Journal of Computer Science

Original Research Paper

A Survey of IoT Security Issues - From Past to Future Trends

[1,2]Imran, [1,4]Syed Mubashir Ali, [1,3]Muhammad Mansoor Alam and [1]Mazliham Mohd Su'ud

[1]Malaysian Institute of Information Technology (MIIT), Universiti Kuala Lumpur, Kuala Lumpur 50250, Malaysia
[2]College of Computer Science and Information Systems, Institute of Business Management, Karachi, Pakistan
[3]Riphah International University, Rawalpindi, Pakistan
[4]College of Computing and Information Sciences, Karachi Institute of Economics and Technology, Karachi, Pakistan

Article history
Received: 18-03-2021
Revised: 26-04-2021
Accepted:03-05-2021

Corresponding Author:
Mazliham Mohd Su'ud,
Malaysian Institute of
Information Technology
(MIIT), Universiti Kuala
Lumpur, Kuala Lumpur 50250,
Malaysia
Email: mazliham@unikl.edu.my

Abstract: This study will focus on Internet of Things (IoT) based security issues. IoT is persuasive in nature and accomplish user's requirement through the intelligent gadgets like sensors, actuators and physical computation devices. IoT is not just about interconnecting embedded devices or gadgets to the Internet, it is about lifestyle. This study aims at identifying existing and future security issues within IoT by performing a comprehensive literature review of peer-reviewed articles from the last 5 years. The review identifies the IoT privacy and security issues from a different perspective and highlights which security issues have been discussed most by the researchers in past and present as well as highlighting future security issues within IoT. The outcomes are presented and highlighted through graphical representation. In the past, confidentiality, integrity and inter-operability and in present, authenticity, data privacy and security issues have been most widely discussed. In future, integrity, confidentiality and authenticity issues will have more significance and need to be addressed in order to successfully implement and achieve benefits from IoT.

Keywords: Confidentiality, Integrity, Authenticity, Authorization, Data Security Privacy, Availability, Non-Repudiation, Access Control, Inter-Operability

Introduction

Internet has revolutionized the way we live. It is being improving our standard of living by leaps and bounds. Nowadays, internet is imperative for performing our day to day activities. According to Figure 1 (Farooq *et al*., 2015), it is predicted that by 2020, there would be more than 50 billion devices connected to the internet. Due to the widespread use of internet, IoT has gained a lot of importance by both the practitioners and academicians. There has been an increase in the trend of IoT adoption by both home users as well as industries and this trend will continue in future (Gaikwad *et al*., 2015). IoT enables two-way communication between humans and computers in different geographical locations through the use of internet. (Hossain *et al*., 2015). The IoT can connect billions of devices at a time without any delay (Alamri *et al*., 2019). Security and privacy issues in IoT are more challenging than in ordinary wireless situations (Conti *et al*., 2018). The major issues of IoT are the message modification and/or alteration, confidentiality, integrity, availability, authenticity and Denial of Service (DoS) etc. (Sfar *et al*., 2018; Wang *et al*., 2018). Security and privacy are one of the most important challenges while sharing critical information within the IoT (Khan and Salah, 2018) (Adat and Gupta, 2018) This study will identify and present various types of security issues in present, past and future (Liu *et al*., 2020a-b). Specifically, this study aims at addressing the following research objectives:

a. To identify potential security issues within IoT
b. To understand which IoT security issues have gained more attention in the literature
c. To identify and highlight the research gap for future researchers in the area of IoT security

To achieve the above mentioned research objectives, this research employs literature review methodology to first identify the security vulnerabilities in IoT. Then further analysis has been done to understand the pattern of how much importance have been given by the researchers to various security issues within IoT. The results are then further analyzed with respect to past, current and future state of least and most addressed security issues within IoT.

© 2021 Imran, Syed Mubashir Ali, Muhammad Mansoor Alam and Mazliham Mohd Su'ud. This open access article is distributed under a Creative Commons Attribution (CC-BY) 4.0 license.

Science Publications

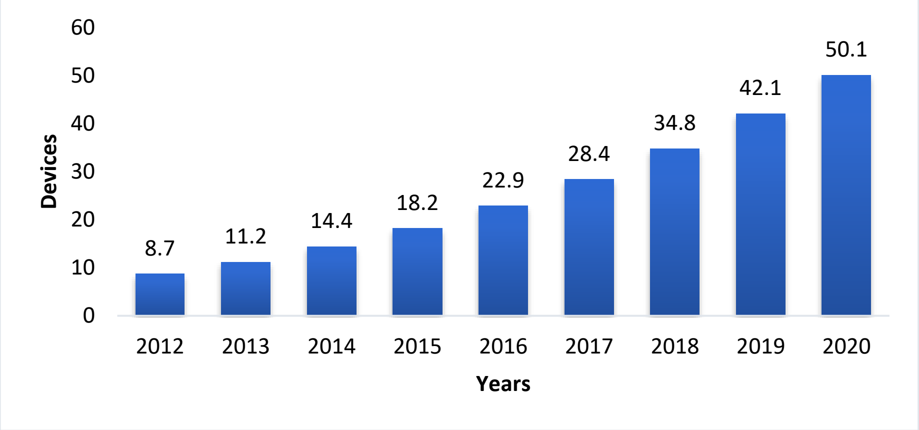

Fig. 1: Predictable perception of smart objects by the year 2020 (Farooq *et al*., 2015)

Research Background

The concept of IoT was first introduced by Kevin Ashton in 1999 (Andrea *et al*., 2015). In the last decade, there has been an increase in the use and adoption IoT by both the home users and industries. (Alsaadi and Tubaishat, 2015). IoT is a set of networking technologies that transforms a regular object into a smart object (Khanna and Kaur, 2019). Wearable devices are also part of IoT applications, such as, pulse screens and smart-watches. Smart IoT has also been termed as Industrial IoT or IIoT when implemented in an industry. Figure 2 depicts an overview of various applications of smart IoT (Sadeeq *et al*., 2018). Network devices within IoT are processing huge amounts of data as they are continuously transmitting and receiving data. This transfer and storage of data within the network are prone to security breach by cybercriminals and hackers for achieving ulterior motives (Sfar *et al*., 2018).

The system attackers can steal sensitive data, for example, area information, credit card numbers, passwords of money related records by hacking into the IoT devices (Amadeo *et al*., 2016). Additionally, smart homes and offices can be monitored and electricity or connectivity can be remotely controlled through IoT by hackers which can be dangerous for the people and their assets in the homes or offices (Almotiri *et al*., 2016). Due to the above mentioned reasons, it is evident that there is great deal of importance of security and privacy issues within IoT.

IoT Security Issues

Confidentiality, Integrity and Availability (CIA) are the main information security issues within any technology (Basu *et al*., 2015) The main security issues within IoT are presented below.

Confidentiality is to protect the sensitive information from being accessed by unauthorized persons (Miloslavskaya and Tolstoy, 2019), (Hameed *et al*., 2019).

Integrity refers to ensuring the authenticity of exchanged information by not allowing anyone to alter or tamper the information (Al-Sharekh and Al-Shqeerat, 2021)

Availability is about making sure the systems/information is available when needed without interruption (Farooq *et al*., 2015).

Authorization is to ensure and verify that the user have the required control permissions or privilege to perform the operation or certain action (Al-Sharekh and Al-Shqeerat, 2021).

Access Control is a security mechanism to handle and grant access rights to only authorized entities (Ali *et al*., 2019).

Authenticity deals with personal information or identification. It includes validating the incoming request against certain identifying credentials (Ali *et al*., 2019).

Non-repudiation is making evidence to prove certain actions in order to ensure that it can't be repudiated later and is achieved by using Digital Signatures and Timestamps (Yaqoob *et al*., 2019).

Inter-operability represents the ability of several systems to connect, exchange and share information with one another, without restrictions ("An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges," 2018). Table 1. IoT Security Vulnerabilities in Each IoT Layer

Security Issues in Each Layer of IoT

IoT has three layers named as perception, network and application layers (Hussain, 2017). Various security issues and challenges have been identified and discussed in the literature which are shown in Table 1 (Mendez Mena *et al*., 2018a).

