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

1-Imran, 1,4-Syed Mubashir Ali, 1,3-Muhammad Mansoor Alam and 1-Mazliham Mohd Su’ud

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
3Riphah International University, Rawalpindi, Pakistan
4College of Computing and Information Sciences, Karachi Institute of Economics and Technology, Karachi, Pakistan

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.
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

<table>
<thead>
<tr>
<th>Layer</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application layer</td>
<td>Data access, authenticity, data protection,</td>
</tr>
<tr>
<td></td>
<td>data privacy, authorization and availability</td>
</tr>
<tr>
<td></td>
<td>vulnerabilities</td>
</tr>
<tr>
<td>Network layer</td>
<td>DoS, Eavesdropping/Sniffing, Routing Attacks</td>
</tr>
<tr>
<td>Perception layer</td>
<td>Node capture, DoS attack, Sybil attack</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>REF #</th>
<th>Contribution (past)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Farooq et al. (2015)</td>
<td>Prospective vulnerabilities and discrepancies in IoT</td>
</tr>
<tr>
<td>Hossain et al. (2015)</td>
<td>Addressing security and frame works related designs in IoT.</td>
</tr>
<tr>
<td>Andrea et al. (2015)</td>
<td>The investigation of security issues, Challenges and open issues in IoT</td>
</tr>
<tr>
<td>Alsaa and Tubaisht (2015)</td>
<td>To evaluate IoT services in terms of security challenges</td>
</tr>
<tr>
<td>Amadeo et al. (2016)</td>
<td>IoT contemplation in field of various patterns utilization.</td>
</tr>
<tr>
<td>Basu et al. (2015)</td>
<td>Presenting security challenges related to IoT.</td>
</tr>
<tr>
<td>Singh and Singh (2015)</td>
<td>The Network security related vulnerabilities in IoT</td>
</tr>
<tr>
<td>Alaba et al. (2017)</td>
<td>The security configuration related discrepancy in IoT</td>
</tr>
<tr>
<td>Kolias et al. (2016)</td>
<td>The shortcomings in security of IoT middleware devices.</td>
</tr>
<tr>
<td>Billure et al. (2015)</td>
<td>Review about the IoT applications and their issues</td>
</tr>
<tr>
<td>Perera et al. (2015)</td>
<td>To assess the security examination of rising IoT with Marketplace</td>
</tr>
<tr>
<td>Riazul Islam et al. (2015)</td>
<td>The overview of an extensive in the health care area utilizing IoT</td>
</tr>
<tr>
<td>Sadeghi et al. (2015)</td>
<td>Review the security and protection challenges in IoT</td>
</tr>
<tr>
<td>Breivold and Sandstrom (2015)</td>
<td>Assess the security, protection and trust in IoT</td>
</tr>
<tr>
<td>Nalbandian (2015)</td>
<td>Apprise weak compliance research papers in IoT</td>
</tr>
<tr>
<td>Zaslavsky and Georgakopoulos (2015)</td>
<td>Analyze the challenges and front line and its answers in web-scale sensor</td>
</tr>
<tr>
<td>Granjal et al. (2015b)</td>
<td>Information Management and Mobile Analytics using IoT</td>
</tr>
<tr>
<td>Pescatore and Shpanzer (2014)</td>
<td>The present status of various security issues with respect to IoT</td>
</tr>
<tr>
<td>Gil et al. (2016)</td>
<td>Review to making sure the IoT security</td>
</tr>
<tr>
<td>Ouaddah et al. (2017)</td>
<td>Address short comings in IoT security and protection.</td>
</tr>
<tr>
<td>Tzounis et al. (2017)</td>
<td>Security and protection suggestions for IoT</td>
</tr>
<tr>
<td>Mosenia and Jha (2016)</td>
<td>The Privacy and Security concerns in Wearable and IoT gadgets</td>
</tr>
<tr>
<td>Yaqoob et al. (2017a)</td>
<td>Discuss about the Taxonomy of security assaults for IoT</td>
</tr>
<tr>
<td>REF #</td>
<td>CONTRIBUTION (PRESENT)</td>
</tr>
<tr>
<td>Conti et al. (2018)</td>
<td>Portray the new interoperability, the executives and Security Challenges in IoT</td>
</tr>
<tr>
<td>Riahi Sfar et al. (2018)</td>
<td>Assess the security different difficulties of the IoT</td>
</tr>
<tr>
<td>Adat and Gupta (2018)</td>
<td>The Recent Advances, Taxonomy, Requirements and Open Challenges for IoT Architecture</td>
</tr>
<tr>
<td>Khanna and Kaur (2019)</td>
<td>Examine the interferences to the utilization of farming, late advances and future difficulties for IoT</td>
</tr>
<tr>
<td>Miloslavskay and Tolstoy (2019)</td>
<td>The point of the various security issues and its solutions and future headings</td>
</tr>
<tr>
<td>Hameed et al. (2019)</td>
<td>Assess the security challenges for cutting edge systems for IoT</td>
</tr>
<tr>
<td>Ali et al. (2019)</td>
<td>Review the innovations, applications and difficulties of IoT</td>
</tr>
<tr>
<td>Sissini et al. (2018)</td>
<td>Overview the safe steering for IoT</td>
</tr>
<tr>
<td>Sun et al. (2018)</td>
<td>The review of various skills, issues and Prospects in IoT for Smart Healthcare</td>
</tr>
<tr>
<td>Nord et al. (2019)</td>
<td>The point of the data-driven systems for IoT difficulties and openings</td>
</tr>
<tr>
<td>Sha et al. (2018)</td>
<td>The survey of product characterized remote systems administration openings and difficulties for IoT</td>
</tr>
<tr>
<td>Grammatikis et al. (2019)</td>
<td>Review the open issues incorporation of distributed computing with IoT</td>
</tr>
<tr>
<td>Atlam et al. (2018)</td>
<td>Discuss and review the dependent on setting careful managements for IoT</td>
</tr>
<tr>
<td>Hua et al. (2019)</td>
<td>Overview the security of IoT</td>
</tr>
<tr>
<td>Mendez Mena et al. (2018b)</td>
<td>Evaluate the various challenges of IoT</td>
</tr>
<tr>
<td>Forsstrom et al. (2018)</td>
<td>Assess the issues and new research frontiers in the field of IoT</td>
</tr>
<tr>
<td>REF #</td>
<td>CONTRIBUTION (FUTURE)</td>
</tr>
<tr>
<td>Stoyanova et al. (2020a)</td>
<td>The Challenges and new endeavors for the inclusion of IoT security and legal sciences</td>
</tr>
<tr>
<td>Song et al. (2020)</td>
<td>Review the top benefits and challenges of IoT and Data Analytics in Agriculture</td>
</tr>
<tr>
<td>Khadam et al. (2020)</td>
<td>Review and guide for security challenges in the IoT</td>
</tr>
<tr>
<td>Perera et al. (2020)</td>
<td>The issues, difficulties, scientific classification and design security in IoT.</td>
</tr>
<tr>
<td>Hossain et al. (2020)</td>
<td>Survey the Blockchain-based Secure IoT Control Scheme.</td>
</tr>
<tr>
<td>Mbarek et al. (2020)</td>
<td>The assessment researches the action towards Secure IoT Communication with Smart Contracts in a Blockchain Infrastructure</td>
</tr>
<tr>
<td>Basahel and Yamin (2020)</td>
<td>The effect on security issues and open issues in IoT</td>
</tr>
<tr>
<td>Hamad et al. (2020)</td>
<td>The investigation to finds the issues of the guide for security challenges in the IoT</td>
</tr>
<tr>
<td>Berger et al., 2020</td>
<td>The investigation reviews how taxonomy, challenges and practice for IoT security and vulnerabilities</td>
</tr>
</tbody>
</table>
Table 3: IoT security issues in the past

