sensors

MDPI

*Systematic Review*

# Systematic Review of Authentication and Authorization Advancements for the Internet of Things

**Michal Trnka [1], Amr S. Abdelfattah [2], Aishwarya Shrestha [3], Michael Coffey [2] and Tomas Cerny [2,*]**

[1] Department of Computer Science, Faculty of Electrical Engineering, Czech Technical University in Prague, 121 35 Prague, Czech Republic; trnkami1@fel.cvut.cz
[2] Computer Science, Baylor University, One Bear Place 97141, Waco, TX 76798, USA; amr_elsayed1@baylor.edu (A.S.A.); michael_coffey@baylor.edu (M.C.)
[3] Computer Science, University of Wisconsin-Milwaukee, 3200 N Cramer St., Milwaukee, WI 53211, USA; shrest23@uwm.edu
* Correspondence: tomas_cerny@baylor.edu; Tel.: +1-254-710-6838

**Abstract:** Technologies for the Internet of Things (IoT) are maturing, yet no common standards dictate their direction, leaving space for a plethora of research directions and opportunities. Among the most important IoT topics is security. When we design a robust system, it is important to know the available options for facing common tasks related to access control, authentication, and authorization. In this review, we systematically analyze 1622 peer-reviewed publications from October 2017 to December 2020 to find the taxonomy of security solutions. In addition, we assess and categorize current practices related to IoT security solutions, commonly involved technologies, and standards applied in recent research. This manuscript provides a practical road map to recent research, guiding the reader and providing an overview of recent research efforts.

**Keywords:** Internet of Things; authentication; authorization; identity management; survey; security



**Citation:** Trnka, M.; Abdelfattah, A.S.; Shrestha, A.; Coffey, M.; Cerny, T. Systematic Review of Authentication and Authorization Advancements for the Internet of Things. *Sensors* **2022**, *22*, 1361. https://doi.org/10.3390/s22041361

Academic Editor: Charith Perera

Received: 28 November 2021
Accepted: 5 February 2022
Published: 10 February 2022



## 1. Introduction

### 1.1. Background

Internet of Things (IoT) is an environment in which numerous heterogeneous and small devices interact and cooperate. However, the large number of cooperating devices raises numerous problems such as:

- With which participants can data be shared?
- Which participants can be interacted with?
- What is the best way to authenticate participants?
- What is the best way to detect a malicious node?
- What is the best way to introduce a new device into the network?
- What is the best way to retire the device, and when should this be done?

Devices in a network have different software versions, operating systems, and manufacturers and are often owned by different users. For this reason, IoT has become more complicated due to the heterogeneity of the nodes.

Building IoT based on the Internet makes it intrinsically inherent to the security problems from the Internet. In the initial stage of IoT development, security is typically not a significant concern to the users or stakeholders [1]. Security in this stage is often ignored [2] as the industry intends to push IoT to be commercialized as soon as possible. Nevertheless, with the rapid development of IoT, security issues have emerged due to the vulnerability of the nodes and the highly distributed and dynamic features of the underlying networks. Therefore, security is one of the most crucial challenges in the IoT system [3,4].

### *1.2. Motivation and Contribution*

Numerous efforts have been made in IoT security research. Noor et al. published an IoT security survey [5] from a comprehensive viewpoint. While the study provides a wide range of perspectives for authentication and authorization, the survey is limited to the years 2016 to 2018. Our previous work on this topic includes another extensive survey [6] but is also limited to the years 2012 to 2017. The most recent overview of security challenges and their solutions is provided in [7]; however, it does not provide sufficient detail on authorization and authentication. Similarly, another study considers the detail of information security and privacy perspectives in IoT [8]. Continuous authentication methods are then elaborated in [9] through a survey that provides a great overview of the specialized perspective but not a general overview for authorization and authentication. Another prominent study [10] goes through industrial IoT security issues. An overview of the related studies is summarized in Table 1. These publications provide reasonable detail but are limited by years or focus on selected security perspectives or application areas, leaving gaps regarding the following three questions:

(1) What does current IoT authentication and authorization research look like?
(2) What are the common properties of IoT application-layer authentication and authorization solutions?
(3) How can a general researchers grasp the main trend of this area quickly?

**Table 1.** Overview of related work.

| Publication | Published | Summary |
|---|---|---|
| Noor et al. [5] | 2019 | A comprehensive overview of authentication and authorization research for years between 2016 and 2018. |
| Trnka et al. [6] | 2018 | Mapping study for authentication and authorization articles from 2012 to 2017. |
| Chanal et al. [8] | 2020 | Survey providing an overview of architectures, privacy and research challenges, and differences of solutions between domains. |
| Milovlaskaya et al. [7] | 2019 | Great overview of IoT back-end security issues, general hardware, and application security, along with a summary of IoT security management and security standards. |
| Al-Naji et al. [9] | 2020 | Focused survey on continuous authentication methods. |
| Tange et al. [10] | 2020 | Focused survey on industrial IoT security issues. |

This work is concerned with currently available IoT security solutions located at the application layer. Our contributions made in this work consist of two parts:

- We offer a useful roadmap of analyzed and distilled key information from recent 1622 peer-reviewed articles located at major academic sources. Unlike previous surveys and reviews focusing on the specific theme of IoT security, our work provides a blueprint to the general readers without much relevant background working in this area.
- Since the IoT application layer includes application-specific vulnerabilities such as authentication, authorization, identification, data management, and information privacy, we position this systematic review primarily concerning the taxonomy of security solutions, context-aware solutions adopted standards, and the distributed vs. centralized nature of given approaches and specific interactions.

The remainder of this manuscript is structured as follows. The goals of this manuscript are listed in Section 2. The literature identification is explained in Section 3. Resulting publications are categorized in Section 4. Respective research goals are elaborated in Section 5. Threats to validity are discussed in Section 6. Section 7 summarizes achieved goals. Finally, the conclusion of the survey is presented in Section 8.

## 2. Goals

This article presents the most recent findings and trends of IoT authentication, authorization, and identity management. Furthermore, it summarizes research efforts for the years 2017 to 2020, inclusive. This allows other researchers in the given domain to get an overview of the progress in the existing research, learn ideas from other publications, shape research into a broader context, and determine the overall direction of the current scientific efforts.

The benefits are not limited only to the scientific audience. The survey lists the primary research on which future production-ready applications (commercial and open-source) will be based. They will serve a significantly larger community, including users with no technical or scientific background.

This survey aims to answer the following research questions:

RQ1 What is the taxonomy of security solutions?
RQ2 Which topologies, communication types, and perspectives are most dominant in the authentication and authorization IoT research?
RQ3 What are the applicability domains and requirements of identified solutions?

The first goal is to group the research into various categories based on similar properties. The second goal explores architecture decisions that affect (de)centralization of the solution, suitability for machine-to-machine (M2M) and user-to-machine (U2M) communication, and usage of context-aware elements. The third goal evaluates whether the solution is generally applicable or is best for a specific domain, or whether specialized tools are needed to implement it (physical access tokens, cameras, etc.).

