Systematic Review of Internet of Things Security

Amiruddin Amiruddin\textsuperscript{1,2}, Anak Agung Putri Ratna\textsuperscript{1}, and Riri Fitri Sari\textsuperscript{1}

\textsuperscript{1}Faculty of Engineering, Universitas Indonesia, Depok, Indonesia
\textsuperscript{2}Sekolah Tinggi Sandi Negara, Bogor, Indonesia

\textbf{Abstract}: The Internet of Things has become a new paradigm of current communications technology that requires a deeper overview to map its application domains, advantages, and disadvantages. There have been a number of in-depth research efforts to study various aspects of IoT. However, to the best of our knowledge, there is no literature that have discussed specifically and deeply about the security and privacy aspects of IoT in recent three years. To that end, this paper aims at providing a comprehensive and systematic review of IoT security based on the most recent literature over the past three years (2015 to 2017). We studied IoT security research based on the research objectives, application domains, vulnerabilities/threats, countermeasures, platforms, proto-cols, and performance measurements. We also provided some security challenges for further research.

\textbf{Keywords}: Internet of Things, protocol, security, systematic review, vulnerabilities.

1. Introduction

Internet of Things (IoT) was first introduced by British technology pioneer Kevin Ashton in 1999, describing a system with physical objects in the real world with the help of sensors connected to the Internet. IoT is an internetworking of physical objects such as sensors, actuators, personal computers, software, intelligent devices, automobile, and network connectivity that enable them to collect and exchange data without human intervention. The emergence of IoT has led to extensive interconnections between people, services, sensors and objects. IoT has been applied in many areas such as smart grids, smart homes, smart transportations, smart cities, smart healthcare, smart metering, and smart energy management.

The side-effect of IoT’s rapid development is the drastic increase in the possibility of threats and security attacks against objects or individuals [1] as a consequence of the connection of so many objects without security guarantees [2]. IoT security is currently a hot research topic for academia, industry, and government. Several research studies have been undertaken to discover and classify potential threats to IoT [3] and its solutions as in [4], but these studies were inadequate, touching only a few aspects or domains. Therefore, in this study we sought to more comprehensively review the security of IoT based on recent literature form the year 2015 to 2017.

Our research contributions are: providing a survey methodology that is general and easy to understand. Our methodology adopted the Jorgensen’s survey methodology [5]; providing a comprehensive description on IoT security based on recent literature; and providing future research challenges on IoT security.

This research adopted a methodology used by Jorgensen [5] in conducting a systematic review on software development cost estimation. Despite different research topics, that method can be adopted for use in conducting systematic reviews devoted to IoT security. Our research methodology consists of 5 stages, started from Define, Identify, Classify, Analyze, and ended up with Report (DICARe). The explanation of each step is as follows:

1. Define. The stage determines the criteria of the reviewed papers, i.e. topic and / or subtopics and time ranges. The topic we selected was IoT or cryptographic, whereas the time span is 2015 to 2017. Given the rapid changes occurring in IoT technology, this time span was considered appropriate. So our survey focused on published papers within the last three years.

2. Identify. This phase is to identify papers written in English that match the topic and or subtopics that have been determined in the previous stage. The way of identification is done by assessing the title, abstraction, keywords, and conclusions of the paper.

3. Classify. The stage of grouping or mapping problems on a paper based on a particular approach. In this survey we used IoT Security as the theme, and provided classification based on application domain, vulnerabilities/attacks, counter-measures, platforms, protocols, and performance measurements.

4. Analyze. The stage of analyzing the results of grouping or mapping that has been done in the previous stage.

5. Report. The reporting stage of the survey results may include the findings, the advantages or benefits or the disadvantage of the research results you submit your paper print it in two-column format.

2. Related Works

In this section we described the results of the literature review on IoT security including application domains, vulnerabilities / threats, countermeasures, platforms and protocols used, and performance measurement.

