto, A. Ferraris, and S. Bresciani, "Internet of Things: Applications and Challenges in Smart Cities: A Case Study of IBM Smart City Projects," *Bus. Process Manag. J.*, vol. 22, no. 2, pp. 357–367, 2016.

[15] S. S. Sruthi and G. Geethakumari, "An Efficient Secure Data Aggregation Technique for Internet of Things Network: An Integrated Approach Using DB-MAC and Multi-path Topology," *2016 IEEE 6th Int. Conf. Adv. Comput.*, pp. 599–603, 2016.

[16] J. T. Kim, "Requirement of Security for IoT Application Based on Gateway," *Int. J. Secur. Its Appl.*, vol. 9, no. 10, pp. 201–208, 2015.

[17] M. Asplund and S. Nadjm-Tehrani, "Attitudes and Perceptions of IoT Security in Critical Societal Services," *IEEE Access*, vol. 4, pp. 2130–2138, 2016.

[18] A. Rullo, D. Midi, E. Serra, and E. Bertino, "Strategic Security Resource Allocation for Internet of Things," in *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*, 2016, pp. 737–738.

[19] M. Mori, Y. Sueda, and M. Aihara, "Secure Connection Assistence Architecture for IoT Devices," *IEEE Access*, pp. 34–35, 2016.

[20] E. Ando and M. Kayashima, "A Proposal of Security Requirements Definition Methodology in Connected Car Systems by

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CVSS v3," *Int. Congr. Adv. Appl. Informatics*, 2016.

[21] N. Oualha and K. Thuat Nguyen, "Lightweight Attribute-based Encryption for the Internet of Things," in *Computer Communication and Networks (ICCCN), 2016 25th International Conference*, 2016.

[22] Y. Sharaf-Dabbagh and W. Saad, "On the Authentication of Devices in the Internet of Things," in *2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Network (WoWMoM)*, 2016, pp. 1–3.

[23] T. Marktscheffel, W. Popp, S. D. Fink, and A. Bilzhause, "QR Code Based Mutual Authentication Protocol for Internet of Things," in *2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Network (WoWMoM)*, 2016.

[24] P. Gope and T. Hwang, "BSN-Care: A Secure IoT-Based Modern Healthcare using Body Sensor Network," *IEEE Sens. J.*, vol. 16, no. 5, pp. 1368–1376, 2016.

[25] A. Skarmeta, "ARMY : Architecture for a Secure and Privacy -Aware Lifecycle of Smart Objects in the Internet of Things," *IEEE Commun. Mag.*, no. September, pp. 28–35, 2016.

[26] H. Fotouhi, A. Cauˇ, K. Lundqvist, and M. Bj, "Communication and Security in Health Monitoring Systems - A Review," in *Annual Computer Software and Applications Conference*, 2016, vol. 40, pp. 545–554.

[27] A. Ometov *et al.*, "Feasibility Characterization of Cryptographic Primitives for Constrained (Wearable) IoT Devices," in *The First International Workshop on Security, Privacy and Trust for IoT*, 2016.

[28] W. Lee, K. Nam, H. Roh, and S. Kim, "A Gateway Based Fog Computing Architecture for Wireless Sensors and Actuator Networks," in *2016 18th International Conference on Advanced Communication Technology (ICACT)*, 2016, pp. 210–213.

[29] H. M. Aldosari, "A Proposed Security Layer for the Internet of Things Communication Reference Model," *Procedia Comput. Sci.*, vol. 65, pp. 95–98, 2015.

[30] T. Tran and Q. P. Ha, "Dependable Control Systems With Internet of Things," *ISA Trans.*, vol. 59, pp. 303–313, 2015.

[31] A. Khanna and R. Anand, "IoT based Smart Parking System," *2016 Int. Conf. Internet Things Appl.*, pp. 266–270, 2016.

[32] M. Vučinić, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, "OSCAR: Object security Architecture for The Internet of Things," *Ad Hoc Networks*, vol. 32, pp. 3–16, 2015.

[33] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-porisini, "Security, Privacy and Trust in Internet of Things: The Road Ahead," *Comput. Networks*, vol. 76, pp. 146–164, 2015.

[34] R. Neisse, G. Steri, I. N. Fovino, and G. Baldini, "SecKit : A Model-based Security Toolkit for The Internet of Things," *Comput. Secur.*, vol. 54, pp. 60–76, 2015.