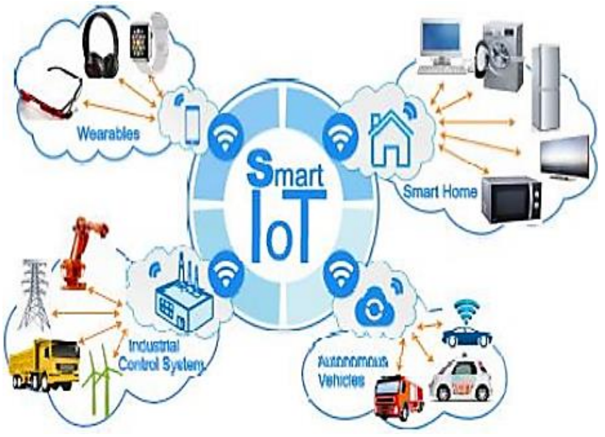

Fig. 2: The smart IoT applications (Sadeeq *et al*., 2018)

Table 1: IoT security vulnerabilities in each IoT layer

Application layer	Data access, authenticity, data protection, data privacy, authorization and availability vulnerabilities
Network layer	DoS, Eavesdropping/Sniffing, Routing Attacks
Perception layer	Node capture, DoS attack, sybil attack

Application Layer

The application layer is liable for conveying application-specific services to the user. It describes various applications of IoT devices such as smart homes, industries and business ("Security and Privacy Grand Challenges for the Internet of Things," 2015) The main security and attack risks on the application layer are data authentication, data privacy, authorization, availability and confidentiality (Sisinni *et al*., 2018).

Network Layer

The network layer is liable for interfacing with other smart things or objects and network gadgets. Its features are also utilized for preparing and transmitting sensor information ("Security and Privacy Grand Challenges for the Internet of Things," 2015) The main security issues in the network layer are DoS, eavesdropping, routing attacks (Chen *et al*., 2018).

Perception Layer

Physical layer consists of sensors for collecting information from the environment. These sensors used some physical parameters to recognize other smart gadgets in the environment (Hussain, 2017). The main security issues in the perception layer are DoS attack, Sybil attack etc. (Sun *et al*., 2018).

Research Methodology

This Section presents the paper that is clear of a detailed inquiry that utilizes precise and the most appropriate method such as the electronics search method, data extraction, eligibility criteria in order to achieve our research objectives. This technique also helps to distinguish, choose and fundamentally evaluate the significant investigate and gather and analyze information from the studies that is remembered for the survey by using PRISMA flowchart (Mendez Mena *et al*., 2018a), (Hassan *et al*., 2020) Figure 3. The following steps are:

a. This literature review is focused on the eligible studies of the different electronics databases and review more than 700 papers and discuss how to filter out the numbers of papers from 2015 to 2020
b. Works on an extensive, reproducible search technique strategies
c. Identifies all relevant studies (both published and unpublished)
d. Evaluates all results for inclusion/exclusion, selection and eligibility criteria and also a balanced summary of findings to complete

Eligible Studies and Criteria

During the literature review, more than 700 research articles are studied from various known research journals by examining and evaluating the different electronic databases related to privacy and security ranging year 2015 to 2020. Most of the papers consist of detailed explicit research which is clear and centered including the method of reasoning for survey having eligibility examine models. The contributions of the qualitative research comparing with upcoming literature (Granjal *et al*., 2015a) in the discussed domain are as follows:

a. Approximate three digits of review papers related to security issues were filtered out because we found one of the major challenges of IoT devices is security
b. This review identifies the IoT limitations with respect to different levels and their security issues
c. During the survey, we gathered information about the different issues of IoT application from the past, present & future perspective
d. This study provides a detailed view of IoT challenges introduced previously and ongoing literature and which is related to the present research work

Search Methods

The distribution of research articles as per the issues concerning to privacy and security in IoT is categorized as past, present and future issues for analytical purposes. The papers reviewed for the issues of the discussed topic chosen as past ranging from January 2015 to December 2017, while for present issues it was considered the range from January 2018 to December 2019 and future issues are considered for the year of 2020 from January to December to explore these issues and challenges in various manner.

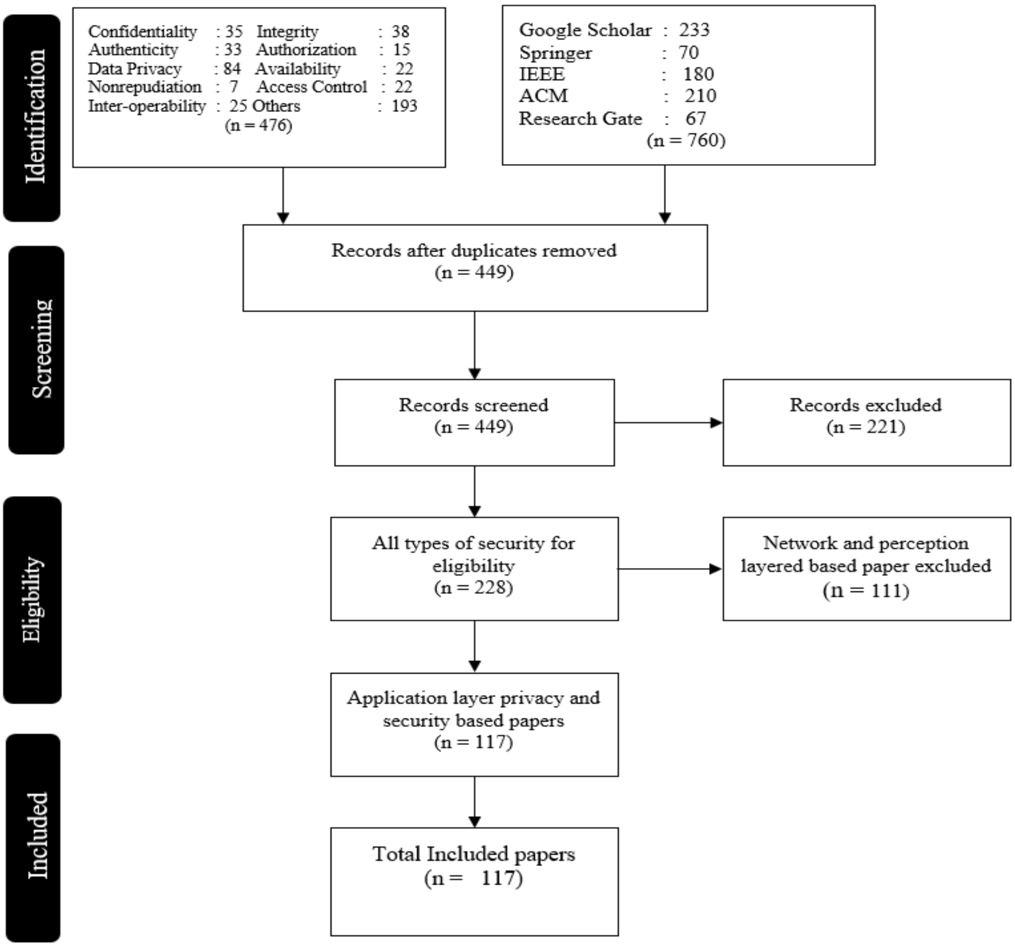
Identification
Confidentiality : 35 Integrity : 38
Authenticity : 33 Authorization : 15
Data Privacy : 84 Availability : 22
Nonrepudiation : 7 Access Control : 22
Inter-operability : 25 Others : 193
(n = 476)
Google Scholar : 233
Springer : 70
IEEE : 180
ACM : 210
Research Gate : 67
(n = 760)
Screening
Records after duplicates removed
(n = 449)
Records screened
(n = 449)
Records excluded
(n = 221)
Eligibility
All types of security for eligibility
(n = 228)
Network and perception layered based paper excluded
(n = 111)
Application layer privacy and security based papers
(n = 117)
Included
Total Included papers
(n = 117)

Fig. 3: PRISMA flowchart of included articles

Electronic Searches

As suggested by (Shafiq *et al*., 2020) and based on our previous experience, this study was accomplished using electronic databases like Google Scholar, Springer, IEEE, ACM and Research Gate containing published articles including many unpublished, on- proceeding drafts as well. This study has also included audit papers through the Google search engine (first 300 papers).

Data Extraction

The factors used to extract this review the author and year of publication, privacy and security, the technique used, methodology and design of the study, which is taken as one complete data set to synthesize the comprehensive report on all parts of the presented survey.

Inclusion and Exclusion Criteria

This study smartly searched 700 research papers out of which 449 papers is removed due to duplication of topic. In the screening, the titles and modified works, a sum of 228 papers or articles were inspected in detail. Out of these, 117 papers or article are related to the application, privacy and security. These included studies were from 2015 to 2020.

Results and Discussion

This Section will analyze and discuss about the results to our research objectives after review the papers. Table 2 shows the contribution of each of the reviewed paper. Our research model has used 3 different analytical aspects for the literature review by analyzing the most and the least discussed IoT security issues in the literature with respect to past, present and future era to understand the research trends and identify research gap within the area of IoT security.

