**Abstract**— It is brief according to the topic that it will focus on IoT based security issues. This study will focus on rigorous literature review which will provides us trustworthy path to satisfy the industry need. In curtail IoT is not just about interconnecting embedded devices or gadgets to the Internet, however, it is also fast and continuously growing to improve the ease or satisfaction of life. The motive of IoT services is to connect the entire globe through sensors. This study reviews the IoT methodologies in the light of qualitative research. The data analysis and synthesis focus over the last three years (2018 to 2020) which are based on the PRISMA block diagram for understanding. The review identifies the IoT privacy and security issues from a different perspective and also finds out which security issue is mostly discussed in the last few years which elaborated as a basis for further research. After a review of this paper, we can easily understand the different problem faces of IoT devices with the help of comparative analysis using summarize tables and graphical representation of IoT in context of the privacy and security challenges and issues face of IoT devices. After vigorous survey, it is clear that in future most of the paper will discuss data security and privacy, confidentiality, and authenticity.

**Index Terms**—Data Security, Privacy, Confidentiality, Internet of Things

**I. INTRODUCTION**

The Internet is a robust technology that become imperative part of every human being nowadays. It has revolutionized communications, to the degree that it is presently our favored medium of daily life communication. Even in our routine life is decided after the utilization of the Internet [1], [2]. Researchers depicts after onerous circumspect assess that approximately 20-50 billion devices will connect to the internet to facilitates humans in their daily life (see figure 1).

The IoT is predictable the most significant domain of present and upcoming revolution and is increasing huge consideration from an extensive collection of several businesses [3], [4].

The Internet for Things (IoT) focuses on the Internet. It has increased its popularity in the last few years [5], [6]. IoT can be the ability to sharing data over a network without using the human-to-human or human-to-PC connection. [7], [8], [9]. The IoT can connect and respond billions of devices at a time without any delay [10], it establishes a data-sharing requirement which improves our lives rapidly [11], [12]. In other words IoT is also adopting exponential growth rate that enacts progress in every walk of life [13], [14], [15].

![Fig: 1. Predictable perception of smart devices by the year 2020][1]

Therefore, in addition to conventional machines, for example, work area PC, workstations, highlight telephone versatile, and so on, all are the physical items or things that will get the capacity to speak with one another [17], [18], [19]. The IoT has

---

1Malaysian Institute of Information Technology (MIIT), Universiti Kuala Lumpur, Kuala Lumpur 50250, Malaysia
2College of Computer Science and Information Systems, Institute of Business Management, Karachi, Pakistan
given better opportunities in the several domain such cloud computing [20], Industrial IoT and its innovation area while carrying a few challenges to an expanded degree of concern [21], [22], [23]. Security and privacy issues in IoT situations would be considerably more challenging than what is been utilized in ordinary wireless situations [24], [25], [26]. The research is beneficial for beginners who want to learn the challenges of IoT from scratch as well as professionals [27], [28], [29]. In IoT devices the major issues are the message modification and/or alteration [30], [31], [32]. This study appraised analysis of the security and privacy for IoT. This review paper presents the categorizing the attacks under nine types of attacks from 2018 to 2020. In particular, this paper targets tending to the following exploration objectives:

1. To identify potential security issues in IoT.
2. To comprehend which IoT security issues have acquired consideration in the literature.

The paper is organized as follows. Section II provides the literature review including application domains of IoT and different security issues of IoT. Section III explores the systematic literature review protocol by using the PRISMA flowchart of included articles. In Section IV the results & discussion regarding security and privacy of IoT using the table and graphs (PI Chart). Then Section V discuss about the comparative analysis of from 2018 to 2020 era. At the end in Section VI establishes the conclusion.

II. LITERATURE REVIEW

The first concept of IoT by Kevin Ashton in 1999, which has now progressed into a realism that interlinks sensors, electronic smart gadgets to the Internet [33].

The Security issues in IoT

For IoT security, CIA objectives are also followed to hinder any cyber threat [34], [35]. The IoT is latest technology and has numerous limitations also which restricts its functionality in new devices or gadgets, power and its computations [36], [37], see in figure 2. The main IoT security concerns are as follows:

- **Confidentiality**
  Confidentiality guarantees that delicate information are accessed to simply by an approved individual person and avoided those not approved to have them. [38] [39].

- **Integrity**
  Integrity guarantees that data is in a configuration that is valid and right to its unique purposes. The recipient of the data should have the information and that can be edited by authorized persons only [40].