[35] S. M. R. Islam, D. Kwak, and H. Kabir, "The Internet of Things for Health Care : A Comprehensive Survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[36] S. R. Moosavi, T. Nguyen Gia, Am. Mohammad Rahmani, S. Virtanen, H. Tenhunen, and J. Isoaho, "Session Resumption-Based End-to-End Security for Healthcare Internet of Things," *2015 IEEE Int. Conf. Comput. Inf. Technol. ; Ubiquitous Comput. Commun. ; Dependable , Auton. Secur. Comput. ; Pervasive Intell. Comput.*, pp. 581–588, 2015.

[37] M. Singh, R. Ma, S. Vl, and P. Balamuralidhar, "Secure MQTT for Internet of Things (IoT)," *2015 Fifth Int. Conf. Commun. Syst. Netw. Technol.*, vol. 16, pp. 746–751, 2015.

[38] L. Wu *et al.*, "Security and Privacy in the Internet of Vehicles," in *2015 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI)*, 2015.

[39] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 3, pp. 1–20, 2015.

[40] D. He and S. Zeadally, "An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography," *IEEE Internet Things J.*, vol. 2, no. 1, pp. 72–83, 2015.

[41] A. Ouaddah, I. B. Anas, A. Elkalam, and A. A. I. T. Ouahman, "Security Analysis and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Proposal of New Access Control Model in the Internet of Thing," in *Ist International Conference on Electrical and Information Technologies ICEIT'2015*, 2015.

[42] H. V. Nguyen and L. Lo Iacono, "REST-ful CoAP Message Authentication," in *2015 International Workshop on Secure Internet of Things*, 2015, pp. 35–43.

[43] H. Zhang and T. Zhang, "Short Paper : 'A Peer to Peer Security Protocol for the Internet of Things,'" in *2015 18th International Conference on Intelligence in Next Generation Networks*, 2015, pp. 154–156.

[44] L. Mu, S. Kandl, P. Puschner, M. Hübl, A. Buzo, and G. Pelz, "Requirement Semi-formalization Methodology for SoC Design," *ISOCC 2015*, pp. 9–10, 2015.

[45] I. Alqassem and D. Svetinovic, "A Taxonomy of Security and Privacy Requirements for The Internet of Things (IoT)," *2014 IEEE Int. Conf. Ind. Eng. Eng. Manag.*, pp. 1244–1248, 2014.

[46] D. Shin, "A socio-technical Framework for Internet-of-Things design: A human-Centered Design for the Internet of Things," *Telemat. Informatics*, vol. 31, no. 4, pp. 519–531, 2014.

[47] F. Razzak, "Spamming the Internet of Things: A Possibility and Its Probable Solution," *Procedia Comput. Sci.*, vol. 10, pp. 658–665, 2012.

[48] M. Zolanvari, "IoT Security: A Survey," pp. 1–15, 2010.

[49] R. H. Weber, "Internet of Things - New Security and Privacy Challenges," *Comput. Law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, 2010.

[50] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed Security Model and Threat Taxonomy for The Internet of Things (IoT)," *Commun. Comput. Inf. Sci.*, vol. 89, pp. 420–429, 2010.

[51] M. Niemeyer, K. Henneböhle, and M. Kuller, "Security Requirements of IoT-based Smart Buildings using RESTful Web Services," pp. 1–10, 2010.

[52] D. G. Rosado, C. Gutierrez, E. Fernandez-Medina, and M. Piattini, "Security Patterns and Requirements for Internet-based Applications," *Internet Res.*, vol. 16, no. 5, pp. 519–536, 2006.

[53] W. Al-mawee, "Privacy and Security Issues in IoT Healthcare Applications for the Disabled Users a Survey," 2012.

[54] N. Gershenfeld, R. Krikorian, and D. Cohen, *The Internet of Things: Converging Technologies for Smart Environment and Integrated Ecosystems*, vol. 291, no. 4. 2004.

[55] J. Yang and B. Fang, "Security Model and Key Technologies for the Internet of Things," *J. China Univ. Posts Telecommun.*, vol. 18, no. December, pp. 109–112, 2011.

[56] R. H. Weber, "Accountability in the Internet of Things," *Comput. Law Secur. Rev.*, vol. 27, no. 2, pp. 133–138, 2011.

