Security in the internet of Things: a systematic Mapping Study

Omer aziz[1], Naveed akhter[2], Naeem aslam[2]

[1]School of System and Technology, UMT
[2]NFC Institute of Engineering and Technology, Multan 60000, Pakistan

Abstract The extension of gadgets has accelerated touchy statistics trade on the Internet the usage of most of the time unsecured channels. Since a large use of RFID (Radio-frequency Identification) tags in the transportation and development industries from 1980 to 1990, with the multiplied use of the Internet with 2G/3G or 4G when you consider that 2000, we are witnessing a new generation of related objects. A massive wide variety of heterogeneous sensors may also accumulate and dispatch touchy facts from an endpoint to a global community on the Internet. Privacy worries in Iot stay essential problems in the research. This paper aims to understand and additionally grant continuing doe's research topic, challenge, and Future Direction related to Iot security. "A systematic mapping finds out about (SMS) is thus utilized on the way to organize the chosen Articles into the following classification: contribution type, Type of Research, Iot Security, and their approach. We take out an overall of twenty-four Articles in support of this systematic discover out about also they categorize the following described criterion. The findings of this SMS are mentioned and the researcher was once given hints on the possible route for future research.

Keywords: Systematic Mapping Study (SMS), Internet of Things (IOT), Classification

I. INTRODUCTION

The rate of partner material contraptions in the region of us to the Internet is extending quickly. As proven by way of a progressing Gartner statement, existing will exist about8.4 billion associated factors international in 2020. This variety is structured to create to20.4 billion by using 2022 [1]. The utilization of the internet of things functions is developing inside all bit of the earth. The noteworthy riding nations inside the fuse Western and Europe, and North America, and China [1]. The quantity of computer to desktop (M2M) affiliations depended upon creating beginning 5.6 billion every 2016 to 27 billion out of 2024 [1]. This jump in numbers itself pronounces Iot to be one of the most important predicted markets that ought to shape an institution of the broadening mechanized economy The Iot commercial enterprise is dependent upon to create similarly as earnings from $892 billion every 2018 to $4 trillion through 2025 [2].

M2Maffiliations unfold a broad extent of makes use of like sharp city networks brilliant condition, smart systems, sharp retail, canny developing, and many others [3]. Figure 1indicates the past, current, and future graph of IOT.

IOT is perhaps the great driver of the extraordinary most impressive features of development, for instance, 5G [3]. 5G and Iot are finally, after right around three decades, making the unrivalled imaginative and quick of EngravingWeiser a reality. The Worldwide Principles Activity characterizes [5] the Iot as "a world framework for the facts society.Empowering most recommended choices with the information of way of interconnecting completely on current and Evolving interoperable data and Discussion Innovations".

This restricts however the regular Web "things, for example, laptop and PC, the Iot definition consists of components, for example, vehicles, attire, and even structures. By interfacing every one of these devices8quintessential for constant presence to the Web, new protection troubles emerge.

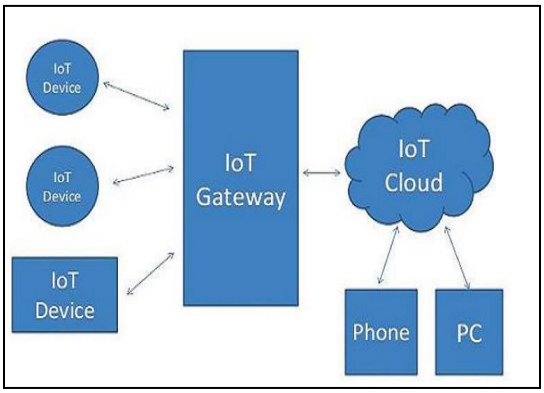


FIGURE 1. IOT Architecture

Network Layer: discover, connect, as well as Translate Device, ended a network.
Perception Layer: sensors, actuators, and devices interact with the environment.
Application Layer: information processing and storage space with specialized examine and functionality For Users.