2.1 Application Domains of IoT Security

The IoT has a wide and diverse application field. Thus, we considered to map briefly the areas where IoT security has been applied based on the current literature. We found application domains of IoT security as follows: ambient assisted living [6], approximate computing [7], big data [8, 9], smart building [1], smart city [10], cloud service [11-15], edge computing [16], energy [1], environmental monitoring [1] [17, 18], fog computing [19, 20], general [21-39], general sensing [2, 40-46], healthcare [1, 40, 41, 47-58], smart home [10, 40, 51, 59, 60], industrial [33], mobile service [59], Personal Area Networks (PAN) [2, 56, 61], production management [1, 18, 62], radio access [63], smart grid [51, 64], transportation [1, 47, 51], universal [65].
We can see in Figure 1 that the top five fields where IoT security have been paid more attention are general (24%), healthcare (19%), general sensing (10%), home (6%), and cloud service (6%). This reflects the potential market of IoT security. However, based on this, we can see that some new application domains of IoT security e.g. radio access, industrial, big data, and approximate computing, have not get enough researcher's attention. Therefore, it can be the next research target.

2.2 Vulnerabilities/Threats of IoT Security

Along with technology advances, there are always security challenges. IoT security vulnerabilities or threats range on wide surface as follows: access control [19, 22, 66-68], bad output [69], brute force [21, 70], cloud attacks [71], computation overhead [33, 72, 73], cryptanalysis [64, 74], cryptography [2, 56, 75, 76], data attacks [1, 18, 19, 22, 47, 49, 51, 53, 62, 67, 77-81], development attacks [45, 52, 69, 75, 76, 82, 83], device attacks [1, 7, 24, 50, 54, 55, 62, 66, 67, 69, 70, 77, 80, 84-86], disruption [2, 47, 51, 69, 86-88], Denial of Service [1, 2, 48, 49, 51, 66, 77, 80, 87-90], eavesdropping [2, 40, 47, 51, 62, 79] [88], firmware attacks [70, 75-77], gateway attacks [12, 66, 80], impersonation [1, 2, 49, 51, 66, 77, 91], key management [22, 70, 88, 92], machine learning [64], malicious code [20, 76, 77] [86, 88], MITM [19, 22, 66, 88], network attacks [1, 21, 51, 68, 70, 75, 80, 93], node attack [1, 2, 40, 43, 47, 80], password issues [22, 66], performance [10], physical attacks [1, 67, 68, 75, 94], quantum computing [95], replay [51, 62, 66, 80, 89], resource attacks [2, 44], social context [59], software management [19, 67, 70, 77, 96], storage attacks [1, 19, 68, 97], surveillance [1, 2, 62, 79], unauthorized attacks [47] [1, 23, 78], user manipulation [60, 77].

As we can see in Figure 2, the main vulnerabilities/threats that have been paid more attention to deal with in IoT security research are device attacks (10%), data attacks (9%), Denial of Service (DoS) (8%), eavesdropping (4.4%), disruption (4.4%), network attacks (4.4%) and development attacks (4.4%). However, there are several new types of vulnerabilities or attacks that have not been widely studied and discussed in literature such as social context which can be used for social engineering, quantum computing that can be used to easily break modern cryptographic algorithms, machine learning to direct targeted individuals or information, and bad output that can be used as entry point of analysis. Thus, those can be interesting to investigate in the future.