## 3. Literature Identification

This systematic review utilizes the following indexing sites to identify evidence: IEEE Xplore, ACM Digital Library (ACM DL), Web of Science (WoS), SpringerLink, and ScienceDirect. Previously published studies [5,6] have proven relevant in the search for scientific evidence and relevant to the review scope but are now dated. We approach this study intending to avoid wheel reinvention. Thus, instead of considering the overall time interval, this study provides an update including publications through the end of 2020. We reuse the same general query from our previous survey review relevancy [6]. It contains an already established, formulated, and tested query, which matches the scope discovered through manual searching, to considered indexing sites. However, we apply current time constraints to integrate recent literature by a complete year. Such an approach warrants continuity across the current study and the previous one.

The considered search query is devised of two distinct parts: the items to include and the items to exclude. We describe target terms and keywords that we expect to find in our results to begin our query. The first keyword that we specify is “Internet of Things” or “IoT”, followed by the term “Security”. These keywords are obvious due to the survey we are conducting; however, there is an enormous amount of research on IoT Security, so we must continue to narrow our search to produce useful results from our query. To constrain our results further, we specify that we only want to include papers with the terms “Authentication”, “Authorization”, “Access Control”, or “Identity” (short for identity management). After specifying what we wanted to find from our query, we added to the query what we wanted to exclude from our results. We excluded papers that discuss security at a low level in the network stack to narrow our search. To accomplish this, we discarded any papers containing the keywords “Network”, “Hardware”, “RFID”, and “protocol”. Furthermore, we are not focusing this survey on “Cryptography”, so we removed any papers with this keyword as well. To end our query, we ensured that our results did not include any surveys by removing all papers with the keywords “Survey” and “Study” in their title.

Due to the differences in the searching procedure found at each site, we turned the query into appropriate forms for each indexer. To promote similarity between indexer results, we manipulated the general query for each individual indexer just enough to get the desired result. We did not want to use queries that were exceedingly different. The

general query, along with the individual queries used for each indexer, is listed in Table 2. Performing these queries returned 1622 results, as detailed in Table 3.

**Table 2.** Queries used for the search.

| Indexer | Query |
|---|---|
| General query | (“Internet of Things” OR “IoT”) AND “Security” AND (“Authentication” OR “Authorization” OR “Identity” OR “Access control”) AND NOT (“Network” OR “Hardware” OR “RFID” OR “Protocol” OR “Cryptography” OR “Survey” OR “Study”) |
| IEEE Xplore | ((“Abstract”: “Internet of Things” OR “Abstract”: “IoT”) AND (“Abstract”: “Authentication” OR “Abstract”: “Authorization” OR documentAbstract: “Identity” OR “Abstract”: “Access Control”) AND “Index Terms”: “Security” AND NOT(“Index Terms”: “Network” OR documentAbstract: “Hardware” OR “Abstract”: “Cryptography” OR “Abstract”: “Protocol” OR “Document Title”: “Survey” OR “Abstract”: “RFID” OR “Document Title”: "Study")) |
| ACM DL | Abstract: (IoT “Internet of Things”) AND Abstract: (“Authentication” OR “Authorization” OR “Identity” OR “Access Control”) AND Title: (-study -Survey) AND Abstract: (-Hardware -rfid -Cryptography) AND Keyword: (-Hardware -Physical -Network) |
| WoS SCIE | TI = (Internet of Things OR IoT) AND TS = (Authentication OR Authorization OR Identity OR Access Control) NOT TS = (Hardware OR Cryptography OR Protocol OR RFID OR Physical OR Network) NOT TS = (Survey OR Study) AND TS = Security |
| SpringerLink | ‘(Authentication OR Authorization OR Identity OR “Access Control”) + title (“Internet of Things” OR IoT)’ |
| ScienceDirect | (“Internet of Things” OR “IoT”) AND (“Authentication” OR “Authorization” OR “Identity” OR “Access control”) AND NOT (“Hardware” OR “Cryptography”) |

**Table 3.** Number of articles processed in the survey.

| Indexer | Results | Prefiltered | Relevant |
|---|---|---|---|
| IEEE Xplore | 442 | 90 | 76 |
| ACM DL | 150 | 43 | 28 |
| WoS | 133 | 56 | 16 |
| SpringerLink | 491 | 6 | 2 |
| ScienceDirect | 406 | 19 | 10 |
| Total | 1622 | 214 | 132 |

To select relevant publications, we established inclusions and exclusion criteria, which we detail below. These criteria are applied to all 1622 results. We proceeded as follows: in the first round of elimination (prefiltering), we considered publication abstract, title, and keyword assessment. When it passed the inclusion and exclusion criteria, we included the publication in the next stage in the next stage. There, we read the full text of the candidate publication and decided whether it was in the scope based on the ability to decode answers for the questions that we raised in this systematic review. The reduction process with relevant publication numbers is detailed in Table 3.

### *3.1. Inclusion and Exclusion Criteria*

The inclusion criteria for the publications can be summarized with the following list:

- Published between October 2017 and 2020 (both inclusive).
- Indexed by either IEEE Xplore, ACM DL, WoS SCIE, SpringerLink, or ScienceDirect.
- Relates to authentication, authorization, identity management, or access control for IoT. In particular, we considered whether the publication proposed a solution to considered topics.

To narrow down the scope, we have also formed exclusion criteria that are applied to the included articles:

- Not written in English.
- Duplicate publication.
- Published before October 2017 (considering our previous survey time scope [6]).
- Less than four pages.

- Could not determine the technical objective (mainly because of poor English).
- Not in the scope of the application layer, i.e., focused on security on the lower level of the network stack.
- Survey or opinion publication without explicit technical contribution.
- Utilized blockchain technology.

Blockchain is excluded from the result not because it does not fall into the scope but rather because of its high prevalence. There were over one hundred articles focused on blockchain technologies for the IoT. To detail the perspective, our previous survey [6] contained only two blockchain articles. This illustrates the massive increase in blockchain-related research. Thus, we do not discuss the differences between blockchain technologies in the scope of a general review due to their similarities from a high-level perspective.

### *3.2. Searched and Filtered Results*

After the queries were run over all indexing services, we were presented with a set of 1622 publications considering inclusion and exclusion criteria from Section 3.1 . We were then able to eliminate one duplicate publication found by the WoS indexer. Finally, we read the abstract of each article and eliminated any publications that did not fit within the scope of this survey, giving us 214 prefiltered candidates.