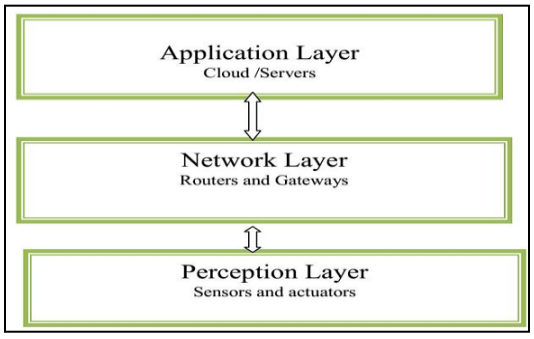


FIGURE 2. IOT Layer

IOT Security Objective:

Our objective is to measure however, privacy and security are managed in the completely different context of using IOT, such as IOT application, Iot survey paper, and foggy environments. We tend to target analysis to research and to map research studies that contain security and privacy considerations in the use of classification criteria. Therefore, we tend to conduct a scientific mapping study to assess knowledge security strategies and the technique of preserving privacy in the field of analysis. We tend to target joint analysis to study research contributions and trends in IOT edge, Iot cloud, and fog environments

IOT security Scope:

a) Data mixing, cloud security auditing, responsibility for composite services, and therefore the impact of cloud decentralization remain areas that require a lot of analysis to provide a more secure Iot.

b) Privacy inside the IOT is of is the majority significant as the plans use generally bringing together non-public private information, such as healthiness information. A large amount has been complete to protect users‘ private information, such as information.

c) In adding together, important work has been done to get used to present the protocol to IOT function or generate entirely original ones for brightness cryptography and protected set of connections broadcast.

Research objective

Our chosen study objective is using systematic mapping study to identify the existing research-approach and future –approach and another is type of research and trend also identify the field of publication year and publication channel.

Proposed system

II. Literature Review

SLR in smart Farming:

Systematic literature Review the developing interest for food as far as feature and amount contain expanded the requirements designed for industrialization and escalation in the farming field. Internet of Things (Iot) is an extremely talented science
with the aim of is given that many modern options to update Research establishments and scientific businesses are consistently working to supply options and products using
Iot to tackle distinctive domains of agriculture. This paper affords a systematic literature review (SLR) by way of surveying Iot applied sciences and their cutting-edge utilization
in different application domains of the agriculture sector. The underlying SLR has been compiled via reviewing research articles posted in well-reputed venues between 2006
and 2019. A whole of sixty-seven papers was carefully chosen thru a systematic method and labeled accordingly. The most important aim of this SMS is the series of all applicable lookup on Iot farming applications, sensors/devices, verbal exchange protocol, and community sorts.

SLR in smart Healthcare:

[32][33] The Internet of Things (Iot) is a system that integrates bodily things, software programs, as well as hardware en route for engage with every other. The aging of the population, scarcity of healthcare resources, and rising scientific expenses make Iot based applied sciences fundamental to be tailor-made to tackle these challenges in healthcare. This systematic literature evaluation has been carried out to decide the primary utility location of Iot in healthcare, aspects of Iot structure in healthcare, most essential applied sciences in Iot, traits of cloud-based architecture protection, and interoperability problems in Iot structure and effects, and challenges of Iot in healthcare. Sixty applicable papers, posted between 2000 and 2016, have been reviewed and analysed.
This evaluation printed that domestic healthcare providers used to be one of the major software areas of Iot in healthcare. Cloud-based architecture, with the aid of presenting first-rate flexibility and scalability, has been deployed in most of their viewed studies.

Communication applied sciences inclusive of Wi-Fi constancy (Wi-Fi), Bluetooth, radio-frequency identification (RFID), and Low-Power Wireless Personal Area Networks (Low PAN) had been often used in exclusive Iot models. The research involving the safety and interoperability troubles in Iot structure in fitness is nonetheless low in number. With appreciate to the most essential consequences of Iot in healthcare, this covered capacity of records exchange, reducing continue to be of hospitalization and healthcare costs. The essential challenge of Iot in healthcare had been safety and privateers difficulty.