2.3 Countermeasures on IoT Security Threats

The Countermeasures on IOT security vulnerabilities are varied and depend on many aspects such as the type of application and protocol used as follows: access control [20, 67, 74, 77, 78, 85, 92], aggregation & correlation [97], anti-malware [70, 77], architecture [24, 48, 53, 82, 85], authentication & authorization [6, 19, 20, 23, 48, 55, 62, 64,
66, 70, 78, 82, 84, 85, 92, 98], automata [93], binary function [42], certificate [11, 20, 68, 77, 82, 83, 92], circuit defense [1, 7], coding [66, 78, 79], configuration [1, 75], context-based [44], elliptic curve cryptography [11, 47, 48, 99] [100], encryption [7, 11, 19, 22, 47, 48, 55, 63, 66, 69, 70, 79, 92, 99-102], forward security [48], framework [12, 18, 44, 45, 54, 60, 76], freshness [48], fuzzy logic [43], game theory [81], general [1, 72], group signature [47], hardware security [99], HARM [40], Hash [21, 47, 66], Homomorphic [47, 78, 79, 97, 101], IPS/IDS [1, 43, 67, 68, 70], isolation [1], key management [6, 22, 67, 69, 73, 78, 92, 102, 103], matrix [42], pairing [86], participatory verification [59], password [22, 75], public key infrastructure (PKI) [20, 78, 92, 100], Privacy Preserving Data Mining (PPDM) [79], product solution [87], Physically Unclonable Function (PUF) [7, 64, 72, 86, 99], Scheduling [63], Software Defined Networks (SDN) [63, 71, 92], secure protocol [22, 41, 48, 49, 72, 77, 84, 85, 91, 96, 104], secure storage [92], signature database [71], signcryption [33, 46, 105], software update [1, 7], standard/policy [1, 76, 79, 80], tagging [1], threat modeling [52, 60], traffic monitoring [71, 75], training [71, 77], trust model [60, 95], virtualization [71], vulnerability analysis [1, 7, 10, 67, 71, 90, 106, 107], watermarking [7], well design [50].

As we can see in Table 1, the top countermeasures that have been proposed by researchers in current literature are encryption (11.4%), authentication and authorization (9%), secure protocol (6%), key management (4.8%), access control (4.2%), certificate usage (4.2%), and security frameworks (4.2%). Unfortunately, due to the variety of countermeasures, our classification of the countermeasures of IoT security attacks are ranging in a large scope which may be overlapping on some cases. However, we hope that this classification will still serve as a useful reference for other researchers. Furthermore, a better classification will be the next research challenge.

Table 1. Countermeasures on IoT Security

<table>
<thead>
<tr>
<th>No.</th>
<th>Countermeasures</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Encryption</td>
<td>11.4</td>
</tr>
<tr>
<td>2</td>
<td>Authentication &amp; authorization</td>
<td>9.0</td>
</tr>
<tr>
<td>3</td>
<td>Secure protocol</td>
<td>6.0</td>
</tr>
<tr>
<td>4</td>
<td>Key management</td>
<td>4.8</td>
</tr>
<tr>
<td>5</td>
<td>Access control</td>
<td>4.2</td>
</tr>
<tr>
<td>6</td>
<td>Certificate</td>
<td>4.2</td>
</tr>
<tr>
<td>7</td>
<td>Framework</td>
<td>4.2</td>
</tr>
</tbody>
</table>

As we can see in Table 1, the top countermeasures that have been proposed by researchers in current literature are encryption (11.4%), authentication and authorization (9%), secure protocol (6%), key management (4.8%), access control (4.2%), certificate usage (4.2%), and security frameworks (4.2%). Unfortunately, due to the variety of countermeasures, our classification of the countermeasures of IoT security attacks are ranging in a large scope which may be overlapping on some cases. However, we hope that this classification will still serve as a useful reference for other researchers. Furthermore, a better classification will be the next research challenge.

2.4 Platforms of IoT Security

We found several platforms used, discussed, or proposed in current literature of IoT security such as Midgar [21], Kaa [84], SicsthSense, SecureSense [11], OpenIoT [78], Midgar, Xively, Exosite, SensorCloud, Etheros, Thingsworx, Carrots, Amazon Web Service, IBM IoT [10], OpenIOT, Hydra, GSN, Ptolemy Assessor Host [108] and are summarized in Figure 3. In fact, there are several other platforms discussed in literature other than the literature we have discussed in this paper (range from year 2015 to 2017). Further investigation on the platforms used in IoT security and classification based on open or proprietary platform is necessary. Thus, it can be a useful insight for other researchers especially for those who have difficulty in the use of proprietary platforms.