Figure 4 shows the graphical representation of total number of papers in the past era addressing each IoT security issue. It can be observed that “data security and privacy” and “integrity” with 32 and 16 papers respectively and authenticity and confidentiality were both equally discussed with 14 papers are the most discussing security issues in the past. “Non-repudiation”, “authorization” and “inter-operability” with 2, 7 and 9 papers respectively are the least discussed IoT security issues in past era. In Table 3 discussed paper in past era i.e. from 2015 to 2017.

Present IoT Security Issues

We have grouped the papers from January 2018 to December 2019 and considered those papers' discussing IoT security issues as present time issues. Table 4 highlights what security issues have been highlighted and discussed by each short listed paper from present era i.e., from 2018 to 2019.

Figure 5 shows the graphical representation of total number of papers in the present era addressing each IoT security issue. It can be observed that "data security and privacy" and "integrity" with 38 and 18 papers respectively and authenticity and confidentiality were both equally discussed with 14 and 16 papers are the most discussing security issues in the present. "Non-repudiation", "authorization" and "inter-operability" with 5, 14 and 14 papers respectively are discussed IoT security issues in present era.

Future IoT Security Issues

We have grouped the papers from January 2020 to November 2020 and considered those papers' discussing IoT security issues as future research trends. Table 5 highlights what security issues have been highlighted and discussed by each short listed paper in year 2020.

Figure 6 shows the graphical representation of total number of papers in the addressing each IoT security issue in year 2020. It can be observed that "data security and privacy" have been discussed in 14 papers, "authenticity" and "confidentiality" both been discussed by 5 papers and "integrity" issue by 4 papers.

The least discussed security issues in future era as evident from literature is "non-repudiation" with no papers discussing this issue. Other least discussed security issues in future can include "Authorization" with 1 paper and "data availability", "access control" and "inter-operability" with 2 papers each.

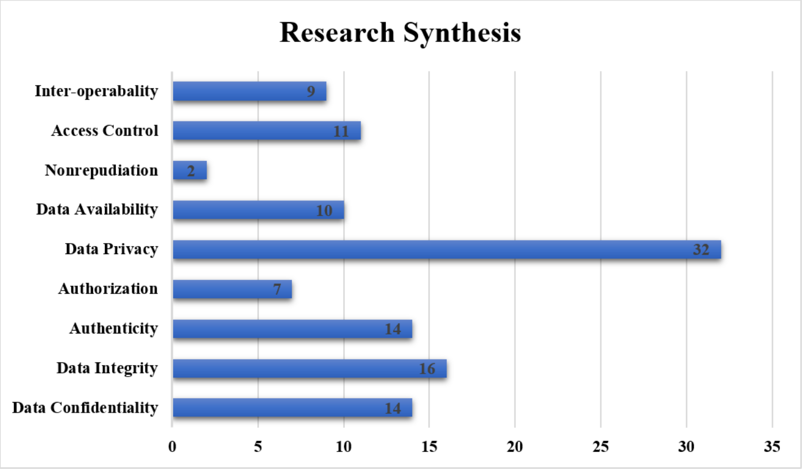

Fig. 4: Distribution of paper by IoT security threats in past

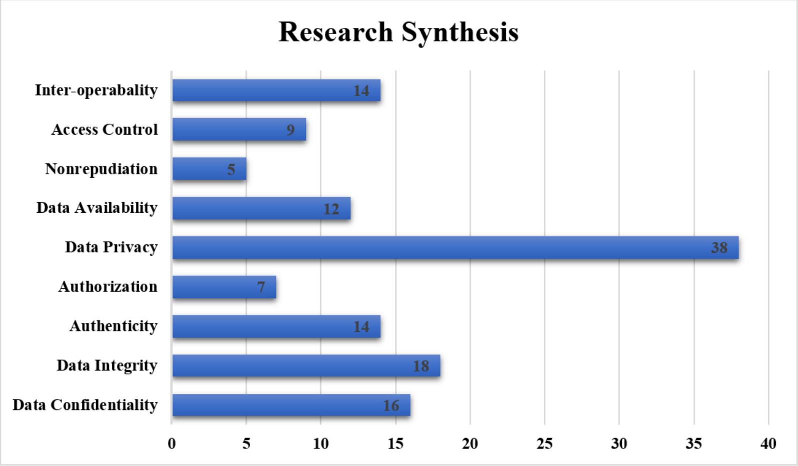

Fig. 5: Distribution of paper by IoT security threats in present

Table 2: Summary of contribution of each reviewed article (Past, Present and Future)

REF #	Contribution (past)
Farooq *et al*. (2015)	Prospective vulnerabilities and discrepancies in IoT
Gaikwad *et al*. (2015)	To utilize IoT framework for smart homes.
Hossain *et al*. (2015)	Addressing security and frame works related designs in IoT.
Andrea *et al*. (2015)	The investigation of security issues, Challenges and open issues in IoT
Alsaadi and Tubaishat (2015)	To evaluate IoT services in terms of security challenges
Amadeo *et al*. (2016)	IoT contemplation in field of various patterns utilization.
Basu *et al*. (2015)	Presenting security challenges related to IoT.
(“Security and Privacy Grand Challenges	The confine IoT security-related matter.
for the Internet of Things,” 2015)	The Network security related vulnerabilities in IoT
Singh and Singh (2015)	The security configuration related discrepancy in IoT
Alaba *et al*. (2017)	
(“Evolving privacy: From sensors to the Internet of Things,” 2017)	The savvy of IIoT security challenges s and vindicated outcomes.
Kolias *et al*. (2016)	The shortcomings in security of IoT middleware devices.
Billure *et al*. (2015)	Review about the IoT applications and their issues
Perera *et al*. (2015)	To assess the security examination of rising IIoT with Marketplace
Riazul Islam *et al*. (2015)	The overview of an extensive in the health care area utilizing IoT
Sadeghi *et al*. (2015)	Review the security and protection challenges in IIoT
Breivold and Sandstrom (2015)	Assess the security, protection and trust in IIoT
Hossain *et al*. (2015)	The security challenges, business openings and reference engineering for E-trade in IoT
Nalbandian (2015)	Apprise weak compliance research papers in IoT.
Zaslavsky and Georgakopoulos (2015)	Analyze the challenges and front line and its answers in web-scale sensor Information Management and Mobile Analytics using IoT
Granjal *et al*. (2015b)	The present status of various security issues with respect to IoT
Pescatore and Shpantzer (2014)	Existing conventions and open research security issues for IoT
Gil *et al*. (2016)	Review to making sure the IoT security
Ouaddah *et al*. (2017)	Address short comings in IoT security and protection.
Tzounis *et al*. (2017)	Security and protection suggestions for IoT
Abomhara and Køien (2015)	Review about the Vulnerabilities, Threats, Intruders and the IoT
Mosenia and Jha (2016)	The Privacy and Security concerns in Wearable and IoT gadgets
Yaqoob *et al*. (2017a)	Discuss about the Taxonomy of security assaults for IoT
REF #	CONTRIBUTION (PRESENT)
Conti *et al*. (2018)	Portray the new interoperability, the executives and Security Challenges in IoT
Riahi Sfar *et al*. (2018)	Assess the security different difficulties of the IoT
Adat and Gupta (2018)	The Recent Advances, Taxonomy, Requirements and Open Challenges for IoT Architecture
Khanna and Kaur (2019)	Examine the interferences to the utilization of farming, late advances and future difficulties for IoT
Miloslavskaya and Tolstoy (2019)	The point of the various security issues and its solutions and future headings
Hameed *et al*. (2019)	Assess the security challenges for cutting edge systems for IoT
Ali *et al*. (2019)	Review the innovations, applications and difficulties of IoT
Sisinni *et al*. (2018)	Overview the safe steering for IoT
Sun *et al*. (2018)	The review of various skills, issues and Prospects in IoT for Smart Healthcare
Nord *et al*. (2019)	The point of the data-driven systems for IoT difficulties and openings
Sha *et al*. (2018)	The survey of product characterized remote systems administration openings and difficulties for IoT
Grammatikis *et al*. (2019)	Review the open issues incorporation of distributed computing with IoT
Atlam *et al*. (2018)	Discuss and review the dependent on setting careful managements for IoT
Alphand *et al*. (2018)	Review of "Hands-On" IoT security
Hou *et al*. (2019)	Overview the security of IoT
Mendez Mena *et al*. (2018b)	Evaluate the various challenges of IoT
Forsstrom *et al*. (2018)	Assess the issues and new research frontiers in the field of IoT
REF #	CONTRIBUTION (FUTURE)
Stoyanova *et al*. (2020a)	The Challenges and new endeavors for the inclusion of IoT security and legal sciences
Song *et al*. (2020)	Review the top benefits and challenges of IoT and Data Analytics in Agriculture
Khadam *et al*. (2020)	Review and guide for security challenges in the IoT
Perera *et al*. (2020)	The issues, difficulties, scientific classification and design security in IoT.
Hossain *et al*. (2020)	Survey the Blockchain-based Secure IoT Control Scheme.
Mbarek *et al*. (2020)	The assessment researches the action towards Secure IoT Communication with Smart Contracts in a Blockchain Infrastructure
Basahel and Yamin (2020)	The effect on security issues and open issues in IoT
Hamad *et al*. (2020)	The investigation to finds the issues of the guide for security challenges in the IoT
Berger *et al*., 2020)	The investigation reviews how taxonomy, challenges and practice for IoT security and vulnerabilities