Security in the internet of things: A systematic Mapping system

Our contribution is that a systematic mapping study in iot security. This paper aims to understand and additionally grant continuing research topic, challenge, and Future Direction related to Iot security. A systematic mapping finds out about (SMS) is thus utilized on the way to organize the chosen Articles into the following classification: contribution type, Type of Research, Iot Security, and their approach. We take out an overall of twenty-four Articles in support of this systematic discover out about also they
categorize the following described criterion. The findings of this SMS are mentioned and the researcher was once given hints on the possible route for future research.

III. RESEARCH METHODOLOGY

Systematic Mapping Study:

There are two main approaches to conduct literature reviews that are "SM S" and"SLR". If the researcher aims to identify, classify, and evaluate results to respond to a specific research question "Systematic Literature Reviews" is the adequate approach but if he seeks to answer multiples research questions "Systematic Mapping Study" is the best one. In this paper, we have conducted the formal guidelines of Systematic Mapping Study from Petersen et al. [5] performed in five steps. The outcome from each step gives the input for the next step. SMS starts with the initial research questions built up to provide a general scope for the study used to find out research papers (step 2) from the selected digital libraries (according to the research fields).In the next step, the screening process starts with a set of inclusion and exclusion Criteria to select relevant papers (step 3). Finally, the key wording process (step 4) enables classification and data extraction (step 5) which would have to answer the research questions.

A. RESEARCH OBJECTIVES

Our chosen study objective is using systematic mapping study to identify the existing research-approach and future –approach and another is type of research and trend also identify the field of publication year and publication channel.

B. Define the Research Question

The general purpose of the research question in our learning is to better understand the solution calculated to solve the Iot protection struggle, such as the problems are identified. For a detailed overview of this subject, the methodical plan study deal with six investigates question (RQ). Table 1are presents the six QRs with their matching motivation. These question motivations allow us to categorize present research at Iot Security and recognize future research plans in the field. Designed for this learns some lookup queries used to be asked, and multiple assessments reviewed. The study strives to reply to numerous queries that lead to higher thoughtful ideas of lookup and future directions. Mainly, the learn about tries to reply to the subsequent questions.

C. Search Scheme/conduct a research

a. Conduct all research papers.
b. Select the most related paper.
c. Search for the primary study
d. Use research string in scientific Dataset/Database.
e. We check the keyword, title, abstracts field within the database

D. *SEARCH STRATEGY*

According to our research questions, we have built up our Search Strings formulated using general terms with AND clause as "IOT AND (security and privacy)". We adopted the use of Boolean operators such as "AND" to focus our search only on specific subjects. Therefore, we have restricted our search items to select from digital libraries only scientific papers, with as the specified keywords related to security and privacy in IOT.

Table 1: Research Question and Motivation

No.	Research Question	Motivation
RQ#1	Which Publication channel is in IOT Research?	To classify the search best publication sources can be used.
RQ#2	Which Type of Search in IOT Application?	To classify type of Search in IOT
RQ#3	What type of Security and privacy issue in IOT	Find out the overview of studies on security and confidentially at IOT
RQ#4	How to improve IOT Security?	Which define Improvement technique.

Table 2a: Search String used in Scientific Libraries

Data Base Name	Search Strings
Google Scholar	Both 2&3
IEEE	Both 3&5
ACM Digital Library	Both 2&4
Science Direct	Both 3&4
Springer Link	Both1 &3
DBLP	Both 1&4

Table 2b: Inclusion and Exclusion Criteria used in selected article

Inclusion	Exclusion
IC1: Study with title Related to IOT.	**EC1**:Paper in another language than English
IC2: Studies Related to security in IOT.	**EC2:**Paper without Abstract
IC3: Studies Related to protection and confidentiality.	**EC3:**Paper from workshop
IC4: Studies presenting safety and confidentiality	**EC4:**Books
IC5: Studies about security and privacy in IOT cloud environments	**EC5:**Studies about another issue in the IOT environment
IC6: Studies about safety and confidentiality in IOT fog environments	**EC6:**Paper out of scope

E. Paper selection criteria

The archives originate via they seem to be for strings had been chosen or eliminate following the name, the précis, and the grasp of the whole text. For the period of this collection, the protection of the papers was once additionally taken into account. Also, beautify the dependability of this procedure and limit attainable subjective series threats, this system used to be made via the first and 2nd writer as well as review by the different authors of this learning. Some papers may additionally have was once chose nor eliminate primarily depend on the article title and article abstract. However, studying the complete -textual content used to be required for some articles. To decide if the position applies to the collection. Within this systematic Mapping study, the archives assembly the following paper has been elected.