- **Availability**
  Availability guarantees that information and resources are accessible to the individuals who need them. It is carried out utilizing strategies [16].

- **Authorization**
  Authorization guarantees that the client have the necessary control authorizations or advantage to play out the activity or certain activity [40].

- **Access Control**
  Access control guarantee that the security perspective mechanisms that handle and assurance access right of just approved users [41].

- **Authenticity**
  Authentication is manages individual data. It incorporates approving the approaching the incoming messages against certain recognizing credentials [41].

- **Non-repudiation**
  Non-repudiation is making proof to demonstrate certain activities and it guarantees that it can't be repudiated later that is accomplished by the utilization of Digital Signature and Timestamps [42].

- **Interoperability**
  Interoperability means to the ability of a different systems to associate and sharing the utilization of data with each other, in one or the other access, without limitation. [43].

![Fig 2. Challenges of IoT Security](image)

III. SYSTEMATIC LITERATURE REVIEW PROTOCOL

In this section shows the literature review which is focused on the eligible studies and review more than 200 papers and discuss how to filter out the numbers of papers from 2018 to 2020. The contributions of the qualitative research paper comparative of literature review papers and selected the security issues related papers of IoT devices is security. This study provides a detailed view of IoTs challenges introduced ongoing literature and which is related to the research work.

The searches by information which are related to the several privacy and security issues in the IoT from January 2018 to
December 2020. This study concentrates in the different electronic databases such as Google Scholar, Springer, IEEE, ACM, Research Gate and MDPI. This study searched 194 research papers out of which 174 papers is removed due to duplication of topic. In the screening, the titles and modified works, a sum of 111 papers were inspected in detail. However, 69 papers were related to the privacy and security based. The summarized in the PRISMA flow diagram Figure [3].
Fig: 3. PRISMA diagram of IoT security review
IV. RESULTS & DISCUSSION

In this section, we describe the results of the literature review on IoT privacy and security which includes studies that have numerical values of data in IoT security threats using graphical representation. The tabulated format shows facts about the challenges of IoT from 2018 till 2020 the fields are reference no., year, and several issues of IoT. The graphical representation numeral each of the challenges facing IoT in a different era which is shows by using a Pie chart.

A. Research synthesis using the graphical and tabular form 2018 till 2020

We distribution of paper by IoT security threats in January 2018 to December 2020, during research synthesis we found application domains of IoT security issues, numbers of papers and citations which is shown in the Tabular analysis of IoT security threats in past Table 1 and Figure 4.

### Table 1

<table>
<thead>
<tr>
<th>Ref. No.</th>
<th>Year</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Authenticity</th>
<th>Authorization</th>
<th>Data Security Privacy</th>
<th>Data Availability</th>
<th>Nonrepudiation</th>
<th>Access Control</th>
<th>Inter-operability</th>
</tr>
</thead>
<tbody>
<tr>
<td>[44]</td>
<td>2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[43]</td>
<td>2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[31]</td>
<td>2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[30]</td>
<td>2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[45]</td>
<td>2018</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[46]</td>
<td>2019</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[47]</td>
<td>2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[48]</td>
<td>2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[24]</td>
<td>2018</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[39]</td>
<td>2019</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[38]</td>
<td>2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[49]</td>
<td>2018</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[21]</td>
<td>2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[50]</td>
<td>2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[51]</td>
<td>2018</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[52]</td>
<td>2018</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[53]</td>
<td>2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[54]</td>
<td>2019</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[55]</td>
<td>2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[40]</td>
<td>2019</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[56]</td>
<td>2018</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[57]</td>
<td>2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[58]</td>
<td>2018</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[59]</td>
<td>2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[60]</td>
<td>2019</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[41]</td>
<td>2019</td>
<td>√</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[61]</td>
<td>2018</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[42]</td>
<td>2019</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[62]</td>
<td>2018</td>
<td>√</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[63]</td>
<td>2018</td>
<td>√</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[64]</td>
<td>2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[65]</td>
<td>2018</td>
<td>√</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[66]</td>
<td>2019</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[67]</td>
<td>2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[68]</td>
<td>2019</td>
<td>√</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[69]</td>
<td>2018</td>
<td>√</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[70]</td>
<td>2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[71]</td>
<td>2018</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[72]</td>
<td>2018</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[73]</td>
<td>2018</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[74]</td>
<td>2018</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[75]</td>
<td>2019</td>
<td>√</td>
<td>√</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[76]</td>
<td>2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[77]</td>
<td>2018</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[78]</td>
<td>2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[79]</td>
<td>2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[80]</td>
<td>2020</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[36]</td>
<td>2020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[81]</td>
<td>2020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[82]</td>
<td>2020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[83]</td>
<td>2020</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[84]</td>
<td>2020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[85]</td>
<td>2020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[86]</td>
<td>2020</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[87]</td>
<td>2020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[88]</td>
<td>2020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[89]</td>
<td>2020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[90]</td>
<td>2020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[91]</td>
<td>2020</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[92]</td>
<td>2020</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[93]</td>
<td>2020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[94]</td>
<td>2020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[95]</td>
<td>2020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[96]</td>
<td>2020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[97]</td>
<td>2020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Fig. 4 shows the graphical representation of total number of papers from 2018 to 2020 era addressing each IoT security issue. It can be observed that “data privacy”, “confidentiality” and “integrity” with 31, 13 and 13 papers respectively and authenticity and data availability with 12 and 8 papers respectively were discussed. The most discussing security issues in the past. “Non-repudiation”, “authorization” and “inter-operability” with 1, 7 and 9 papers respectively are the least discussed IoT security issues in past era.