Upon completion of the filtering process, we read through the remaining publications, categorized them based on the criteria discussed in this survey, and performed property coding detailed in Section 3.3. During this read-through, we were able to remove more articles that at first looked as though they fit our scope but upon further examination were proven unrelated. The complete statistics of publications found, prefiltered, and included for every indexing site can be seen in Table 3. This shows that the indexer, IEEE Xplore, returned 442 total results originally, 90 articles remained after prefiltering, and 76 articles were declared relevant. ACM DL returned 150 results originally; 43 articles remained after prefiltering, and 28 articles were declared relevant. WoS returned 133 results originally; 56 articles remained after prefiltering, and 16 articles were declared relevant. SpringerLink returned 491 results originally; 6 articles remained after prefiltering, and 2 were declared relevant. Finally, ScienceDirect returned 406 articles originally; 19 articles remained after prefiltering, and 10 were declared relevant. The summation of these indexers showed 1622 articles were originally returned; 214 articles remained after prefiltering, and 132 were declared relevant. The survey process-flow is illustrated in Figure 1.

### *3.3. Property Coding*

Each publication that passed through inclusion and exclusion criteria was read full-text with the intent to extract information relevant to this study. If we could not extract the information, we excluded the publication.

We assessed each publication's metadata (i.e., years, conferences, authors, etc.). In the full text, we targeted the target domain, motivations, and goals to categorize the metadata. We determined whether the particular publication topic applies a specific approach in the application layer if it is a context-aware approach for addressed and architectural properties, such as whether the solution tends to be centralized or decentralized . We assessed whether any specific constraints were assumed for the solution and devices and if a special device (i.e., external one) is needed for the considered approach. We also identified where the schema applied to both user-to-machine and machine-to-machine interactions. We compiled all considered publications into a large roster detailed in the taxonomy section based on this coding scheme.

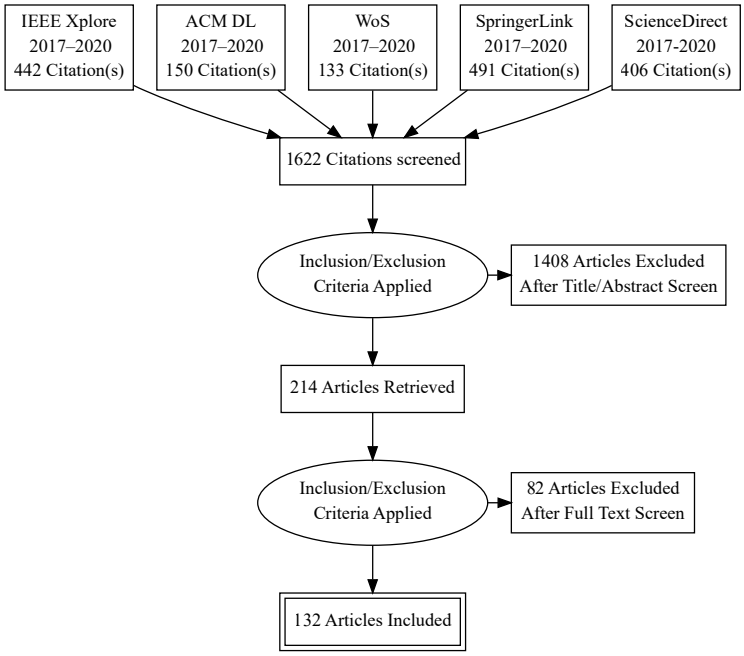


**Figure 1.** Illustration of the survey process-flow inclusion and exclusion of articles.

## 4. Taxonomy and Trends

Categorizing the filtered publications into specific groups is one of the main goals of this survey. This categorization is done with three different taxonomy models; they are described in the following subsections:

1. Years-based Taxonomy.
2. Goals-based Taxonomy.
3. Automation-based Taxonomy.
4. The three-year perspective trends.

### *4.1. Years Based Taxonomy*

This graph projects data in the period of October 2017 till December 2020. Since early 2017, published papers have already been included in the previous survey [6]; the graph starts from October 2017. As represented in Figure 2, the values of the graph show a fair increase in the number of papers regarding this research scope since the last survey we conducted, such that it varies in the range of 30 to 50 papers per year. However, it is noted that the number of papers slightly decreased in 2020, probably because of the appearance of the COVID-19 pandemic that affected most industries and fields then.

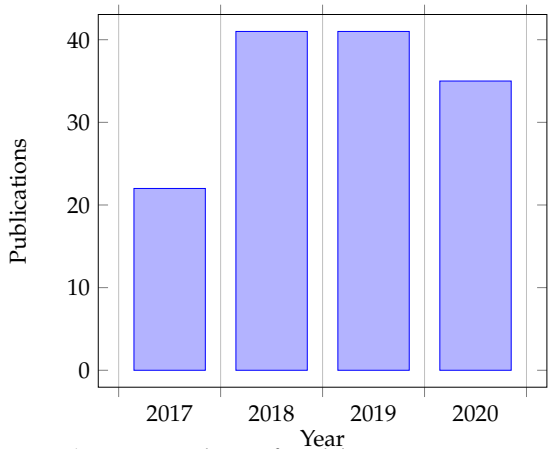


**Figure 2.** Number of publications per year.

### *4.2. Goals-based Taxonomy*

Assigning the filtered papers into specific and predefined categories (as detailed in Section 3.3) is one of the main directions of this article. Therefore, four categories are explored to satisfy the research goals and to answer the research questions mentioned in Section 2. Accordingly, the characteristics of papers are fully surveyed to be classified into the following categories:

1. *Context-awareness (yes/no)*: the ability of a system to gather information about its environment at any given time and adapt behaviors accordingly.
2. *Centralized vs. decentralized network topology (centralized/decentralized/both or N/A)*: the solution topology could require either centralization, decentralization, or combination between such elements.
3. *Communication model (M2M/U2M/both or N/A)*: the different communication methods in terms of the machine-to-machine (M2M) or user-to-machine (U2M), which strictly require some user input information.
4. *Existing vs. new method (existing, new, extension)*: the novelty of the method. It is unusual for solutions to be novel as a whole. It is common to reuse existing technology in novel ways .

These categories are considered common and valuable for most IoT approaches. Therefore, they are individually described in the upcoming sections. One contribution of this survey is the large property coding described in Section 3.3, and it is shared through Tables 4 and 5.