1) Documents that deal with the privatives and protection thing of Iot safety answer in typical terms.
2) Articles' focal point on a unique function of Iot security.
3) Industrialized case study, anyplace protection factor are discussed.
4) Approaches for the internet of things application and Security.
5) The full-text collection introduced into the chosen database.
6) Articles on hand with crammed reproduction on-line from 2015 towards 2020 The safety aspect, they reflect on consideration on all issue associated to the reliability, accuracy, the Iot solution, and durability. Documents assembly the following standards had been excluded.

1) Papers now not introduced in English.
2) Documents now not precisely related to the potential of this document.
3) Articles with no entire textual content handy in the chosen one database
4) Books and grey journalism.
5) Documents from the non-peer evaluation sources

F.Quality Assessments

Feature evaluation is usually approved out in a methodical review of the creative writing and also less in methodical map study. On the other hand, to improve or learn, literature of questionnaires was also planned to access the excellence of the selected work.

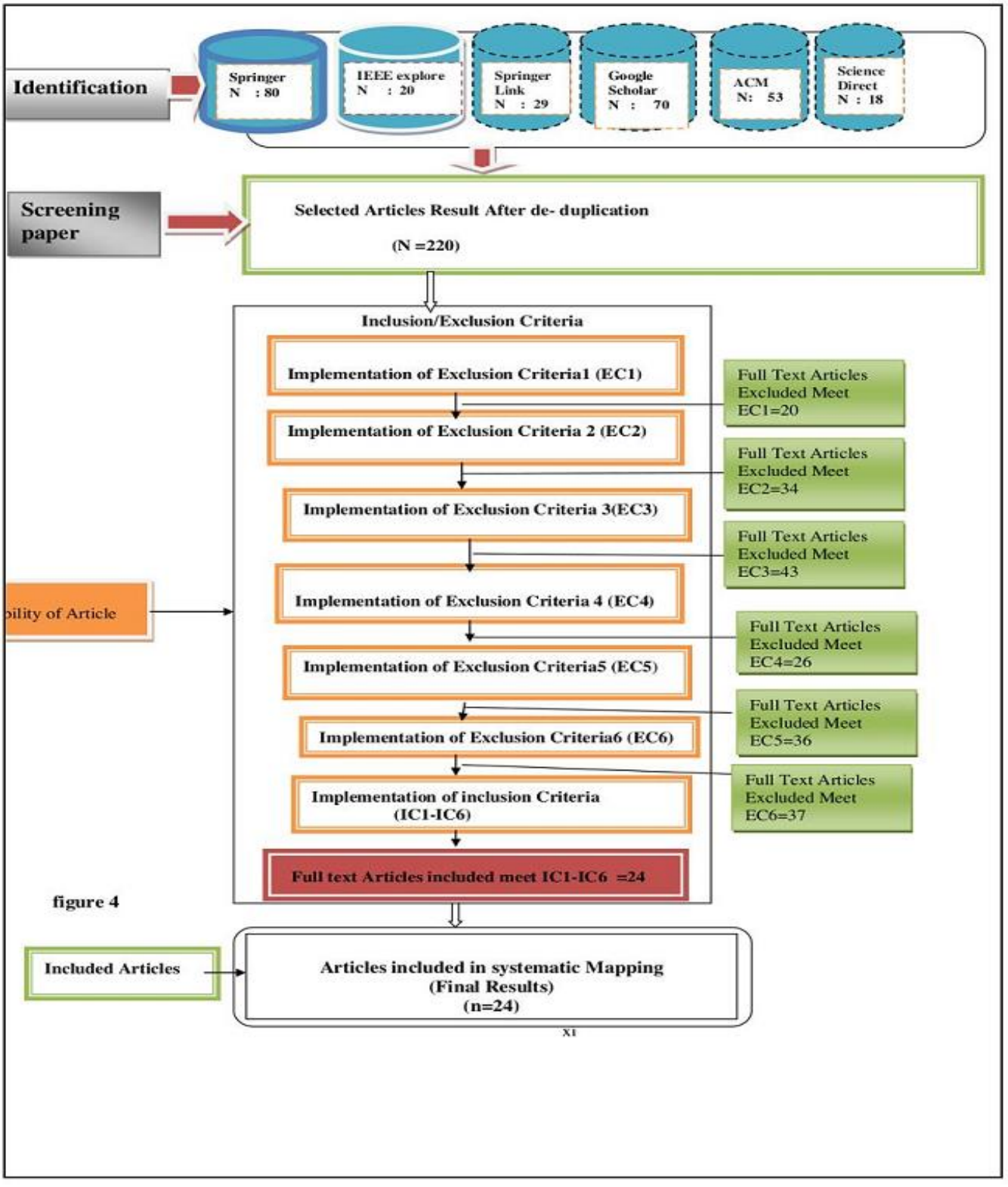
The study contributes to the security of the IOT. Possible responses were "of course yes (1) and negative not found No (0) moderates (0.5) The research currently an understandable clarification of the safety problem of the IOT.