**Graphical Representation**

![Graphical Representation]

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

V. **Comparative Analysis**

The comparative analysis this distribution of paper by IoT security threats in 2018, 2019 and 2020.

A. **Confidentiality**

Figure 10 show the comparative study of IoT challenges with respect to confidentiality issue in 2018, 2019 and 2020 (see figure 5).
B. Integrity
Figure 11 show the comparative study of IoT challenges with respect to Integrity issue in 2018, 2019 and 2020 (see figure 6).

C. Authenticity
Figure 12 show the comparative study of IoT challenges with respect to Authenticity issue 2018, 2019 and 2020 (see figure 7).

D. Authorization
Figure 13 show the comparative study of IoT challenges with respect to Authorization issue in 2018, 2019 and 2020 (see figure 8).

E. Data Security and Privacy
Figure 14 show the comparative study of IoT challenges with respect to data security and privacy issue in 2018, 2019 and 2020 (see figure 9).
**Graphical Representation**

**Data Privacy**

- 2018: 49%
- 2019: 23%
- 2020: 28%

**Nonrepudiation**

- 2018: 0%
- 2019: 0%
- 2020: 0%

**Fig: 9. Distribution of paper with respect to data security and privacy issue**

**Fig: 11. Distribution of paper with respect to nonrepudiation issue**

**Availability**

Figure 15 show the comparative study of IoT challenges with respect to Availability issue in 2018, 2019 and 2020 (see figure 10).

**Graphical Representation**

**Data Availability**

- 2018: 50%
- 2019: 33%
- 2020: 17%

**Access Control**

- 2018: 62%
- 2019: 23%
- 2020: 15%

**Fig: 10. Distribution of paper with respect to availability issue**

**Fig: 12. Distribution of paper with respect to access control issue**

**Nonrepudiation**

Figure 16 show the comparative study of IoT challenges with respect to Nonrepudiation issue in 2018, 2019 and 2020 (see figure 11).

**Access Control**

- 2018: 62%
- 2019: 23%
- 2020: 15%

**Fig: 11. Distribution of paper with respect to nonrepudiation issue**

**Fig: 12. Distribution of paper with respect to access control issue**

**H. Access Control**

Figure 17 show the comparative study of IoT challenges with respect to Access Control issue in 2018, 2019 and 2020 (see figure 12).

**Graphical Representation**

**Interoperability**

Figure 18 show the comparative study of IoT challenges with respect to data security and privacy issue in 2018, 2019 and 2020 (see figure 13).

**Graphical Representation**
VI. CONCLUSION

IoT is an emerging technology that has requirements to progress in the privacy and security area. In this paper, we have studied the comparison among the principle critical issues facing the IoT regarding security and privacy concerns. The IoT faced the several of critical issue in privacy and security. The review provided with this survey, Comparative analysis emerges different issues and focuses on research guidelines in the IoT security domain This paper has done the review of the last 3 years from 2018-2020 to focus on different security challenges in IoT and then analyzed and identified issues with respect to this era. It has been identified that “data security and privacy”, “integrity” and “confidentiality are the most discussed security issues whereas “non-repudiation”, “authorization” and “access control” are least discussed.

REFERENCES


[34] S. S. Basu, S. Tripathy, and A. R. Chowdhury, “Design challenges and security issues in the Internet of Things,”...