[57] M. Blowers and J. Iribarne, "The Future Internet of Things and Security of its Control Systems."

[58] R. Roman, P. Najera, and J. Lopez, "Securing The Internet of Things," *IEEE Computer Society*, Spain, pp. 51–58, Sep-2011.

[59] H. J. Kim, H. S. Chang, J. J. Suh, and T. S. Shon, "A Study on Device Security in IoT Convergence," in *2016 International Conference Industrial Engineering, Management Science and Application (ICIMSA)*, 2016.

[60] J. Mineraud, O. Mazhelis, X. Su, and S. Tarkoma, "A Gap Analysis of Internet-of-Things Platforms," *Comput. Commun.*, vol. 89–90, pp. 5–16, 2015.

[61] E. Alsaadi and A. Tubaishat, "Internet of Things : Features, Challenges, and Vulnerabilities," *Int. J. Adv. Comput. Sci. Inf. Technol.*, vol. 4, no. 1, pp. 1–13, 2015.

[62] A. Ukil, S. Bandyopadhyay, A. Bhattacharyya, A. Pal, and T. Bose, "Lighweight Security Scheme for IoT Application using CoAP," *Int. J. Pervasive Comput. Commun.*, vol. 10, no. 4, pp. 372–392, 2014.

[63] E. Borgia, "The Internet of Things Vision: Key Features, Applications and Open Issues," *Comput. Commun.*, vol. 54, pp. 1–31, 2014.

[64] Y. Lee and D. H. Kim, "Threats Analysis, Requirements and Considerations for Secure Internet of Things," *Int. J. Smart Home*, vol. 9, no. 12, pp. 191–198, 2015.

[65] R. Aggarwal and M. Lal Das, "RFID Security in the Context of 'Internet of Things,'" in *Proceedings of the First International Conference on Security of Internet of Things (SecurIT' 12)*, 2012, pp. 51–56.

[66] A. Kanuparthi, R. Karri, and S. Addepalli,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

"Hardware and Embedded Security in the Context of Internet of Things," in *Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles - CyCAR '13*, 2013, pp. 61–64.

[67] R. Lea and M. Blackstock, "Smart Cities: An IoT-centric Approach," in *Proceedings of the 2014 International Workshop on Web Intelligence and Smart Sensing (IWWISS '14)*, 2014, pp. 1–2.

[68] M. Ferati, A. Kurti, B. Vogel, and B. Raufi, "Augmenting Requirements Gathering for People with Special Needs using IoT : A Position Paper," *2016 9th Int. Work. Coop. Hum. Asp. Softw. Eng. Augment.*, pp. 48–51, 2016.

[69] B. Tank, H. Upadhyay, and H. Patel, "A Survey on IoT Privacy Issues and Mitigation Techniques," *IEEE Int. Symp. Circuits Syst. (ISCAS),* pp. 9–12, 2016.

[70] I. Alqassem, "Privacy and Security Requirements Framework for the Internet of Things (IoT)," *ICSE Companion 2014 Companion Proc. 36th Int. Conf. Softw. Eng.*, pp. 739–741, 2014.

[71] L. Riliskis, H. Shafagh, and P. Levis, "POSTER : Computations on Encrypted Data in the Internet of Things Applications," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015, pp. 1668–1670.

[72] R. Banu, N. Fathima, and G. F. Ali Ahammad, "A Review on Biologically Inspired Approaches to Security for Internet of Things (IoT)," *Int. Conf. Electr. Electron. Optim. Tech. (ICEEOT)-2016*, pp. 1062–1066, 2016.

[73] C. Lee, C. Byun, and H. Shin, "A Resource-Efficient System Architecture for Processing Various Sensor Data in Smart home Environment," *Int. J. Smart Home*, vol. 10, no. 11, pp. 69–78, 2016.

[74] J. J. Lee and K. Y. Lee, "An User Authentication Scheme Based on the ECC and OpenID Techniques in the Internet of Things," *Int. J. Secur. Its Appl.*, vol. 10, no. 11, pp. 79–88, 2016.

[75] Y. P. Tsang, K. L. Choy, and T. C. Poon, "An IoT-based Occupational Safety Management System in Cold Storage Facilities," in *International Workshop of Advanced Manufacturing and Automation (IWAMA 2016)*, 2016, pp. 7–13.