The plausible reply was once "yes (1)" incompletely (0.5), "no (0)"

The research affords experimental results. Manageable responses had been "yes ((1)" and "no (0)" question was related to the classification of the CORE conference on IT
(A, B, C).

For surveys, conferences, and workshops Ranking

(1.5) condition CORE has classified,
Condition CORE B is classified.
0.5 (0.5) if CORE C is evaluated.
If it is not part of the CORE classification.



• **FIGURE 3 EXLUSION /EXCLUSION CRETRIA**

G. Data Extraction

At this phase of the study, we extract information as of the chosen set of journal papers. This step expected in the direction of plan and classify documents to allow us to manage the QR address inside Section III-A. In support of an enhanced group and a methodical run of work, we produced a worksheet pattern (see table III) also with all the important information on all things. The sheet is a complete page through additional features than what has been initially presented by [2], [6], and [3].

Table 3: Data Extraction Template

information point	Value
learn identification	Digit
Paper Name	given name of the Paper
writer Name	Given name of Authors
Year of Publication	Calendar year
Venue	Name of Publication venue
State	Name of the country each author participate
Area of Research	Knowledge Area of Research
Research Topic	Main topic
Research problem	The research problem addressed by the study
Proposal	Proposal solution to the problem
Contribution	The main contribution of the problem
Evaluation Process	Benchmark adopted for evaluation
Case Study	Which case study used?

.

Results

This section describes the outcome associated with the device. Map the questions supplied in table 1. A few studies had been selected to illustrate examples of the consequences of every RQs Results. We suppose that they are related and create an important contribution to IOT security.

Selection Results

.

A total of 220 articles tested in-depth, 196 articles have been thrown away and Twenty – Four were subsequently decided on. The twenty -four gadgets diagnosed were analyzed to answer are explain on top of table 2 gives the list of those selected. Documents with information about the outcomes of the overall category and your satisfactory control classification result from their RQ.

Classification

a. Apply on Primary Research paper
b. Publication Year
c. Publication Channel
d. Research type
e. Quality Assessment
f. A total score of each Paper
g. Research topic

RQ 1: Which Publication channel is fundamental in Iot Research?

Publication channel found in Systematic mapping study
Conference (8)(0.78)
Journal (9)(0.98)
Workshop (4)(0.48)
Case study (3)(0.34)

RQ2: what are the Research Type in IOT?