Table 3: IoT security issues in the past

Issues/Era	2015	2016	2017
Confidentiality	Gaikwad *et al*. (2015; Hossain *et al*., 2015; Andrea *et al*., 2015; Alsaadi and Tubaishat, 2015; Riazul Islam *et al*., 2015; Pescatore and Shpantzer, 2014; Abomhara and Køien, 2015; Sicari *et al*., 2015; Vasilomanolakis *et al*., 2015; Weber, 2015; Mahmoud *et al*., 2015; Granjal *et al*., 2015a)	(Weber and Boban, 2016)	Alaba *et al*. 2017; Ouaddah *et al*., 2017; Mosenia and Jha, 2016)
Integrity	Gaikwad *et al*. (2015; Hossain *et al*., 2015; Andrea *et al*., 2015; Basu *et al*., 2015; Billure *et al*., 2015; Riazul Islam *et al*., 2015; Breivold and Sandstrom, 2015; Abomhara and Køien, 2015; Mahmoud *et al*., 2015; Granjal *et al*., 2015a)	Gil *et al*. (2016; Elkhodr *et al*., 2016; Weber and Boban, 2016)	Alaba *et al*. (2017; Ouaddah *et al*., 2017; Mosenia and Jha, 2016; Yaqoob *et al*., 2017b)
Authenticity	Gaikwad *et al*. (2015; Hossain *et al*., 2015; Andrea *et al*., 2015; Riazul Islam *et al*., 2015; Pescatore and Shpantzer, 2014; Abomhara and Køien, 2015; Sicari *et al*., 2015; Vasilomanolakis *et al*., 2015; Mahmoud *et al*., 2015; Granjal *et al*., 2015a)	Elkhodr *et al*. (2016; Gupta and Shukla, 2016; Sood *et al*., 2015)	(Alaba *et al*., 2017)
Authorization	Farooq *et al*. (2015; Riazul Islam *et al*., 2015; Abomhara and Køien, 2015; Vasilomanolakis *et al*., 2015)	Gupta and Shukla (2016)	Alaba *et al*. (2017; Ouaddah *et al*., (2017)
Data security privacy	Gaikwad *et al*. (2015; Andrea *et al*., 2015) ("Security and Privacy Grand Challenges for the Internet of Things," 2015) Singh and Singh (2015) Perera *et al*. (2015) Sadeghi *et al*. (2015), Breivold and Sandstrom (2015) Ali *et al*. (2015) Nalbandian (2015) Abomhara and Køien. (2015; Granjal *et al*., (2015a) Sicari *et al*. (2015) Vasilomanolakis *et al*. (2015) Weber (2015; Fersi, 2015) Whitmore *et al*. (2015) Maras (2015; Arias *et al*. (2015)	(Amadeo *et al*., 2016), (Kolias *et al*., 2016), (Gil *et al*., 2016), (Elkhodr *et al*., 2016), (Weber and Boban, 2016), (Kumar *et al*., 2016), (Shah and Yaqoob, 2016), (Airehrour *et al*., 2016), (Sicari *et al*., 2016)	(Hussain, 2017), ("Evolving privacy: From sensors to the Internet of Things," 2017), (Ouaddah *et al*., 2017), (Tzounis *et al*., 2017), (Mosenia and Jha, 2016), (Yaqoob *et al*., 2017a), (Yaqoob *et al*., 2017b), (Risteska Stojkoska and Trivodaliev, 2017), (Atlam *et al*., 2017), (Guarda *et al*., 2017), (Baker *et al*., 2017), (Mehmood *et al*., 2017)
Availability	Gaikwad *et al*. (2015; Hossain *et al*., 2015; Andrea *et al*., 2015; Singh and Singh, 2015; Riazul Islam *et al*., 2015; Breivold and Sandstrom, 2015; Abomhara and Køien, 2015; Vasilomanolakis *et al*., 2015; Mahmoud *et al*., 2015)	(Shah and Yaqoob, 2016)	Ouaddah *et al*. (2017; Mosenia and Jha, 2016)
Non-repudiation	Hossain *et al*. (2015; Riazul Islam *et al*., 2015; Vasilomanolakis *et al*., 2015)		(Mosenia and Jha, 2016)
Access control	Hossain *et al*. (2015; Andrea *et al*., 2015; Pescatore and Shpantzer, 2014; Sicari *et al*., 2015; Granjal *et al*., 2015a; Granjal *et al*., 2015a)	Gil *et al*. (2016) Elkhodr *et al*., 2016)	Alaba *et al*. (2017) Ouaddah *et al*. (2017)
Inter-operability	Billure *et al*. (2015; Perera *et al*., 2015; Breivold and Sandstrom, 2015; Ali *et al*., 2015; Nalbandian, 2015; Weber, 2015; Fersi, 2015)	Elkhodr *et al*. (2016) Shah and Yaqoob (2016)	Hussain (2017; Tzounis *et al*., 2017; Yaqoob *et al*., 2017a; Risteska Stojkoska and Trivodaliev, 2017; Mehmood *et al*., 2017)

Table 4: IoT security issues in the present era

Issues/Era	2018	2019
Confidentiality	Adat and Gupta (2018; Mendez Mena *et al*., 2018a; Chen *et al*., 2018; Atlam *et al*., 2018; Mendez Mena *et al*., 2018b; Ali *et al*., 2020)	Khanna and Kaur (2019; Hameed *et al*., 2019; Al-Sharekh and Al-Shqeerat, 2019; Nord *et al*., 2019; Grammatikis *et al*., 2019; Hou *et al*., 2019; Chen *et al*., 2019)
Integrity	Adat and Gupta (2018; Mendez Mena *et al*., 2018a; Chen *et al*., 2018; Sun *et al*., 2018; Atlam *et al*., 2018; Mendez Mena *et al*., 2018b; Ali *et al*., 2020; Ni *et al*., 2018; Fakhri and Mutijarsa, 2018; Choi *et al*., 2018; Yu *et al*., 2018)	Alamri *et al*., 2019; a-Shqeerat, 2019; Nord *et al*., 2019; Grammatikis *et al*., 2019)
Authenticity	Conti *et al*. (2018; Chen *et al*., 2018; Atlam *et al*., 2018; Mendez Mena *et al*., 2018b; Choi *et al*., 2018; Yu *et al*., 2018; Agrawal *et al*., 2018; Das *et al*., 2018)	Alamri *et al*., 2019; Al-Sharekh and Al-Shqeerat, 2019; Ali *et al*., 2019; Grammatikis *et al*., 2019; Hou *et al*., 2019; Mohamad Noor and Hassan, 2019)
Authorization	Conti *et al*. (2018; Chen *et al*., 2018; Ali *et al*., 2020; Das *et al*., 2018)	Al-Sharekh and Al-Shqeerat (2019; Zhang *et al*., 2018)
Data security privacy	Conti *et al*. (2018; Wang *et al*., 2018; Adat and Gupta, 2018; "An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges," 2018; Mendez Mena *et al*., 2018a;	Alamri *et al*. (2019; Khanna and Kaur, 2019; Hameed *et al*., 2019; Al-Sharekh and Al-Shqeerat, 2019; Yaqoob *et al*., 2019; Nord *et al*., 2019; Grammatikis *et al*., 2019; Hou *et al*., 2019; Mohamad Noor and Hassan, 2019;

Table 4: Continue

	Sisinni *et al*., 2018; Chen *et al*., 2018; Sun *et al*., 2018; Sha *et al*., 2018; Atlam *et al*., 2018; Forsstrom *et al*., 2018; Ali *et al*., 2020; Ni *et al*., 2018; Yu *et al*., 2018; Das *et al*., 2018; Singh *et al*., 2018; Omar and Basir, 2018; Reyna *et al*., 2018; Jeon *et al*., 2018; Javed *et al*., 2018; Banerjee *et al*., 2018; Li *et al*., 2018)	Viriyasitavat *et al*., 2019; Dai *et al*., 2019)
Availability	Mendez Mena *et al*. (2018a; Chen *et al*., 2018; Atlam *et al*., 2018; Mendez Mena *et al*., 2018b; Ali *et al*., 2020)	Khanna and Kaur (2019; Al-Sharekh and Al-Shqeerat, 2019; Nord *et al*., 2019; Grammatikis *et al*., 2019)
Non-repudiation	Choi *et al*. (2018)	
Access control	Conti *et al*. (2018; Adat and Gupta, 2018; Chen *et al*., 2018; Sun *et al*., 2018; Atlam *et al*., 2018; Ni *et al*., 2018; Yu *et al*., 2018)	Ali *et al*. (2019; Hou *et al*., 2019; Zhang *et al*., 2018)
Inter-operability	Adat and Gupta (2018; "An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges," 2018; Sisinni *et al*., 2018; Jeon *et al*., 2018; Javed *et al*., 2018; Li *et al*., 2018)	(Khanna and Kaur, 2019), (Dai *et al*., 2019), (Noura *et al*., 2019)