2.5 Protocols of IoT Security

Based on current literature, we found several protocols used, discussed, improved, or proposed as follows: TLS/DTLS, MQTT [8, 59, 102, 109], DDS [8], ZigBee [110], HTTP/HTTPS [70], XMPP [109], LoRaWAN [89], 802.15.4 [41]. Figure 4 presents protocols of IoT security found on the current literature.

Figure 3. Platforms of IoT Security

2.6 Performance Measurements of IoT Security

We found several metrics of performance measurement of IoT security in current literature such as follows: Security cost, processing time [21], Data evaluation: timeliness, completeness, accuracy, precision [22], delay time [84], Transmission overview, communication latency, data header, run time, energy consumption, required memory [48, 111], theoretical evaluation, empirical evaluation [97], Computation time, additional encryption time [101], Attack probability, attack cost, average time to compromise, average connectivity [40], NIST Statistical Test [102], computational and communication cost, formal verification [66], compression and reconstruction validation [42], low jitter [63]. The types of measurements described in this sub-section as in Figure 5 are considered not sufficient. For example, there is no measurement of the randomness level of an encryption algorithms; and how to measure the performance of IoT security applications in the era of quantum [110] computing. IoT security measurements performed by [40] are still new.
and can be further investigated to measure their validity.

4. In terms of security measurement, there is no parameter validation used. Some protocols use encryption algorithms in it. However, the data encryption process is not fast because it requires considerable capabilities or resources while IoT devices have limitations on these aspects.

5. The available policy services are still vague in dealing with issues of authorization and authentication.

3.3 Future Research Directions

Based on the findings in previous section, in this Sub-section we provided future research directions on IoT security based on our previous classification as follows:

1. Application domains. We found that some new application domains of IoT security e.g. radio access, industrial, big data, and approximate computing, have not been get enough researches' attention and hence they can be the next research target to extent and expand the use of IoT in human life.

2. Vulnerabilities/attacks. There are several new types of vulnerabilities or attacks found in the literature such as social context, quantum computing, machine learning, and bad output, and these can be interesting to be scrutinized in the future.

3. Countermeasures. Due to the varied types of attacks, there are many countermeasures in IoT applications found in the literature and classification of them is necessary. Our classification of the countermeasures of IoT security attacks still seems to be wide category and some parts may overlap. Thus, a better classification will be a research challenge to provide and enhance understanding of IoT security awareness.

4. Platforms. Further investigation on the platforms used in IoT security and classification based on open or proprietary platform is necessary to provide a useful insight for other researchers especially for those who have difficulty in the use of proprietary platforms.

5. Protocols. There are many protocols in the IoT application, but the protocols most discussed or used for IoT security are CoAP, DTLS, and MQTT. Other protocols can be investigated to find ways to provide or improve IoT security.

6. Performance measurements. There is still a lack in performance measurement of IoT security. For example, in the reviewed literature, there is no measurement of the randomness level of cryptography algorithms. In addition, how to measure the performance of IoT security applications in the era of quantum computing is also a research challenge.

7. Others. Blockchain is a new paradigm of securing distributed implementation of IoT. The integration of blockchain to IoT implementation that can avoid the single point of failure occurring in centralized system become a research challenge to be investigated and realized by the researchers.

4. Conclusions

In this paper, a systematic review of IoT security during last three years (2015 - mid 2017) has been presented.
Classification of IoT security based application domains, vulnerabilities/attacks, countermeasures, platforms, protocols, and performance measurements has also been proposed. Based on the literature study, we highlighted some findings as follows: specific application domain that was widely discussed is healthcare; the most discussed vulnerability/attack is device attack; and the most discussed and proposed countermeasure is the use of encryption. We have also identified some research directions that can be explored in the future.

References