In systematic mapping study (SMS) identifying six types of Research
a. Proposal study (4)(0.45)
b. Comparative study (5)(0.58)
c. Implementation & Evaluation- Research
d. Experimental-Research (5)(0.68)
e. Conceptual-research (4)(0.48)
f. Analytical Research -study (5)(0.59)

Table 4: Classification Table selected Articles

Reference	Paper. Year	Paper Channel	Study Type	Research Topic	Application	Approaches	QualitAssessment	Score
[12]	2019	Conference	Solution proposal	Design and Implement Iot open source	Iot open Source	Framework	**1.5 1 0**	2.5
[8]	2017	Workshop	Experimental research	Security and Privacy Iot smart Home	Iot smart Home	Method	**1 0.5 0**	1.5
[18]	2019	Journal	Analytical Study	Test event Generation Iot for Fall Detection Iot system	Iot event Detection	Method	**1 1.5 0**	2.5
[20]	2013	Case Study	Comparative-Study	Iot in Mobile	Iot Mobile	Guideline	**1 1 1**	3
[14]	2019	Conference	comparative -study	Iot Based Efficiency Management	Iot smart app	Method	**1 0.5 1**	2.5
[9]	2018	Journal	Experimental research	Implementation and Evaluation Iot in smart home	Smart home	Method	**1 0 0.5**	1.5

Reference	Paper. Year	Paper .Channel	Study Type	Research Topic	Application	Approaches	Quality Assessment	Score
							A B C	
[11]	2018	conference	Research Proposal	Iot based E-Business &Retail IoT	E-business	Architecture	**0 1 1**	**2**
[21]	2017	Case study	Experimental research	conceptual study Iot Interconnecting Education	Iot Education	Model	**0.5 0 0.5**	**1**
[15]	2018	conference	comparative Study	securing the IOT	IOT Security	Architecture	**1 1 1**	**3**
[22]	2014	Workshop	research Proposal	Internet of thing Development	Iot open sources	Architecture	**0 0.5 1**	**1.5**
[5]	2016	Journal	Analytical Study	internet of thing in smart farming	Iot smart farming	Architecture	**1 0.5 1**	**2.5**
[10]	2018	Journal	Experimental research	Implementation and Evaluation Iot in smart home	Smart home	Method	**0.5 1 0**	**1.5**
[13]	2018	conference	Conceptual-Research	internet of thing challenge and solution	Iot security open sources	Guideline	**1 1 0.5**	**2.5**
[19]	**2013**	Case study	Analytical-Survey	internet of thing in industry		Method	**1 0 1**	**2**
[16]	2017	Journal	Experimental-Study	practical perspective Iot in 5G	iot 5G	Framework	**1 1 0.5**	**2.5**

Reference	Paper. Year	Paper .Channel	Study Type	Research Topic	Application	Approaches	Quality Assessment	Score
							A B C	
[2]	2014	conference	Research Proposal	Iot challenges in smart Grid	Iot smart Grid	Framework	**1 0.5 1**	**2.5**
[32]	2017	Journal	Experimental research	Iot in Digital Health	Iot Health	Model	**0.5 1 1**	**2.5**
[15]	2013	conference	comparative Study	Challenges In Industrial internet using IOT	Industrial IOT	Architecture	**0.5 0.5 1**	**2**
[23]	2014	Workshop	research Proposal	Iot architecture for connected Cars	Iot open sources	Architecture	**0.5 1 1**	**2.5**
[28]	2016	Journal	Analytical Study	Iot using in wearable Devices	Iot devices	Model	**1 1 1**	**3**
[6]	2018	Journal	Comparative study	Challenges in smart farming	Smart farming	Method	**0.5 1 0**	**1.5**
[27]	2017	conference	Conceptual-Research	internet of thing challenge and solution	Iot security open sources	Guideline	**0.5 1 1**	**2.5**
[23]	2015	Workshop	Analytical-Survey	Survey internet of thing in industry	Industrial survey	Guideline	**0.5 0 1**	**1.5**
[24]	2019	Journal	Implementation and Evaluation Research	Security in IOT	Iot security	Framework	**1 0.5 1**	**2.5**

Table 5: Quality Assessment selected Articles

Reference	Total Score	No
[8][22][9][10][6][23]	1.5	6
[24][27][23][32][2][12][18][14] [5][13][16]	2.5	11
[28][15][20][21][3][25][4]	3	7

V. DISCUSSION

The most frequent is privateness concern, recognition, verification, and authorization issues, and requirements of administration (e.g. application). Confidentiality on the internet of things is of extreme significance; due to the fact, the units use to acquire personal and private information, such as fitness Data a great deal has been accomplished to shield users' exclusive information, as private as well as bodily data(i.e. a authenticate with statistics that a consumer remember, p. a password), ii) the customers themselves knowledge-based authentication with clever in performance cards or get admission to in performance cards and iii) bodily traits [18]. Based on the find out about these results, the most lacking component of Iot protection it is presently authentication and authorization.