**Table 4.** Selected paper categorization part 1/2.

| References | Context Aware? | Topology (Centr./Distr.) | Communication Model | Existing vs. New | Domains | Constrained/ Unconstrained Devices | Required Special or External Devices |
|---|---|---|---|---|---|---|---|
| Ibrahim et al. [11] | N | C | U2M | Extension | Smart Home | C | Biometric |
| Baruah et al. [12] | N | D | Both | Extension | Industrial IoT Devices | C | Sensor, Router |
| Zulkipli et al. [13] | N | D | M2M | New | General | N/A | - |
| Chen et al. [14] | N | N/A | U2M | Extension | General | C | Biometrics ECG |
| Kashmar et al. [15] | Y | N/A | N/A | Existing | General | N/A | - |
| Karimibiuki et al. [16] | Y | D | Both | Existing | General | U | - |
| Chen et al. [17] | N | Both | Both | Extension | General | U | - |
| Olazabal et al. [18] | Y | C | U2M | Extension | Biometrics | U | - |
| Terkawi et al. [19] | N | N/A | N/A | Extension | General | N/A | - |
| Hoang et al. [20] | Y | C | U2M | Existing | General | N/A | - |
| Cattermole et al. [21] | Y | D | M2M | Existing | General | N/A | - |
| Mathew et al. [22] | Y | C | U2M | Existing | Home security | C | Biometrics |
| Jain et al. [23] | Y | C | Both | Existing | Automated Attendance System | U | Camera |
| Guo et al. [24] | Y | D | U2M | Extension | Fog Computing authentication | C | - |
| Renuka et al. [25] | N | N/A | M2M | Extension | IoT Environment | N/A | - |
| Kim et al. [26] | Y | C | U2M | Existing | General | U | - |
| Felde et al. [27] | N | D | M2M | Extension | Dynamic groups | U | - |
| Mahbub et al. [28] | N | Both | M2M | Existing | General | C | RFID |
| Heydari et al. [29] | N | N/A | U2M | Extension | Fog Computing | N/A | - |
| Ning et al. [30] | N | D | Both | Existing | General | U | - |
| Leung et al. [31] | N | D | U2M | New | General | C | Smart Watch |
| Bilgen et al. [32] | Y | C | U2M | Existing | General | U | - |
| Oh et al. [33] | N | C | Both | New | IoT Platforms | U | - |
| Dammak et al. [34] | N | N/A | Both | Extension | General | C | - |
| Nespoli et al. [35] | Y | D | U2M | Existing | IoT Environments | U | - |
| Rothe et al. [36] | Y | N/A | N/A | New | General | N/A | - |
| Ouaddaha et al. [37] | N | D | N/A | New | General | N/A | - |
| Yan et al. [38] | N | C | Both | Extension | Home security | C | Smart device (Door Lock), Smartphone |
| Chiu et al. [39] | N | C | U2M | Existing | Wearable Devices | C | Wearable brainwave headsets |
| Phoka et al. [40] | N | D | U2M | Existing | Security door | C | IR Sensor |
| Heydaria et al. [41] | N | N/A | N/A | New | General | N/A | - |
| Malarvizhi et al. [42] | N | C | U2M | Extension | Multi-bio authentication | C | Biometric scanners |
| Sharif et al. [43] | N | C | M2M | Existing | Road Construction | N/A | - |
| Ashibani et al. [44] | Y | D | U2M | Extension | Smart Home | C | Sensor |
| Ulz et al. [45] | N | N/A | Both | Existing | General | U | - |
| Gebrie et al. [46] | Y | C | U2M | New | Healthcare and Smart Home | C | Biometrics |

**Table 4.** *Cont.*

| References | Context Aware? | Topology (Centr./Distr.) | Communication Model | Existing vs. New | Domains | Constrained/ Unconstrained Devices | Required Special or External Devices |
|---|---|---|---|---|---|---|---|
| Wang et al. [47] | N | D | Both | Extension | General | U | - |
| Nespoli et al. [48] | Y | C | U2M | Extension | IoT Platforms | C | Security devices, Sensor |
| Ghosh et al. [49] | Y | C | Both | Existing | Home IoT platform or Web service | C | Security devices |
| Gad et al. [50] | N | N/A | U2M | Existing | General | C | - |
| Mbarek et al. [51] | N | C | U2M | Existing | Smart Home | C | - |
| Hasan et al. [52] | Y | D | Both | Extension | General | C | Maxim DS2411 |
| Arfaoui et al. [53] | Y | C | Both | Extension | General | U | - |
| Murphy et al. [54] | N | D | M2M | Extension | General | C | Accelerometers |
| Durand et al. [55] | N | D | M2M | Existing | General | N/A | - |
| Pallavi et al. [56] | N | D | Both | Extension | Fog computing | C | Sensor |
| Saadeh et al. [57] | N | N/A | N/A | Existing | General | N/A | - |
| Carnley et al. [58] | N | D | N/A | Extension | Smartphone Devices | U | - |
| Chifora et al. [59] | Y | C | U2M | Extension | Smart Home | U | - |
| Batool et al. [60] | Y | C | U2M | Existing | Healthcare | C | Electrocardiogram (ECG) |
| Gamundani et al. [61] | N | N/A | N/A | New | Smart Home | N/A | - |
| Chauhan et al. [62] | N | D | U2M | Existing | General | C | Smartphone, Smartwatch, Raspberry Pi |
| Dabbagh et al. [63] | Y | D | Both | Existing | All Wireless devices | U | Biometrics |
| Ali et al. [64] | N | D | U2M | Extension | Healthcare | U | - |
| Wallis et al. [65] | Y | C | M2M | New | General | U | - |
| Krašovec et al. [66] | Y | Both | M2M | Existing | General | C | Sensors |
| Yang et al. [67] | N | C | Both | Existing | Healthcare | C | Sensor |
| Sahoo et al. [68] | N | C | U2M | Extension | General | U | - |
| Zhu et al. [69] | N | D | N/A | Existing | Smart Home | C | - |
| Das et al. [70] | N | C | U2M | Extension | Industrial Internet of Things | C | Biometric sensor |
| R. Khan [71] | N | C | Both | Existing | General | U | - |
| Chien [72] | Y | D | Both | Existing | General | U | - |
| Aski et al. [73] | Y | D | U2M | Existing | Healthcare | U | Raspberry pi |
| Alkhresheh et al. [74] | Y | N/A | Both | Extension | IoT Platforms | C | Raspberry Pi |
| Ethelbert et al. [75] | Y | C | U2M | Extension | Cloud SaaS Applications | U | - |
| Sun et al. [76] | Y | C | U2M | Existing | Wearable Devices | C | Accelerometer |