<table>
<thead>
<tr>
<th>Issues/Era</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>Gaikwad et al. (2015; Hossain et al., 2015; Andrea et al., 2015; Alsaadi and Tab-a, 2015, Riazul Islam et al., 2015; Pescatore and Shpantzer, 2014; Ambornhara and Kenen, 2015; Sicari et al., 2015, Vasilomanolakis et al., 2015; Weber, 2015, Mahmoud et al., 2015a)</td>
<td>(Weber and Boban, 2016)</td>
<td>Alaba et al. 2017; Ouaddah et al., 2017; Moseina and Jha, 2016)</td>
</tr>
<tr>
<td>Integrity</td>
<td>Gaikwad et al. (2015; Hossain et al., 2015; Andrea et al., 2015; Basa et al., 2015, Billurota, 2015; Riazul Islam et al., 2015; Breivold and Sandstorm, 2015; Ambornhara and Kenen, 2015; Mahmoud et al., 2015a)</td>
<td>Gil et al. (2016; Elkodhr et al., 2016; Weber and Boban, 2016)</td>
<td>Alaba et al. 2017; Ouaddah et al., 2017; Moseina and Jha, 2016, Yaqoob et al., 2017b)</td>
</tr>
<tr>
<td>Authenticity</td>
<td>Gaikwad et al. (2015; Hossain et al., 2015; Andrea et al., 2015; Riazul Islam et al., 2015; Pescatore and Shpantzer, 2014; Ambornhara and Kenen, 2015; Sicari et al., 2015; Vasilomanolakis et al., 2015; Mahmoud et al., 2015; Granjal et al., 2015a)</td>
<td>Elkodhr et al. (2016; Gupta and Shukla, 2016; Sood et al., 2015)</td>
<td>(Alaba et al., 2017)</td>
</tr>
<tr>
<td>Authorization</td>
<td>Farooq et al. (2015; Riazul Islam et al., 2015; Ambornhara and Kenen, 2015; Vasilomanolakis et al., 2015)</td>
<td>Gupta and Shukla (2016)</td>
<td>Alaba et al. 2017; Ouaddah et al., 2017</td>
</tr>
<tr>
<td>Data security privacy</td>
<td>Gaikwad et al. (2015; Andrea et al., 2015)</td>
<td>(Amadeo et al., 2016; Kolias et al., 2016; Gil et al., 2016)</td>
<td>(Hussain, 2017, “Evolving privacy: From sensors to the Internet of Things,“ 2017), (Ouaddadh et al., 2017), (Tzounis et al., 2017), (Moseina and Jha, 2016), (Yaqoob et al., 2017a), (Yaqoob et al., 2017b), (Risteska Stokoska and Trivodaliev, 2017), (Adlam et al., 2017), (Guarda et al., 2017), (Baker et al., 2017), (Mehmood et al., 2017)</td>
</tr>
<tr>
<td>Availability</td>
<td>Gaikwad et al. (2015; Hossain et al., 2015; Andrea et al., 2015; Singh and Singh, 2015, Riazul Islam et al., 2015; Breivold and Sandstorm, 2015; Ambornhara and Kenen, 2015; Vasilomanolakis et al., 2015; Mahmoud et al., 2015)</td>
<td>(Shah and Yaqoob, 2016)</td>
<td>Ouaddah et al. 2017; Moseina and Jha, 2016</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>Hossain et al. (2015; Riazul Islam et al., 2015; Vasilomanolakis et al., 2015)</td>
<td>(Shah and Yaqoob, 2016)</td>
<td>(Moseina and Jha, 2016)</td>
</tr>
<tr>
<td>Access control</td>
<td>Hossain et al. (2015; Andrea et al., 2015, Pescatore and Shpantzer, 2014; Sicari et al., 2015, Granjal et al., 2015a; Granjal et al., 2015a)</td>
<td>Gil et al. (2016)</td>
<td>Alaba et al. 2017</td>
</tr>
</tbody>
</table>