Table 5: IoT security issues future trends

Issues/Era	2020
Confidentiality	Perera *et al*. (2020; Hossain *et al*., 2020; Mbarek *et al*., 2020; Berger *et al*., 2020; Yin *et al*., 2020)
Integrity	Mbarek *et al*. (2020; Hamad *et al*., 2020; Berger *et al*., 2020; Yin *et al*., 2020)
Authenticity	Mbarek *et al*. (2020; Hamad *et al*., 2020; Berger *et al*., 2020; Zhang and Xu, 2020; Li *et al*., 2020)
Authorization	Berger *et al*. (2020)
Data security privacy	Yuxin Liu *et al*. (2020; Mbarek *et al*., 2020; Basahel and Yamin, 2020; Hamad *et al*., 2020; Berger *et al*., 2020; Li *et al*., 2020; Yang *et al*., 2020; Stoyanova *et al*., 2020b; Yu Liu *et al*., 2020; Lin Liu *et al*., 2020; Abd EL-Latif *et al*., 2020; Mridha *et al*., 2020; Mawgoud *et al*., 2020; Al-Emran *et al*., 2020)
Availability	Berger *et al*. (2020; Yin *et al*., 2020)
Non-repudiation	
Access control	Hamad *et al*. (2020; Yu Liu *et al*., 2020)
Inter-operability	Mridha *et al*. (2020; Khan *et al*., 2020)

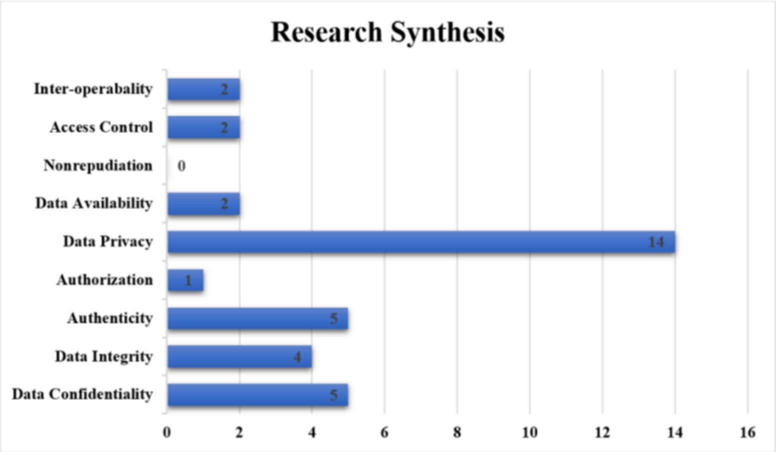

Fig. 6: Distribution of paper by IoT security threats in future

Our Contribution, Limitations and Future Research Direction

Several researchers have reviewed articles on security issues within IoT. Maria et-al discussed about IoT security with respect to IoT forensics and highlighted challenges and open issues (Stoyanova *et al*., 2020a). Another paper discussed about various security protocols implemented within IoT to ensure security within IoT (Granjal *et al*., 2015b). Researchers in (Neshenko *et al*., 2019) identified various vulnerabilities within IoT which are although same as what this study has identified such as availability, access control, authorization etc. but their analytical model is different from ours as they have segregated the reviewed articles with respect to IoT layers, security impact, countermeasures, security attacks and situational awareness capabilities after which they have discussed various remedies/solutions available in the literature to address these issues. This research study makes following novel contribution to the body of knowledge:

a. This is the first paper to the best of our knowledge, which has surveyed papers from years 2015-2020 to analyze the past, present and future trends in IoT security issues
b. This study has identified the most discussed security issues in last 5 years which clearly highlighted the most and the least discussed IoT security issues in the literature
c. By identifying most and the least discussed IoT security issues, we have identified and highlighted the gap within IoT security issues which needs to be addressed in future

There are a number of limitations of this research study which are:

a. This study only highlighted the most and the least discussed IoT security issues in the literature but not how those security issues have been addressed by the researchers
b. The survey has taken the most recent 5 years articles for the analysis which may provide us with the state of the art but not a comprehensive result
c. This research paper lacks discussion about the security algorithms/protocols being used to address various IoT security issues

In future, this research can be further extended into various directions with respect to IoT security issues:

a. More exhaustive literature review can be carried out to understand the mechanisms, tools, algorithms and protocols to address each of the security issues within IoT
b. There is a clear need to address the least discussed IoT security issues such as non-repudiation and inter-operability
c. New methods, algorithms and frameworks may be developed and introduced to address the most addressed security issues that needs optimization as well as the least addressed issues

Conclusion

IoT is an emerging technology that provides consumer satisfaction in terms of privacy and security. In this study, we have examined past, present and future of IoT security issues trends by identifying and reviewing already addressed in IoT security vulnerabilities. As IoT is gaining more popularity among researchers and practitioners, more security issues main arise in future which needs to be addressed if we need to harness the benefits of the IoT technology. This study has done extensive literature review of the last 5 years from 2015-2020 to identify various security issues within IoT and then analyzed the trend in discussion in the literature of the identified issues with respect to past, present and future. It has been identified that in the past, “data security and privacy”, “integrity” and “confidentiality are the most discussed security issues whereas “non-repudiation”, “authorization” and “access control” are least discussed. In present and even in future, “data security and privacy” and “integrity”, “authenticity and “confidentiality” are the most discussed security issues within IoT while authorization and non-repudiation are the least discussed security issues. This research can act as a starting point for a researcher who decides to work in this imperative area of IoT security.

Acknowledgement

This research is funded by Universiti Kuala Lumpur (UniKL) and Centre for Research and Innovation (CORI).

Funding Information

This work was supported by the Universiti Kuala Lumpur, Malaysia, through the Short Term Research Grant (STRG) and Center of Research and Innovation (CORI).

Author’s Contributions

Every author has equal contribution in this research.

Ethics

This research paper is genuine and all authors have read it thoroughly and approved that it does not contain any material which is already published. In this article no ethical issues are involved.

References

Abd EL-Latif, A. A., Abd-El-Atty, B., & Abou-Nassar, E. M., Venegas-Andraca, S. E., (2020). Controlled alternate quantum walks based privacy preserving healthcare images in Internet of Things. Optics & Laser Technology 124, 105942. doi.org/10.1016/j.optlastec.2019.105942

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 65-88. https://journals.riverpublishers.com/index.php/JCSANDM/article/view/6087

Adat, V., & Gupta, B. B. (2018). Security in Internet of Things: issues, challenges, taxonomy and architecture. Telecommunication Systems, 67(3), 423-441. https://link.springer.com/article/10.1007/s11235-017-0345-9

Agrawal, R., Verma, P., Sonanis, R., Goel, U., De, A., Kondaveeti, S. A., & Shekhar, S. (2018, April). Continuous security in IoT using blockchain. In 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 6423-6427). IEEE. doi.org/10.1109/ICASSP.2018.8462513

Airehrour, D., Gutierrez, J., & Ray, S. K. (2016). Secure routing for internet of things: A survey. Journal of Network and Computer Applications, 66, 198-213. doi.org/10.1016/j.jnca.2016.03.006

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10-28. doi.org/10.1016/j.jnca.2017.04.002

Alamri, M., Jhanjhi, N. Z., & Humayun, M. (2019). Blockchain for Internet of Things (IoT) research issues challenges & future directions: A review. Int. J. Comput. Sci. Netw. Secur, 19, 244-258. https://expert.taylors.edu.my/file/rems/publication/109566_6018_1.pdf

Al-Emran, M., Malik, S. I., & Al-Kabi, M. N. (2020). A survey of internet of things (IoT) in education: Opportunities and challenges. Toward social internet of things (SIoT): Enabling technologies, architectures and applications, 197-209. doi.org/10.1007/978-3-030-24513-9_12

Ali, I., Sabir, S., & Ullah, Z. (2019). Internet of things security, device authentication and access control: A review. arXiv preprint arXiv:1901.07309. https://arxiv.org/abs/1901.07309