VI. CONCLUSION

The article introduced an SMS to learn about summarizing the current lookup in IOT. Out of 265 studies, 220 works have been recognized between 2011 and 2020 out of Twenty-four which had been chosen and labelled following 5 criteria: kind of research, empirical type, kind of approach, pastime and find out about plans for the iot. Sour publication trends have additionally been identified. Results bought confirmed that growing interest used to be paid to the protection of IOT 2017. About half of the articles chosen seemed in workshops, and solely a small number of articles had reached the maturity of a journal publication.

RQ3: What kind of security issue in Iot?

Safety problems that you have raised through the lookup neighbourhood in the latest years and how they had been classified. Primary research I had 9 classes of concerns. For this SMS, they have been then categorized into 4 first-rate subgroups recognize the problem (Key factors – Environment restrictions, susceptible devices, information privacy; Functional restrictions: enforcement mechanisms, Dependencies between devices, identification, Authentication, and authorization; Control.

I) Environments Constraint:
ii) Data privacy
iii) Sources of threats
iv) Identification, authentication, and authorization:
V) Attacker Model
vi) Legislative issue
vii) vulnerable devices
Viiii) Cross-device dependencies

VII. FUTURE DIRECTION

Our future work will be to entire this work by using writing a survey to examine as an lot as feasible options to assurance and keep confidentiality in the Iot environment. Finally, the more than one Iot assault vectors are disturbing. Besides the cutting-edge Internet threats, several new vectors have been introduced. Opening and the community environment of a lot of Iot structures make them especially susceptible to hateful attacks. This is accentuated by way of frequently negative protection deployed on the gadgets themselves. Communication via radio waves is in all likelihood of many sorts of attacks, from spying to direct Do's attacks. Lack of implementation of the techniques makes it even greater severe, developing extra strain to make structures as fault-tolerant as possible. If protection stays a serious hassle in Iot should probably stop the adoption of science via cease customers and consequently gradual the floor development. Also, look up and evaluate efforts are wanted to assist system manufacturers, regulators, and performers to prioritize efforts whilst enhance Iot safety strategies By identifying, inspecting, and classifying the publications, we have carried out a systematic mapping find out about for thematic analysis, tendencies, and future work on protection and confidentiality at IOTambient. 220 publications had been selected, solely fifty-four types of research had been deemed relevant according to the inclusion-exclusion standards that we define. to check present-day contributions tolookup and your future trends.

References

[1] Stankovic, John A. "Research directions for the internet of things." IEEE Internet of ThingsJournal 1.1 (2014): 3-9.7.

[2] Atzori, Luigi, Antonio Iera, and GiacomoMorabito. "The internet of things: A survey." Computernetworks 54.15 (2010): 2787-2805.

[3] S. Latre, P. Leroux, T. Coenen, B. Braem, P. Ballon, and P. Demeester,´ "City of things: Anintegrated and multi-technology testbed for iot smart city experiments," in *IEEE ISC2 2016*. IEEE, 2016, pp. 1 –8.

[4] Z. K. Aldein Mohammeda and E. S. Ali Ahmed, ―Internet of Things Applications, Challenges
and Related Future Technologies,‖ no. February, 2017.

[5] A. Whitmore, A. Agarwal, and L. Da Xu, ―The Internet of Things—A survey of topics and trends,‖ Inf. Syst. Front., vol. 17, no. 2, pp. 261 – 274, 2015.

[6] B. L. R. Stojkoska and K. V Trivodaliev, ―A review of Internet of Things for smart home:Challenges and solutions,‖ J. Clean. Prod., vol. 140, pp. 1454–1464, 2017..