[76] G. A. Fink, D. V. Zarzhitsky, T. E. Carroll, and E. D. Farquhar, "Security and Privacy Grand Challenges for the Internet of Things," *2015 Int. Conf. Collab. Technol. Syst.*, vol. 9, pp. 27–34, 2015.

[77] Z. A. Hussien *et al.*, "Secure and Efficient E-health Scheme Based on the Internet of Things," in *2016 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, 2016.

[78] P. E. Idoga, M. Agoyi, E. Y. Coker-Farrell, and O. L. Ekeoma, "Review of Security Issues in E-healthcare and Solutions," *HONET-ICT, 2016*, pp. 97–100, 2016.

[79] J.-J. Huang, W.-S. Juang, C.-I. Fan, Y.-F. Tseng, and H. Kikuchi, "Lightweight Authentication Scheme with Dynamic Group Members in IoT Environments," *Proc. 13th Int. Conf. Mob. Ubiquitous Syst. Comput. Netw. Serv. - MOBIQUITOUS 2016*, pp. 88–93, 2016.

[80] M. Kamalrudin, J. Hosking, and J. Grundy, "Improving Requirements Quality using Essential Use Case Interaction Patterns," in *33rd International Conference of Software Engineering (ICSE), 2011*, 2011, pp. 531–540.

[81] H. Hibshi, T. D. Breaux, and S. B. Broomell, "Assessment of risk perception in security requirements composition," *23rd IEEE Int. Conf. Requir. Eng. (RE), 2015*, pp. 146–155, 2015.

[82] M. Mumtaz, S. Muftic, and N. Abdullah, "Strong Authentication Protocol based on Java Crypto Chip as a Secure Element," *J. Adv. Sci. Technol. Eng. Syst.*, vol. 1, no. 5, pp. 21–26, 2016.

[83] T. Islam and S. C. Mukhopadhyay, "Smart Sensors and Internet of Things : A Postgraduate paper," *IEEE Sens. J.*, pp. 1–8, 2016.

[84] R.-M. Abraham, P. J. Escamilla-Ambrosio, J. Happa, and E. Ahuirre-Anaya, "GARMDROID : IoT Potential Security Threats Analysis Through the Inference of Android Applications Hardware Features Requirements," *Appl. Futur. Internet*, vol. 2, pp. 63–74, 2017.

[85] Y. Maleh, A. Ezzati, and M. Belaissaoui, "An enhanced DTLS protocol for Internet of Things applications," *2016 Int. Conf. Wirel. Networks Mob. Commun.*, pp. 168–173, 2016.

[86] Y. F. Wang, W. M. Lin, T. Zhang, and Y. Y. Ma, "Research on Application and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Security Protection of Internet of Things in Smart Grid," in *IET International Conference on Information Science and Control Engineering 2012 (ICISCE 2012)*, 2012, no. 1.

[87] V. Kowkutla and S. Ravi, "Security Standards for Embedded Devices and Systems," in *Fundamentals of IP and SoC Security*, 2017, pp. 295–311.

[88] J. Muvuna, T. Boutaleb, S. B. Mickovski, and K. J. Baker, "Systems Engineering Approach to Design and Modelling of Smart Cities," in *International Conference for Students on Applied Engineering (ICSAE) 2016*, 2016.

[89] H. Gabriel, C. Ferreira, R. Timoteo, and D. S. Junior, "Security Analysis of a Proposed Internet of Things Middleware," *Cluster Comput.*, 2017.

[90] V. Kamalakannan and S. Tamilselvan, "Design of Secure and Intelligent Architecture for Security in Perceptual Layer and Interney of Things," *Indian J. Sci. Technol.*, vol. 3, no. 12, pp. 1040–1043, 2016.

[91] R. Ribeiro, A. Santin, V. Abreu, J. Marynowski, and E. Viegas, "Providing Security and Privacy in Smart House Through Mobile Cloud Computing," in *2016 8th Latin-American Conference on Communication (LATINCOM)*, 2016, pp. 1–6.

[92] K. Reddy, R. Khaladkar, A. Khedekar, P. Khare, and M. Rajput, "Building Smart Cities Based on Web Architecture and using IoT," *Imp. J. Interdiscip. Reserach*, vol. 3, no. 1, pp. 1075–1076, 2017.