**Table 5.** Selected paper categorization part 2/2.

| References | Context Aware? | Topology (Centr./Distr.) | Communication Model | Existing vs. New | Domains | Constrained/ Unconstrained Devices | Required Special or External Devices |
|---|---|---|---|---|---|---|---|
| Shayan et al. [77] | Y | C | U2M | Extension | Smart Home | C | Smart phone, Biometrics |
| Elganzoury et al. [78] | N | N/A | U2M | Existing | Mobile banking | U | - |
| Oh et al. [79] | N | D | M2M | Extension | General | C | - |
| Zhou et al. [80] | N | N/A | U2M | Extension | General | U | Brainwave Sensor |
| Oh et al. [81] | N | D | Both | Extension | IoT platforms | C | Sensor |
| Belk et al. [82] | N | C | U2M | Existing | General | U | - |
| Hassan et al. [83] | N | D | U2M | Extension | Wearable Devices | C | Smart phone |
| Kaliya et al. [84] | N | N/A | N/A | Existing | General | U | - |
| Wazid et al. [85] | N | D | U2M | Extension | Medicine validity detection | C | - |
| Shah et al. [86] | Y | N/A | N/A | New | General | N/A | - |
| Amoon et al. [87] | Y | D | M2M | Extension | Any access-control | U | - |
| Yazdanpanah et al. [88] | N | C | M2M | Extension | Wireless Sensor Networks | C | Sensor |
| Barbareschi et al. [89] | N | D | M2M | Extension | Computing Fog | C | - |
| Loske et al. [90] | Y | N/A | N/A | New | General | N/A | - |
| Shahzad et al. [91] | Y | C | Both | Extension | General | U | - |
| Rattanalerdnusorn et al. [92] | Y | D | U2M | Existing | IoT Environments | U | - |
| Prathibha et al. [93] | N | C | U2M | New | Smart Home | U | Biometrics |
| Whaiduzzaman et al. [94] | N | C | U2M | Existing | Fog IoT Environment | U | - |
| Liu et al. [95] | Y | C | M2M | Existing | Smartphone-centric | C | Smartphone |
| El Kalam et al. [96] | N | D | M2M | Existing | General | N/A | - |
| Genç et al. [97] | Y | D | Both | Extension | Smart device | U | - |
| Ashibani et al. [98] | Y | D | U2M | Existing | Smart Home | U | - |
| Bhatt et al. [99] | N | Both | M2M | Existing | General | N/A | - |
| Pal et al. [100] | Y | D | U2M | Existing | Healthcare (only Smartphone Device) | C | - |
| Miettinen et al. [101] | Y | C | M2M | Existing | General | N/A | - |

**Table 5.** *Cont.*

| References | Context Aware? | Topology (Centr./Distr.) | Communication Model | Existing vs. New | Domains | Constrained/ Unconstrained Devices | Required Special or External Devices |
|---|---|---|---|---|---|---|---|
| Lu et al. [102] | Y | C | U2M | Existing | General | C | Biometrics |
| Gupta et al. [103] | Y | C | M2M | Existing | Cars, Vehicles | C | Cars Location Tools |
| Salama et al. [104] | Y | D | U2M | Existing | Healthcare | C | - |
| Blue et al. [105] | Y | D | U2M | Existing | General | C | Microphones |
| Islam et al. [106] | N | D | U2M | Extension | Healthcare | U | - |
| Srinivas et al. [107] | Y | N/A | U2M | Existing | Industrial Internet of Things | C | Smartcard, Biometrics |
| Pal et al. [108] | Y | D | Both | Extension | General | U | - |
| Atlamab et al. [109] | N | C | M2M | New | General | U | - |
| Khalil et al. [110] | N | D | M2M | Extension | IoT Environments | U | - |
| Djilali et al. [111] | Y | C | Both | Extension | IoT Platforms | U | - |
| Van hamme et al. [112] | Y | C | U2M | Existing | General | N/A | - |
| Schuster et al. [113] | Y | D | M2M | Existing | General | N/A | - |
| Alianea et al. [114] | Y | D | M2M | Extension | Any access-control | U | - |
| Nakouri et al. [115] | N | D | M2M | Extension | Video Surveillance Systems | U | Camera, Fingerprint sensor |
| Ranaweera et al. [116] | N | D | Both | Existing | Multi-access Edge Computing platform | N/A | - |
| Selvarani et al. [117] | N | N/A | N/A | Extension | General | N/A | - |
| Aski et al. [118] | N | D | U2M | Existing | Healthcare | U | Biometrics |
| Ahmed et al. [119] | N | N/A | U2M | Extension | General | U | - |
| Lupascu et al. [120] | Y | D | M2M | Existing | Industrial IoT Devices | C | IoT device/Sensor |
| Krishnan et al. [121] | Y | D | Both | Existing | Controlled IoT device | C | Blockchain, Sensor |
| Jonnada et al. [122] | N | C | U2M | Extension | Remote Collaboration Systems | U | - |
| Gebresilassie et al. [123] | N | D | N/A | Existing | General | N/A | - |
| Martinez et al. [124] | Y | D | Both | Extension | Smart city | C | Smartphone, Smart meter |
| Colombo et al. [125] | Y | C | M2M | Existing | General | N/A | - |
| Rech et al. [126] | N | Both | U2M | Existing | Cross-Domain Service | C | Bluetooth |
| Lee et al. [127] | N | C | M2M | New | General | N/A | - |
| S. Hazra [128] | N | N/A | U2M | Extension | ATM service | C | Biometrics |
| Tandon et al. [129] | Y | D | M2M | Existing | General | U | - |
| Shieng et al. [130] | N | C | M2M | Extension | Smart Home | C | - |
| Xiong et al. [131] | N | D | Both | Extension | IoT Cloud Storage | U | - |
| Wu et al. [132] | N | C | U2M | Extension | Distributed Cloud Computing | U | - |
| Han et al. [133] | Y | C | U2M | Existing | General | U | - |
| Fremantle et al. [134] | N | C | Both | Extension | IoT Platforms | U | - |
| Daoud et al. [135] | N | D | U2M | Existing | Healthcare cloud environment | C | Sensor, ECG |
| Cui et al. [136] | N | D | U2M | Extension | General | U | - |
| Vorakulpipat et al. [137] | Y | C | U2M | Existing | Card reader, finger print reader | C | Cards |
| Li [138] | N | Both | M2M | Existing | General | U | - |
| Gur et al. [139] | Y | D | U2M | Existing | IoT Platforms | C | IHG |
| Gong et al. [140] | N | N/A | M2M | Existing | Smart city | C | Sensor |
| Gwak et al. [141] | N | D | U2M | Existing | General | U | - |
| Chen [142] | Y | D | Both | Extension | Security | C | Sensors |

### *4.3. Automation Based Taxonomy*

To further broaden our categorization, we utilized automated algorithms. In particular, we used the automated algorithms that produced the most common categories among all of the relevant publications. For this process we used *pdftotxt* [143] for transforming the PDF documents into plain searchable text. Then, the *RAKE* [144] algorithm was used for keyword extraction. After that, the extracted keywords were grouped together into 10 major categories. Note that categories are not exclusive in such a process, and one publication can be a member of multiple categories at the same time.

For 12 publications [11–22], no categorization was detected automatically due to generic keywords extracted (i.e., "devices" or "Internet"), which are not closely related to one of the major categories. For these papers, we extracted their keywords manually.