Ali, J., Ali, T., Musa, S., & Zahrani, A. (2020). Towards secure IoT communication with smart contracts in a blockchain infrastructure. arXiv preprint arXiv:2001.01837. doi.org/10.14569/IJACSA.2018.091070

Almotiri, S. H., Khan, M. A., & Alghamdi, M. A. (2016, August). Mobile health (m-health) system in the context of IoT. In 2016 IEEE 4th international conference on future internet of things and cloud workshops (FiCloudW) (pp. 39-42). IEEE. doi.org/10.1109/W-FiCloud.2016.24

Alphand, O., Amoretti, M., Claeys, T., Dall'Asta, S., Duda, A., Ferrari, G., ... & Zanichelli, F. (2018, April). IoTChain: A blockchain security architecture for the Internet of Things. In 2018 IEEE wireless communications and networking conference (WCNC) (pp. 1-6). IEEE. doi.org/10.1109/WCNC.2018.8377385

Alsaadi, E., & Tubaishat, A. (2015). Internet of things: Features, challenges and vulnerabilities. International Journal of Advanced Computer Science and Information Technology, 4(1), 1-13. http://elvedit.com/journals/IJACSIT/wp-content/uploads/2015/02/internet-of-things.pdf

Al-Sharekh, S. I., & Al-Shqeerat, K. H. (2020, February). An Overview of Privacy Issues in IoT Environments. In 2019 International Conference on Advances in the Emerging Computing Technologies (AECT) (pp. 1-6). IEEE. doi.org/10.1109/AECT47998.2020.9194197

Amadeo, M., Campolo, C., Quevedo, J., Corujo, D., Molinaro, A., Iera, A., ... & Vasilakos, A. V. (2016). Information-centric networking for the internet of things: Challenges and opportunities. IEEE Network, 30(2), 92-100. doi.org/10.1109/MNET.2016.7437030

Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015, July). Internet of Things: Security vulnerabilities and challenges. In 2015 IEEE symposium on computers and communication (ISCC) (pp. 180-187). IEEE. doi.org/10.1109/ISCC.2015.7405513

Arias, O., Wurm, J., Hoang, K., & Jin, Y. (2015). Privacy and security in internet of things and wearable devices. IEEE Transactions on Multi-Scale Computing Systems, 1(2), 99-109. doi.org/10.1109/TMSCS.2015.2498605

Atlam, H. F., Alenezi, A., Alharthi, A., Walters, R. J., & Wills, G. B. (2017, June). Integration of cloud computing with internet of things: Challenges and open issues. In 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 670-675). IEEE. doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.105

Atlam, H. F., Walters, R. J., & Wills, G. B. (2018, August). Internet of nano things: Security issues and applications. In Proceedings of the 2018 2nd International Conference on Cloud and Big Data Computing (pp. 71-77). doi.org/10.1145/3264560.3264570

Baker, S. B., Xiang, W., & Atkinson, I. (2017). Internet of things for smart healthcare: Technologies, challenges and opportunities. IEEE Access, 5, 26521-26544. doi.org/10.1109/ACCESS.2017.2775180

Banerjee, M., Lee, J., & Choo, K. K. R. (2018). A blockchain future for internet of things security: a position paper. Digital Communications and Networks, 4(3), 149-160. doi.org/10.1016/j.dcan.2017.10.006

Basahel, A. M., & Yamin, M. (2020). Cyber Security and Privacy in Internet of Things. International Journal of Human Potentials Management, 2(1), 43-53. http://abmjournal.org/index.php/ijhpm/article/view/26

Basu, S. S., Tripathy, S., & Chowdhury, A. R. (2015, May). Design challenges and security issues in the Internet of Things. In 2015 IEEE Region 10 Symposium (pp. 90-93). IEEE. doi.org/10.1109/TENSYMP.2015.25

Berger, S., Bürger, O., & Röglinger, M. (2020). Attacks on the Industrial Internet of Things–Development of a multi-layer Taxonomy. Computers & Security, 93, 101790. doi.org/10.1016/j.cose.2020.101790

Billure, R., Tayur, V. M., & Mahesh, V. (2015, June). Internet of Things-a study on the security challenges. In 2015 IEEE International Advance Computing Conference (IACC) (pp. 247-252). IEEE. doi.org/10.1109/IADCC.2015.7154707

Breivold, H. P., & Sandström, K. (2015, December). Internet of things for industrial automation--challenges and technical solutions. In 2015 IEEE International Conference on Data Science and Data Intensive Systems (pp. 532-539). IEEE. doi.org/10.1109/DSDIS.2015.11

Chen, H., Pendleton, M., Njilla, L., & Xu, S. (2019). A survey on Ethereum systems security: Vulnerabilities, attacks and defenses. arXiv preprint arXiv:1908.04507. https://arxiv.org/abs/1908.04507

Chen, K., Zhang, S., Li, Z., Zhang, Y., Deng, Q., Ray, S., & Jin, Y. (2018). Internet-of-things security and vulnerabilities: Taxonomy, challenges and practice. Journal of Hardware and Systems Security, 2(2), 97-110. https://link.springer.com/article/10.1007/s41635-017-0029-7

Choi, S. S., Burm, J. W., Sung, W., Jang, J. W., & Reo, Y. J. (2018, June). A blockchain-based secure iot control scheme. In 2018 International Conference on Advances in Computing and Communication Engineering (ICACCE) (pp. 74-78). IEEE. doi.org/10.1109/ICACCE.2018.8441717

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. doi.org/10.1016/j.future.2017.07.060

Dai, H. N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. IEEE Internet of Things Journal, 6(5), 8076-8094. doi.org/10.1109/JIOT.2019.2920987

Das, A.K., Zeadally, S., He, D., 2018. Taxonomy and analysis of security protocols for Internet of Things. Future Generation Computer Systems 89, 110–125. doi.org/10.1016/j.future.2018.06.027

Elijah, O., Rahman, T. A., Orikumhi, I., Leow, C. Y., & Hindia, M. N. (2018). An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges. IEEE Internet of Things Journal, 5(5), 3758-3773. doi.org/10.1109/JIOT.2018.2844296

Elkhodr, M., Shahrestani, S., & Cheung, H. (2016). The internet of things: New interoperability, management and security challenges. arXiv preprint arXiv:1604.04824. doi.org/10.5121/ijnsa.2016.8206

Fakhri, D., & Mutijarsa, K. (2018, October). Secure IoT communication using blockchain technology. In 2018 International Symposium on Electronics and Smart Devices (ISESD) (pp. 1-6). IEEE. doi.org/10.1109/ISESD.2018.8605485

Farooq, M. U., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T. (2015). A review on internet of things (IoT). International journal of computer applications, 113(1), 1-7. file:///C:/Users/123/Downloads/56%20(1).pdf

Fersi, G. (2015, June). Middleware for internet of things: A study. In 2015 International Conference on Distributed Computing in Sensor Systems (pp. 230-235). IEEE. doi.org/10.1109/DCOSS.2015.43

Forsström, S., Butun, I., Eldefrawy, M., Jennehag, U., & Gidlund, M. (2018, April). Challenges of securing the industrial internet of things value chain. In 2018 Workshop on Metrology for Industry 4.0 and IoT (pp. 218-223). IEEE. doi.org/10.1109/METROI4.2018.8428344

Gaikwad, P. P., Gabhane, J. P., & Golait, S. S. (2015, April). A survey based on Smart Homes system using Internet-of-Things. In 2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC) (pp. 0330-0335). IEEE. doi.org/10.1109/ICCPEIC.2015.7259486

Gil, D., Ferrández, A., Mora-Mora, H., & Peral, J. (2016). Internet of things: A review of surveys based on context aware intelligent services. Sensors, 16(7), 1069. /doi.org/10.3390/s16071069

Grammatikis, P. I. R., Sarigiannidis, P. G., & Moscholios, I. D. (2019). Securing the Internet of Things: Challenges, threats and solutions. Internet of Things, 5, 41-70. doi.org/10.1016/j.iot.2018.11.003

Granjal, J., Monteiro, E., & Silva, J. S. (2015a). Security for the internet of things: A survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials, 17(3), 1294-1312. doi.org/10.1109/COMST.2015.2388550

Granjal, J., Monteiro, E., & Sa Silva, J., (2015b). Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. IEEE Communications Surveys & Tutorials 17, 1294–1312. doi.org/10.1109/COMST.2015.2388550

Guarda, T., Leon, M., Augusto, M. F., Haz, L., De la Cruz, M., Orozco, W., & Alvarez, J. (2017, June). Internet of Things challenges. In 2017 12th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-4). IEEE. doi.org/10.23919/CISTI.2017.7975936

Gupta, K., & Shukla, S. (2016, February). Internet of Things: Security challenges for next generation networks. In 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH) (pp. 315-318). IEEE. doi.org/10.1109/ICICCS.2016.7542301

Ali, Z. H., Ali, H. A., & Badawy, M. M. (2015). Internet of Things (IoT): Definitions, challenges and recent research directions. International Journal of Computer Applications, 128(1), 37-47.