[93] V. Kamalakannan and S. Tamilselvan, "Design of Secured and Intelligent Architecture for Security in Perceptual Layer of the Internet of Things," *Indian J. Sci. Technol.*, vol. 10, no. January, pp. 1–9, 2017.

[94] K. Kishore and S. Sharma, "Evolution of Wireless Sensor Networks as the framework of Internet of Things- A Review," *Int. J. Emerg. Res. Manag. &Technology*, vol. 5, no. 12, pp. 49–52, 2016.

[95] P. K. Dhillon and S. Kalra, "A Lightweight Biometrics Based Remote User Authentication Scheme for IoT Services," *J. Inf. Secur. Appl.*, vol. 0, pp. 1–16, 2017.

[96] J. Oltsik, "The Internet of Things: A CISO and Network Security Perspective," 2014.

[97] H. David and G. Sarah, "Lack of security in Internet of Things devices," *Network Security*, vol. 2014, no. 8, p. 2, 2014.

[98] K. Dhariwal and A. Mehta, "Architecture and Plan of Smart hospital based on Internet of Things (IoT)," *Int. Res. J. Eng. Technol.*, vol. 4, no. 4, pp. 1976–1980, 2017.

[99] M. Selinger, A. Sepulveda, and J. Buchan, "Education and the Internet of Everything," 2013.

[100] B. Russell, C. Garlati, and D. Lingenfelter, "Security Guidance for Early Adopters of the Internet of Things (IoT)," *Mob. Work. Gr. Peer Rev. Doc.*, no. April, 2015.

[101] K. Rose, S. Eldridge, and L. Chapin, "The Internet of Things : An Overview," 2015.

[102] S. Peter and R. K.Gopal, "Multi-level Authentication System for Smart Home Security Analysis and Implementation," in *International Conference on Inventive Computation Technologies (ICICT)*, 2016.

[103] A. Ukil, J. Sen, and S. KOlaikonda, "Embedded Security for the Internet of Things," *M2 Press.*, 2015.

[104] F. Mattern and C. Floerkemeier, "From the Internet of Computers to The Internet of Things," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6462 LNCS, pp. 242–259, 2010.

[105] C. Tankard, "The Security Issues of The Internet of Things," *Comput. Fraud Secur.*, vol. 2015, no. 9, pp. 11–14, 2015.

[106] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswani, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Futur. Gener. Comput. Syst.*, no. 1, pp. 1–19, 2013.

[107] Z. Liu, X. Huang, Z. Hu, M. K. Khan, H. Seo, and L. Zhou, "On Emerging Family of Elliptic Curves to Secure Internet of Things : ECC Comes of Age," *IEEE Trans. Dependable Secur. Comput.*, vol. XX, no. XX, pp. 1–12, 2016.

[108] P. K. Das, S. Narayanan, and N. K. Sharma, "Context-Sensitive Policy Based Security in Internet of Things," 2016.

[109] J. Nolin and N. Olson, "The Internet of Things and Convenience," *Internet Res.*, vol. 26, no. 2, pp. 360–376, 2016.

[110] D. Thatmann, S. Zickau, F. Alexander, and K. Axel, "Applying Attribute-based Encryption on Publish Subscribe Messaging Patterns for the Internet of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Things," *2015 IEEE Int. Conf. Data Sci. Data Intensive Syst.*, pp. 556–563, 2015.

[111] D. H. Summerville, K. M. Zach, and Y. Chen, "Ultra-Lightweight Deep Packet Anomaly Detection for Internet of Things Devices," in *Computing and Communications Conference (IPCCC), 2015 IEEE 34th International Performance*, 2015.

[112] E. Vasilomanolakis, "On the Security and Privacy of Internet of Things Architectures and Systems," in *2015 International Workshop on Secure Internet of Things (SIoT)*, 2015, pp. 49–57.

[113] I. Bouij-pasquier, A. Abou El Kalam, A. Ait Ouhman, and M. Ouabiba de Montront, "SmartOrBAC Security and Privacy in The Internet of Things," in *2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA)*, 2015.

[114] H. Boujezza, M. Al-mufti, H. Kaffel, B. Ayed, and L. Saidane, "A Taxonomy Of Identities Management Systems In lOT," in *2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA)*, 2015.

[115] K. Dempsey, R. Ross, and K. Stine, "Supplemental Guidance on Ongoing Authorization," 2014.