This taxonomy process produces the following eight categories, are shown in Figure 3 with their included number of publications:

1. *Authentication*: [12,23–95]
2. *Context*: [11,14,18,22,23,29,32,35–37,39,41,42,44,48,49,53,57,64,69,70,74,76,80,90,92,96–115]
3. *Services*: [26,33,35,37–41,44,46,48,52,57,65,66,69,72,81,84–87,93,97,98,103,106,107,111,113,116–128]

4. *Authorization*: [13,15–21,32,33,35,37–40,48,49,53,58,59,64,71,74,79,81,91,95,99,103,111,122,126,129,130]
5. *Cloud*: [24,29,37–39,41,56,57,59,60,63,70,71,75,83,85–87,94,95,99,103,117,131–137]
6. *Attributes*: [23,29,32,33,37,49,53,65,74,75,97,99,100,103,104,108,110,111,114,124,125,131,138–140]
7. *Roles*: [32,33,37,65,71,97,100,106,111,120,141,142]
8. *Health*: [85,100,104,106,118,135]

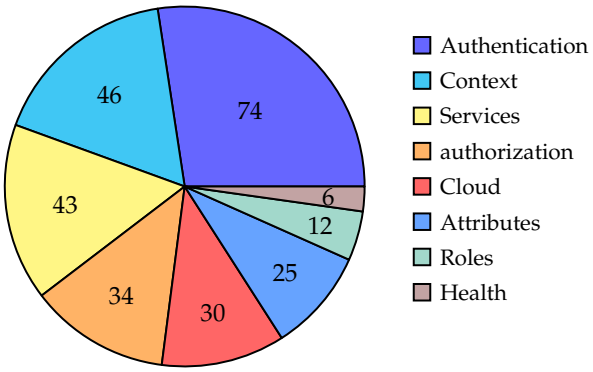


**Figure 3.** Number of articles in each category.

The resulting categories are expected for security IoT research. The major one is *Authentication*, followed by *Context* and *Services*. The first one is closely related to the nature of the IoT solutions with their access to the context, and the second one illustrates distributed nature of those solutions. The top three categories are followed in fairly closed order by *Authorization*, *Cloud*, and *Attributes*, and the two least populous are *Roles* and *Health*. We have included those two only as illustrations for comparison with the previous survey from 2017 [6]. Figure 3 illustrates the categories with respect to the number of included papers.

There are interesting observations, such as that Attribute-Based Access Control (ABAC) [145] has become increasingly popular for security. This is due to its higher flexibility and ability to better describe complex rules. Vice-versa, the Role-Based Access Control (RBAC) [146], is slowly losing its popularity. One other interesting observation is that there are very few healthcare applications. In our last survey [6] from 2017, 14% of the papers were concerned about healthcare. In contrast, now it is only 4.4%.

### *4.4. The Three-Year Perspective Trends*

Compared to our previous survey [6], we can observe trends. We can constantly see high interest in the authentication (51% before vs. 55% now). The second most populous category now is context, which has a share of 35% versus 23% in 3 years ago. Our perspective shows that IoT security research is moving towards solutions that can capitalize on one of the main IoT advantages (inherent access to context). Services have experienced a slight loss in popularity (37% vs. 32%). The authorization research has dropped significantly from 46% to 25%. However, we attribute that to the fact that we have skipped all research related to blockchain solutions in this study. Moreover, in our experience, blockchain is a promising technology to share security rules, and therefore most of the omitted papers would fall into this category. The cloud category does not exhibit any significant popularity changes (19% vs. 22%). Finally, the ABAC, as mentioned above, is getting more popular, with an increase from 14% to 19%. Roles are still a minor topic. The most surprising category is healthcare. There is a notable drop in healthcare solutions. In 2017, 14% of related publications were concerned about healthcare. In contrast, now it is only 4.4%. What was a notable research topic three years ago was identity management and tokens. However, these were not identified for the current publications.

## 5. Details on Goal-Based Taxonomy Perspectives

Goals-based taxonomy is summarized by Tables 4 and 5. We discuss the statistics in the following subsections.

### 5.1. Context-Awareness

Context-awareness in IoT is the ability of a system to gather information about its environment by detecting context entities using various methods, such as collecting data via sensors, smartphones, tablets, wearable devices, smart bands, cameras, microphones, GPS devices, and user input. The collected information can be turned into higher-level knowledge and is useful in various applications. Utilizing this functionality, numerous objects in the environment are monitored, notify the consumer of potentially dangerous situations, provide the ability to communicate with trusted devices, and address eventual accidents. These abilities allow for increased safety, efficiency, and economic benefit for those environments. In this subsection, we first provide the papers that utilize contextual information to achieve security in an IoT environment using authentication and access control techniques, and then we present papers that could meaningfully avail information in various domains and perspectives.

Authenticating a user is paramount when it comes to security. When implemented in conjunction with password-based authentication methods, context-aware authentication systems append an additional security layer. They can replace the conventional authentication methods. For example, in the paper [98], to strengthen authentication security, the author has presented a dynamic authentication model for accessing smart home devices by utilizing traditional credentials with context-aware information. Context-aware authentication is an important characteristic of smart homes. The goal of context-aware authentication systems in smart homes is to provide security services that maximize the user's comfort and safety while minimizing the user's explicit interaction with the environment [46,49,147]. For instance, ref. [35,48,66] utilizes location-based information in authentication framework for smart environment.

The growth of IoT technology presents excellent opportunities but also produces many new challenges related to authentication in IoT devices. Using passwords or pre-defined keys has drawbacks that limit the use of different IoT applications. Thus, authenticating users on password mechanisms is not always feasible. To overcome this issue, some papers focus on different authentication methodologies. For example, one paper implements JSON Web Token (JWT) [148], which is an open standard that uses encoded JSON objects as a payload while transmitting information between two parties [75,119], and Two Microphone Authentication [105], which uses the audio and network channel to authenticate commands. It provides an additional security check against maliciously injected commands.

IoT device authentication is fundamental to ensure the identity of connected devices can be trusted. Alongside authentication, Access Control (AC) provides selective restriction of access to services and data, or for performing a certain operation on a resource, service, or connected object. There are various paradigms of access control mechanisms, which are shifted from fixed desktop to dynamic context-aware environments. Mainstream approaches in access control systems include RBAC [146] and ABAC [145]. For example, to mitigate malicious attacks in IoT environments, the paper [87] uses the Role-Based Reputed Access Control method and achieves device security by tracking the activities of the device based on location. With ABAC, access decisions are made based on attributes (characteristics) about the subject. While RBAC covers broad access [65,111], ABAC can control access on a more detailed level. Several researchers have developed ABAC models that support context-based access control [20,32,104,113,125].

Different types of dynamic context information bring new challenges to access control systems. To improve the classic access control techniques, Alianea and Adda published an extension to the ABAC in the form of the High-Order Attribute-Based Access Control model (HoBAC) [114]. This new model makes it possible to implement IoT AC policies based on hierarchies of entities (objects, subjects, and environment attributes) built using

aggregation operations on the attributes of existing entities. Furthermore, ref. [103] presents additional functionality in which the model not only considers system-wide attributes-based security policies but also takes into account the individual user privacy preferences for allowing or denying services. Additionally, utilization of context information can also be performed in Operation-Based Access (grouping is performed on the basis of operations instead of roles) [97], Event-Based Access Control (only authorized device can send data and initiate the events) [13], Capability-Based Access Control (CBAC) [130], and Hybrid Access Control Model [100] (a combination of RBAC, ABAC, and CBAC, employing attributes, roles, and capabilities). Moreover, in order to improve access control mechanisms, contextual information can also be taken into consideration at the time of trust value verification [108,112].