Hamad, S. A., Sheng, Q. Z., Zhang, W. E., & Nepal, S. (2020). Realizing an internet of secure things: A survey on issues and enabling technologies. IEEE Communications Surveys & Tutorials, 22(2), 1372-1391. doi.org/10.1109/COMST.2020.2976075

Hameed, S., Khan, F. I., & Hameed, B. (2019). Understanding security requirements and challenges in Internet of Things (IoT): A review. Journal of Computer Networks and Communications, 2019. doi.org/10.1155/2019/9629381

Hassan, R., Qamar, F., Hasan, M. K., Aman, A. H. M., & Ahmed, A. S. (2020). Internet of Things and its applications: A comprehensive survey. Symmetry, 12(10), 1674 doi.org/10.3390/sym12101674

Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. Computer networks, 148, 283-294. doi.org/10.1016/j.comnet.2018.11.025

Hossain, M. M., Fotouhi, M., & Hasan, R. (2015, June). Towards an analysis of security issues, challenges and open problems in the internet of things. In 2015 ieee world congress on services (pp. 21-28). IEEE. doi.org/10.1109/SERVICES.2015.12

Hossain, M. S., Waheed, S., Rahman, Z., Shezan, S. K. A., & Hossain, M. M. (2020). Blockchain for the security of Internet of Things: A smart home use case using Ethereum. International Journal of Recent Technology and Engineering, 8(5), 4601-4608.

Hou, J., Qu, L., & Shi, W. (2019). A survey on internet of things security from data perspectives. Computer Networks, 148, 295-306. doi.org/10.1016/j.comnet.2018.11.026

Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The internet of things for health care: A comprehensive survey. IEEE access, 3, 678-708. doi.org/10.1109/ACCESS.2015.2437951

Javed, F., Afzal, M. K., Sharif, M., & Kim, B. S. (2018). Internet of Things (IoT) operating systems support, networking technologies, applications and challenges: A comparative review. IEEE Communications Surveys & Tutorials, 20(3), 2062-2100. doi.org/10.1109/COMST.2018.2817685

Jeon, K. E., She, J., Soonsawad, P., & Ng, P. C. (2018). Ble beacons for internet of things applications: Survey, challenges and opportunities. IEEE Internet of Things Journal, 5(2), 811-828. doi.org/10.1109/JIOT.2017.2788449

Khadam, U., Iqbal, M. M., Alruily, M., Al Ghamdi, M. A., Ramzan, M., & Almotiri, S. H. (2020). Text data security and privacy in the internet of things: Threats, challenges and future directions. Wireless Communications and Mobile Computing, 2020. doi.org/10.1155/2020/7105625

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions and open challenges. Future generation computer systems, 82, 395-411. doi.org/10.1016/j.future.2017.11.022

Khan, W. Z., Rehman, M. H., Zangoti, H. M., Afzal, M. K., Armi, N., & Salah, K. (2020). Industrial internet of things: Recent advances, enabling technologies and open challenges. Computers & Electrical Engineering, 81, 106522. doi.org/10.1016/j.compeleceng.2019.106522

Khanna, A., & Kaur, S. (2019). Evolution of Internet of Things (IoT) and its significant impact in the field of Precision Agriculture. Computers and electronics in agriculture, 157, 218-231. doi.org/10.1016/j.compag.2018.12.039

Kolias, C., Stavrou, A., Voas, J., Bojanova, I., & Kuhn, R. (2016). Learning Internet-of-Things security" hands-on". IEEE Security & Privacy, 14(1), 37-46. doi.org/10.1109/MSP.2016.4

Kumar, S. A., Vealey, T., & Srivastava, H. (2016, January). Security in internet of things: Challenges, solutions and future directions. In 2016 49th Hawaii International Conference on System Sciences (HICSS) (pp. 5772-5781). IEEE. doi.org/10.1109/HICSS.2016.714

Li, J., Zhang, Z., Hui, L., & Zhou, Z. (2020). A Novel Message Authentication Scheme With Absolute Privacy for the Internet of Things Networks. IEEE Access, 8, 39689-39699. doi.org/10.1109/ACCESS.2020.2976161

Li, S., Da Xu, L., & Zhao, S. (2018). 5G Internet of Things: A survey. Journal of Industrial Information Integration, 10, 1-9. doi.org/10.1016/j.jii.2018.01.005

Liu, L., Su, J., Zhao, B., Wang, Q., Chen, J., & Luo, Y. (2020a). Towards an efficient privacy-preserving decision tree evaluation service in the Internet of Things. Symmetry, 12(1), 103. doi.org/10.3390/sym12010103

Liu, Y., Xue, K., He, P., Wei, D. S., & Guizani, M. (2020b). An Efficient, Accountable and Privacy-Preserving Access Control Scheme for Internet of Things in a Sharing Economy Environment. IEEE Internet of Things Journal, 7(7), 6634-6646. doi.org/10.1109/JIOT.2020.2975140

Liu, Y., Ma, M., Liu, X., Xiong, N. N., Liu, A., & Zhu, Y. (2018). Design and analysis of probing route to defense sink-hole attacks for Internet of Things security. IEEE Transactions on Network Science and Engineering, 7(1), 356-372. doi.org/10.1109/TNSE.2018.2881152

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015, December). Internet of things (IoT) security: Current status, challenges and prospective measures. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 336-341). IEEE. doi.org/10.1109/ICITST.2015.7412116

Maras, M. H. (2015). Internet of Things: Security and privacy implications. International Data Privacy Law, 5(2), 99. researchgate.net/profile/Marie-Helen-Maras/publication/275228804_Internet_of_Things_security_and_privacy_implications/links/586d4dfa08ae329d62138f0a/Internet-of-Things-security-and-privacy-implications.pdf

Mawgoud, A. A., Taha, M. H. N., & Khalifa, N. E. M. (2020). Security threats of social internet of things in the higher education environment. In Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications (pp. 151-171). Springer, Cham. doi.org/10.1007/978-3-030-24513-9_9

Mbarek, B., Ge, M., & Pitner, T. (2020). An efficient mutual authentication scheme for internet of things. Internet of Things, 9, 100160. doi.org/10.1016/j.iot.2020.100160

Mehmood, Y., Ahmad, F., Yaqoob, I., Adnane, A., Imran, M., & Guizani, S. (2017). Internet-of-things-based smart cities: Recent advances and challenges. IEEE Communications Magazine, 55(9), 16-24. doi.org/10.1109/MCOM.2017.1600514

Mendez Mena, D., Papapanagiotou, I., & Yang, B. (2018). Internet of things: Survey on security. Information Security Journal: A Global Perspective, 27(3), 162-182. doi.org/10.1080/19393555.2018.1458258

Miloslavskaya, N., & Tolstoy, A. (2019). Internet of things: information security challenges and solutions. Cluster Computing, 22(1), 103-119. https://link.springer.com/article/10.1007/s10586-018-2823-6

Mosenia, A., & Jha, N. K. (2016). A comprehensive study of security of internet-of-things. IEEE Transactions on emerging topics in computing, 5(4), 586-602. doi.org/10.1109/TETC.2016.2606384

Mridha, M. F., Hamid, M. A., & Asaduzzaman, M. (2020). Issues of Internet of Things (IoT) and an intrusion detection system for IoT using machine learning paradigm. In Proceedings of International Joint Conference on Computational Intelligence (pp. 395-406). Springer, Singapore. doi.org/10.1007/978-981-13-7564-4_34

Nalbandian, S. (2015, November). A survey on Internet of Things: Applications and challenges. In 2015 International Congress on Technology, Communication and Knowledge (ICTCK) (pp. 165-169). IEEE. doi.org/10.1109/ICTCK.2015.7582664

Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. IEEE Communications Surveys & Tutorials, 21(3), 2702-2733. doi.org/10.1109/COMST.2019.2910750

Nord, J. H., Koohang, A., & Paliszkiewicz, J. (2019). The Internet of Things: Review and theoretical framework. Expert Systems with Applications, 133, 97-108. doi.org/10.1016/j.eswa.2019.05.014

Noura, M., Atiquzzaman, M., & Gaedke, M. (2019). Interoperability in internet of things: Taxonomies and open challenges. Mobile Networks and Applications, 24(3), 796-809. https://link.springer.com/article/10.1007/s11036-018-1089-9