Table 4: IoT security issues in the present era

<table>
<thead>
<tr>
<th>Issues/Era</th>
<th>2018</th>
<th>2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>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)</td>
<td>Khanna and Kaur (2019; Hameed et al., 2019, Al-Sharekh and Al-Sharekh, 2019, Njord et al., 2019; Grammatikis et al., 2019; Hou et al., 2019; Chen et al., 2019)</td>
</tr>
<tr>
<td>Integrity</td>
<td>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; Fakhr and Mitijarsa, 2018; Choi et al., 2018; Yu et al., 2018)</td>
<td>Alamri et al., 2019; a-Shqeerat, 2019; Nord et al., 2019; Grammatikis et al., 2019)</td>
</tr>
<tr>
<td>Authenticity</td>
<td>Conti et al. (2018; Chen et al., 2018, Ali et al., 2018; Mendez Mena et al., 2018b; Choi et al., 2018; Yu et al., 2018; Agrawal et al., 2018; Das et al., 2018)</td>
<td>Alamri et al., 2019; Al-Sharekh and Al-Sharekh, 2019, Ali et al., 2019; Grammatikis et al., 2019; Hou et al., 2019; Mohamed Noor and Hassan, 2019)</td>
</tr>
</tbody>
</table>
| 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-Sharekh, 2019, Yaqoob et al., 2019; Nord et al., 2019; Grammatikis et al., 2019; Hou et al., 2019; Mohamed Noor and Hassan, 2019;
Discussed various remedies situations awareness capabilities after which they have segregated the reviewed articles with respect to IoT layers, an analytical model is different from ours as they have 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

**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

doi.org/10.1109/ICASSP.2018.8462513

doi.org/10.1016/j.jnca.2016.03.006


doi.org/10.1007/978-3-030-24513-9_12

https://arxiv.org/abs/1901.07309

doi.org/10.14569/IJACSA.2018.091070

doi.org/10.1109/W-FiCloud.2016.24

doi.org/10.1109/WCNC.2018.8377385


doi.org/10.1109/AECT47998.2020.9194197

doi.org/10.1109/MNET.2016.7437030

doi.org/10.1109/ISCC.2015.7405513

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


doi.org/10.1109/ACCESS.2017.2775180

doi.org/10.1016/j.dcan.2017.10.006

http://abmjournals.org/index.php/jhpm/article/view/26

doi.org/10.1109/TENSYMP.2015.25

doi.org/10.1016/j.cose.2020.101790

1040