A context-aware system uses heterogeneous data sources to adapt and provide services to the user according to his needs, his localization, or his interaction with the environment. This results in the ubiquitous source of context data in mobile devices that can provide different services in different contexts—where context is strongly related to a device's location . Due to this, most initial research in context-aware computing focused on location-aware systems. For example, context-based information is utilized from the MAC address of devices that support information such as the owner name or location for user authentication [92]. However, context is more than just location. Biometric data as addressed in [22,92,102] are also considered "contextual" by definition. Contextual data help to obtain the background information and can be used to frame what you know in a larger picture. Moreover, the authors of [28] utilized the contextual data using Radio Frequency Identification (RFID) technology.

In summary, 58 context-aware solutions have been proposed in systems, middleware, applications, techniques, and models [15,16,18,20–24,26,32,35,36,44,46,48,49,52,53,59,60,63,65,66,72–77,86,87,90–92,95,97,98,100–105,107,108,111–114,120,121,124,125,129,133,137,139,142]. The particular works that address context-awareness are shared in Tables 4 and 5. They can be used to address different challenges in IoT. The results in these papers clearly show the importance of context-awareness in the IoT paradigm.

### 5.2. *Distributed vs. Centralized Network Topology*

With IoT systems, we typically expect to follow the decentralized nature of solutions. However, authentication and authorization are sometimes designed with centralism in mind. This leads us to two strategies of security solutions: distributed and centralized.

The *centralized approach* has benefits related to global governance and simplicity. It is easy to control and enforce identical policies across the ecosystem from a single focal point. Moreover, this model allows for migration between non-IoT-based software and that which is IoT-based. However, the drawbacks of this approach include the potential lack of scalability and creating a system bottleneck; this implies potential issues with resilience and a single point of failure. Centralized approaches often consider a component in the middle [95]. This approach seems natural for smart homes [59,77,93,103,130] and cars where the scale does not introduce an issue. However, as apparent from Tables 4 and 5, this is not not always the case [69,98].

In contrast, the *distributed approach* addresses concerns related to resilience and scalability by not relying on a central node for processing. The distributed solution makes individual nodes more responsible for their logic, which limits coupling. However, this approach adds a layer of complexity to the system's synchronization, maintenance, and auditing. It also introduces a new problem, whether devices can be trusted.

Distributed Secure Multi-Party Computation (SMPC) nodes [120] were used to make policy decisions for authentication of devices. These learn device behavior and limits using a distributed registry and assemble a decentralized decision based on the honesty of a device.

In order to produce a scalable, decentralized public key distribution scheme, [55] called for a decentralized, permissionless Public Key Infrastructure (PKI) running on a blockchain. First, it ensures that the public keys belong to the real device and owner

without involving a Trusted Third Party (TTP). Second, it considers an authentication flow to define the process for an entity to grant approval to access a resource.

A History-Based Capability System (HCAP) [129] regulates the order in which permissions are exercised in a distributed authorization environment. HCAP capabilities carry sequencing constraints in the form of security automata. An HCAP works well as a building block suite for centralized policy administration and decentralized policy enforcement.

The rule-attribute-based access control model proposed in [19] targets a distributed environment. It is based on using digitally signed documents or certificates that convey identity, authorization, and attributes.

A data protection framework introduced in [16] has a set of constraints for policy construction. It proposed an access-control framework (policy-based language) to govern the security operation of distributed data in dynamic IoT networks.

In [132], smart meters mutually authenticate each other with a service provider to establish a session key for secret communication.

A security framework for edge-computing [118] has been connected to healthcare systems. It utilizes multi-factor access control and ownership transfer mechanism to create an authentication system. Furthermore, scalability is achieved by employing a distributed approach for clustering techniques that analyze and aggregate voluminous data acquired from heterogeneous devices individually before it transits to the cloud.

Unfortunately, the ability to distinguish a solution between these two categories is not always possible. Some solutions can work with both centralized and distributed environments, causing a blur in the categorization. Due to this, we have split up these categories further by introducing the subcategories: strictly centralized, strictly distributed, both, and not applicable.

Identity management through a centralized server is essential for certain practices due to the added difficulty of securing distributed operations. This added security may be a result of IoT in a specific domain [46], or it might just be derived from the methods or technologies employed [33,109,111,112,134]. The authors of [123] proposed a self-sovereign identity offered by distributed ledger technology to provide a secure, decentralized, and persistent identity for IoT devices. This allows a device identity, along with all its relationships, to be securely managed throughout its entire lifecycle.

However, some proposals decide to take a distributed approach by necessity. ABAC systems [32,33,97,100,103,104,111,114,124,125,140] rely on peer devices for entity attribute confirmation, which also requires a distributed architecture to function.

To summarize from the identified publications, as shown in Tables 4 and 5, we identified 47 centralized approaches [11,18,20,22,23,26,32,33,38,39,42,43,46,48,49,51,53,59,60,65,67,68,70,71,75–77,82,88,91,93–95,101–103,109,111,112,122,125,127,130,132–134,137], 56 distributed ones [12,13,16,21,24,27,30,31,35,37,40,44,47,52,54–56,58,62–64,69,72,73,79,81,83,85,87,89,92,96–98,100,104–106,108,110,113–116,118,120,121,123,124,129,131,135,136,139,141,142], and 6 approaches that use both [17,28,66,99,126,138]. Finally, 23 publications were not relevant or did not specify the results.

### *5.3. Communication Model*

The communication model can be seen in the perspectives of machine-to-machine (M2M) or user-to-machine (U2M). U2M strictly requires some user input information. IoT interaction may, similar to other distributed systems, consider stimuli from users or other autonomous parts of the system. The subcategories to encompass all articles involve M2M, U2M, and both.

*U2M communication* centers around user actors. Thus, we need to authenticate users, either in a conventional way or sometimes through unconventional means such as biological information [32,46,66,77,102,104,117] or even forms such as a user's mental state [39].

For *M2M communication*, there is no restriction that U2M systems possess (user stimuli/intervention); however, the abilities of these systems are often limited to the initial programming of users upon setup. M2M enables devices on the network to exchange

information and perform actions without the manual assistance of humans. This fits IoT as the common use case is to tap into sensor data and transmit it to a target system for processing or further escalation of automated actions. There are times when a user wants the responsibility of maintaining the security of an IoT system [66,120,140], and this is where M2M becomes valuable. Among examples, monitoring, supply chain management, and smart homes are all great fits for IoT solutions.

Authentication and authorization for M2M use cases are designed in [79], which specifically discusses one M2M security architecture, OAuth 2.0 framework, and Mobius. A more specific use case can be shown through a video surveillance system [115]. This system enables the active (automatic) monitoring of the controlled areas as it allows for the detection and the pre-alarm of abnormal events in real-time. A Diffie–Hellman-inspired protocol was used to allow two smart cameras to share a secret image. A tunneling framework was provided to protect the M2M communications established between the cameras using their fingerprints as an authentication factor and a secret image they share as a cipher key. A password-based authentication scheme for M2M Networks in [25] was achieved using hash invocations and symmetric key encryption. The scheme is suitable for environmental sensors, which are limited in resources (computation, storage, energy, etc.) Furthermore, a novel security model approach in [65] introduced security-related attributes combined with privilege management infrastructure to overcome known drawbacks in machine-to-machine communication such as poor extensibility, lacking use-case-related authorization schemas, and weak separation between information and authorization model.