[7] R. Davies, ―The Internet of Things opportunities and challenges,‖ Eur. Parliam. Res. Serv.,2015.

[8] M. Wu, T. J. Lu, F. Y. Ling, J. Sun, and H. Y. Du, ―Research on the architecture of Internet ofThings,‖ ICACTE 2010 - 20114 3rd Int. Conf. Adv. Comput. Theory Eng. Proc., vol. 5, pp. 484–487,2010

. [9] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Cla, ―Middleware for internet of things: A survey,‖ IEEE Internet Things J., vol. 3, no. 1, pp. 70–95, 2016.

.[10] M. Ammar, G. Russello, and B. Crispo, ―Internet of Things: A survey on the security of IoTframeworks,‖ J. Inf. Secur. Appl., vol. 38, pp. 8–27, 2018. 61

[11] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, ―Internet of Things security andforensics: Challenges and opportunities,‖ Futur. Gener. Comput. Syst., vol. 78, pp. 544–546, 2018.

[12] B. Xu, L. Da Xu, H. Cai, C. Xie, … J. H.-I. T. on, and U. 2014, Ubiquitous data accessing method in IoT-based information system for emergency medical services,‖ ieeexplore.ieee.org,2014..

[13] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, ―Future internet: The internet of things architecture, possible applications and key challenges,‖ Proc. - 10th Int. Conf. Front. Inf. Technol. FIT 2012, pp. 257–260, 2012.

[14] A Zanella, N. Bui, a Castellani, L. Vangelista, and M. Zorzi, ―Internet of Things for SmartCities,‖ IEEE Internet Things J., vol. 1, no. 1, pp. 22–32, 2014

[15] B. L. R. Stojkoska and K. V Trivodaliev, ―A review of Internet of Things for smart home: Challenges and solutions,‖ J. Clean. Prod., vol. 140, pp. 1454–1464, 2017.

[16] A. Al-Fuqaha et al., ―Internet of Things: A Survey on Enabling Technologies, Protocols, andApplications,‖ vol. 17, no. 4, 2015.

[17] M. Wu, T. J. Lu, F. Y. Ling, J. Sun, and H. Y. Du, ―Research on the architecture of Internet of Things,‖ ICACTE 2010 - 2010 3rd Int. Conf. Adv. Comput. Theory Eng. Proc., vol. 5, pp. 484–487, 20114

[18] V. Adat and B. B. Gupta, ―Security in Internet of Things: issues, challenges, taxonomy, andarchitecture,‖ Telecommun. Syst., vol. 67, no. 3, pp. 423–441, 201 8.

[19] P. Fremantle, ―A reference architecture for the internet of things,‖ vol. 0, p. 21, 2015.

[20] D. He, R. Ye, S. Chan, M. Guizani, and Y. Xu, ―Privacy in the Internet of Things for Smart Healthcare,‖ IEEE Commun. Mag., vol. 56, no. 4, pp. 38–44, 2018

[21] I. Yaqoob et al., ―Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges,‖ IEEE Wirel. Commun., vol. 24, no. 3, pp. 10–16, 2017.

[22] A. L. Chan, G. G. Chua, D. Z. L. Chua, S. Guo, P. M. C. Lim, M. Mak,and W. S. Ng, "Practical experience with smart cities platform design," in *4th IEEE WF-IoT 2018*. IEEE, 2018, pp. 470–475.

[23] L Calderoni, D. Maio, and S. Rovis, "Deploying a network of smart cameras for traffic monitoring on a "city kernel"," *Expert Syst. Appl.*,vol. 41, no. 2, pp. 502–507, 2014

[25] A. Zanella, N. Bui, A. P. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smartcities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, 2014

[26]A. Krylovskiy, M. Jahn and E. Patti, "Designing a Smart City Internet of Things Platform withMicroservice Architecture," 3rd Int'l Conf. on Future Internet of Things and Cloud, 2015, pp. 25-30.
doi: 10.1109/FiCloud.2015.55

[27] Khanna, D. (2019). Internet of Things Challenges and Opportunities. "International Journal ForTechnological Research In Engineering"