Omar, A. S., & Basir, O. (2018, July). Identity management in IoT networks using blockchain and smart contracts. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 994-1000). IEEE. doi.org/10.1109/Cybermatics_2018.2018.00187

Ouaddah, A., Mousannif, H., Abou Elkalam, A., & Ouahman, A. A. (2017). Access control in the Internet of Things: Big challenges and new opportunities. Computer Networks, 112, 237-262. doi.org/10.1016/j.comnet.2016.11.007

Perera, C., Barhamgi, M., Bandara, A. K., Ajmal, M., Price, B., & Nuseibeh, B. (2020). Designing privacy-aware internet of things applications. Information Sciences, 512, 238-257. doi.org/10.1016/j.ins.2019.09.061

Perera, C., Liu, C. H., & Jayawardena, S. (2015). The emerging internet of things marketplace from an industrial perspective: A survey. IEEE transactions on emerging topics in computing, 3(4), 585-598. doi.org/10.1109/TETC.2015.2390034

Pescatore, J., & Shpantzer, G. (2014). Securing the internet of things survey. SANS Institute, 1-22. file:///C:/Users/PC/Downloads/securing-internet-things-survey-34785.pdf

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. Future generation computer systems, 88, 173-190. doi.org/10.1016/j.future.2018.05.046

Sadeeq, M. A., Zeebaree, S. R., Qashi, R., Ahmed, S. H., & Jacksi, K. (2018, October). Internet of Things security: a survey. In 2018 International Conference on Advanced Science and Engineering (ICOASE) (pp. 162-166). IEEE. doi.org/10.1109/ICOASE.2018.8548785

Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015, June). Security and privacy challenges in industrial internet of things. In 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC) (pp. 1-6). IEEE. doi.org/10.1145/2744769.2747942.

Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, 4(2), 118-137. doi.org/10.1016/j.dcan.2017.04.003

Sha, K., Wei, W., Yang, T. A., Wang, Z., & Shi, W. (2018). On security challenges and open issues in Internet of Things. Future Generation Computer Systems, 83, 326-337. doi.org/10.1016/j.future.2018.01.059

Shafiq, M., Zhang, Q., Akbar, M. A., Alsanad, A., & Mahmood, S. (2020). Factors influencing the requirements engineering process in offshore software development outsourcing environments. IET Software, 14(6), 623-637. https://ieeexplore.ieee.org/document/9278577/

Shah, S. H., & Yaqoob, I. (2016, August). A survey: Internet of Things (IOT) technologies, applications and challenges. In 2016 IEEE Smart Energy Grid Engineering (SEGE) (pp. 381-385). IEEE. doi.org/10.1109/SEGE.2016.7589556

Sicari, S., Rizzardi, A., Grieco, L.A., & Coen-Porisini, A., (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks 76, 146–164. doi.org/10.1016/j.comnet.2014.11.008

Sicari, S., Rizzardi, A., Miorandi, D., & Coen-Porisini, A. (2016, November). Internet of Things: Security in the keys. In Proceedings of the 12th ACM Symposium on QoS and Security for Wireless and Mobile Networks (pp. 129-133). doi.org/10.1145/2988272.2988280

Singh, M., Singh, A., & Kim, S. (2018, February). Blockchain: A game changer for securing IoT data. In 2018 IEEE 4th World Forum on Internet of Things (WF-IoT) (pp. 51-55). IEEE. doi.org/10.1109/WF-IoT.2018.8355182

Singh, S., & Singh, N. (2015, October). Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce. In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT) (pp. 1577-1581). Ieee. doi.org/10.1109/ICGCIoT.2015.7380718

Sisinni, E., Saifullah, A., Han, S., Jennehag, U., & Gidlund, M. (2018). Industrial internet of things: Challenges, opportunities and directions. IEEE transactions on industrial informatics, 14(11), 4724-4734. doi.org/10.1109/TII.2018.2852491

Sood, K., Yu, S., & Xiang, Y. (2015). Software-defined wireless networking opportunities and challenges for Internet-of-Things: A review. IEEE Internet of Things Journal, 3(4), 453-463. doi.org/10.1109/JIOT.2015.2480421

Stojkoska, B. L. R., & Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. Journal of Cleaner Production, 140, 1454-1464. doi.org/10.1016/j.jclepro.2016.10.006

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020a). A survey on the internet of things (IoT) forensics: Challenges, approaches and open issues. IEEE Communications Surveys & Tutorials, 22(2), 1191-1221. doi.org/10.1109/COMST.2019.2962586

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K., (2020b). A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches and Open Issues. IEEE Communications Surveys & Tutorials 1-1. https://doi.org/10.1109/comst.2019.2962586

Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G. (2018). Security and privacy in the medical internet of things: a review. Security and Communication Networks, 2018. doi.org/10.1155/2018/5978636

Tzounis, A., Katsoulas, N., Bartzanas, T., & Kittas, C. (2017). Internet of Things in agriculture, recent advances and future challenges. Biosystems engineering, 164, 31-48. doi.org/10.1016/j.biosystemseng.2017.09.007

Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., & Kikiras, P. (2015, September). On the security and privacy of Internet of Things architectures and systems. In 2015 International Workshop on Secure Internet of Things (SIoT) (pp. 49-57). IEEE. doi.org/10.1109/SIOT.2015.9

Viriyasitavat, W., Anuphaptrirong, T., & Hoonsopon, D. (2019). When blockchain meets Internet of Things: Characteristics, challenges and business opportunities. Journal of industrial information integration, 15, 21-28. doi.org/10.1016/j.jii.2019.05.002

Wang, S., Yuan, Y., Wang, X., Li, J., Qin, R., & Wang, F. Y. (2018, June). An overview of smart contract: Architecture, applications and future trends. In 2018 IEEE Intelligent Vehicles Symposium (IV) (pp. 108-113). IEEE. doi.org/10.1109/IVS.2018.8500488

Weber, M., & Boban, M. (2016, May). Security challenges of the internet of things. In 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 638-643). IEEE. doi.org/10.1109/MIPRO.2016.7522219

Weber, R. H. (2015). Internet of things: Privacy issues revisited. Computer Law & Security Review, 31(5), 618-627. doi.org/10.1016/j.clsr.2015.07.002

Whitmore, A., Agarwal, A., Da Xu, L., 2015. The Internet of Things-A survey of topics and trends. Information Systems Frontiers 17, 261–274. https://link.springer.com/article/10.1007%2Fs10796-014-9489-2

Yang, P., Kang, X., Wu, Q., Yang, B., & Zhang, P. (2020). Participant selection strategy with privacy protection for internet of things search. IEEE Access, 8, 40966-40976. doi.org/10.1109/ACCESS.2020.2976614

Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., & Guizani, M. (2017a). Internet of things architecture: Recent advances, taxonomy, requirements and open challenges. IEEE wireless communications, 24(3), 10-16. doi.org/10.1109/MWC.2017.1600421

Yaqoob, I., Ahmed, E., ur Rehman, M. H., Ahmed, A. I. A., Al-garadi, M. A., Imran, M., & Guizani, M. (2017b). The rise of ransomware and emerging security challenges in the Internet of Things. Computer Networks, 129, 444-458. doi.org/10.1016/j.comnet.2017.09.003

Yaqoob, I., Hashem, I. A. T., Ahmed, A., Kazmi, S. A., & Hong, C. S. (2019). Internet of things forensics: Recent advances, taxonomy, requirements and open challenges. Future Generation Computer Systems, 92, 265-275. doi.org/10.1016/j.future.2018.09.058

Yin, L., Fang, B., Guo, Y., Sun, Z., & Tian, Z. (2020). Hierarchically defining Internet of Things security: From CIA to CACA. International Journal of Distributed Sensor Networks, 16(1), 1550147719899374. doi.org/10.1177/1550147719899374

Yu, Y., Li, Y., Tian, J., & Liu, J. (2018). Blockchain-based solutions to security and privacy issues in the internet of things. IEEE Wireless Communications, 25(6), 12-18. doi.org/10.1109/MWC.2017.1800116

Zaslavsky, A., & Georgakopoulos, D. (2015, June). Internet of things: Challenges and state-of-the-art solutions in internet-scale sensor information management and mobile analytics. In 2015 16th IEEE International Conference on Mobile Data Management (Vol. 2, pp. 3-6). IEEE. doi.org/10.1109/MDM.2015.72

Zhang, Q., & Xu, D. (2020). Security authentication technology based on dynamic Bayesian network in Internet of Things. Journal of Ambient Intelligence and Humanized Computing, 11(2), 573-580. https://link.springer.com/article/10.1007/s12652-018-0949-2

Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2018). Smart contract-based access control for the internet of things. IEEE Internet of Things Journal, 6(2), 1594-1605. doi.org/10.1109/JIOT.2018.2847705