There may be instances where either a U2M or M2M model exists in a researched technology. For these instances, a M2M tool can be transformed to work with a U2M model [81], or the tool can exist in both models [33,38,56,74,111].

To summarize, we identified 57 U2M approaches [11,14,18,20,22,24,26,29,31,32,35,39,40,42,44,46,48,50,51,59,60,62,64,68,70,73,75–78,80,82,83,85,92–94,98,100,102,104–107,112,118,119,122,126,128,132,133,135–137,139,141], 31 M2M ones [13,21,25,27,28,43,54,55,65,66,79,87–89,95,96,99,101,103,109,110,113–115,120,125,127,129,130,138,140], and 30 approaches where both were used [12,16,17,23,30,33,34,38,45,47,49,52,53,56,63,67,71,72,74,81,91,97,108,111,116,121,124,131,134,142]. Finally, 14 publications were not relevant or did not specify the model. The majority of centralized topologies involved U2M. For distributed topology, the distribution was slightly in advance of U2M. There was no impact of the communication model for the context-aware solutions.

### 5.4. Existing versus New Methods

Here, we consider the method novelty. It is common to build on existing solutions and extends them, but some researchers propose novel alternatives.

In this taxonomy, current publications on IoT security can roughly be divided into three categories: applying existing methods, extending them to better suit the IoT specifications, and building new methods.

Studies that adapted or applied existing technologies and methods from other security domains to the IoT environment often considered extensions to ABAC and RBAC [32,33,97,100,103,104,111,114,124,125,140]. While RBAC is a method of restricting network access based on the roles of individual users within an enterprise, ABAC is an authentication and authorization model under the identity management umbrella that uses attributes rather than roles to grant users access.

Other interesting technologies in this taxonomy include OAuth 2.0 [81,134] and the Fuzzy logic system [42,109]. OAuth 2.0 is an authorization protocol that is used by online applications to gain access to resources hosted by other online applications. The Fuzzy logic system is an attempt to imitate how people think through computation. This allows reasoning to be considered regarding a problem, as opposed to an approach with basic evaluation. Three works focused on the use of JSON Web Token (JWT) [148] for different authentication techniques [75,119,124]. JWT is similar to regular web tokens, but it contains a set of claims to transmit information between two entities.

Studies that focus on novel ideas make use of very diverse methods to achieve unique results. One proposal [26] introduces the security framework, named SODA, to centralize security policy and service management for IoT environments, acting as an intermediate device that all devices are connected to, which allows all security concerns to be routed through it. Other approaches based on physical authentication discuss the use of brainwaves for authentication by considering the familiarity between users and certain images [39], and two methods use an accelerometer to measure a person's gait and authenticate the user based on this metric [60,76].

In summary, there are various brand-new proposals with novel ideas in 14 publications [13,31,33,36,37,41,46,61,65,86,90,93,109,127] that have great potential to address the IoT security issue from the perspectives of scalability, maintainability, and flexibility. However, it is still difficult to predict which ideas might be adopted widely. Although a significant amount of research is focused on adoption of existing technologies with 63 of identified publications [15,16,20–23,26,28,30,32,35,39,40,43,45,49–51,55,57,60,62,63,66,67,69,71–73,76,78,82,84,92,94–96,98–105,107,112,113,116,118,120,121,123,125,126,129,133,135,137–141], there were 55 publications related to extensions [11,12,14,17–19,24,25,27,29,34,38,42,44,47,48,52–54,56,58,59,64,68,70,74,75,77,79–81,83,85,87–89,91,97,106,108,110,111,114,115,117,119,122,124,128,130–132,134,136,142].

Extensions were more common for context-unaware works. There was no significant impact from topologies or communication models.

### *5.5. Domains and Constraints Used in Research of Security Solutions*

The publications we assessed considered security solutions in general and specific domains. Tables 4 and 5 indicate the specifics for each publication. Overall, nearly half of the publications considered solutions applicable to any domain, which we classify as general. Among specific domains were mentioned IoT platforms, smart homes, healthcare, fog computing, wearable, surveillance, ATM, smart city, and cars.

Often, the security solutions considered constrained devices or even a specialized or external device such as smartwatches and other wearable technology, which we highlight in Tables 4 and 5 as well.

Most approaches did not require special devices. However, a large number required special devices such as biometric sensors, wearables, cameras, security devices, mobile devices/smartphones, and RFID and sensors.

## 6. Threats to Validity

It is usual for systematic reviews, mapping studies, and surveys to suffer from several threats to validity that need to be addressed. We have discovered multiple threats to mention. In this context, we discuss the validity threats from the perspective of Wohlin's taxonomy [149]. In particular, four potential threats are considered: construct validity, internal validity, external validity, and conclusions validity.

The construct validity is meant to consider the research questions within the investigated area. Our queries are motivated by a previously performed study, which dated results. The primary terms were combined with secondary terms and exclusion parts to execute this study. All used terms are commonly recognized in the community and domain of this work, and all are suitable to be used as search strings. A possible threat of omitting relevant research from our review was addressed by experimenting with several other search strings identifying related work. Still, this study could miss relevant work, although given threads would be slightly impacted. Moreover, selected major research databases were considered but not all. The analyzed sample only considered peer-reviewed articles published by journals or conferences to ensure the objectivity and reliability of the information sources. It did not include reprints of the papers submitted to or accepted in journals and conferences published by arXiv.org, researchgate.net, or individual personal pages. These reprints might contain novel ideas, methods, and new challenges relevant to

the scope of analyzed papers. Furthermore, our article queries were limited to the abstracts of the articles, so we could have missed relevant work with poorly stated abstracts.

Internal validity involves methods to study and analyze data (e.g., the types of bias involved). One potential threat is related to inclusion and exclusion, a process that included metadata, abstracts, and possibly full-text assessments; this could be further affected by our bias when performing the filtering. Multiple authors performed this, with primary authors assigned to a particular indexer and secondary authors to spot-checking. Apart from the filtering process, we performed question coding, leading to improper interpretation of results. We addressed the above by assigning distinct indexers to different researchers, with spot-check validation by others on sample publications. Our goal-based taxonomy is a result of our discussions of interpreted results and represents our view on the identified literature. We also performed automated keyword extraction meant to address potential bias threats.

External validity is related to knowledge generalization. This survey interprets and categorizes works we gathered from established scientific channels, and our observations related to IoT. We could have missed related work; however, we aimed to minimize the impact possibly resulting from the presented trends and their generalization given through the diversity of scientific channels.

The conclusions result from several brainstorming sessions independently settled by all authors. To address the validity of the conclusions, we involved multiple authors in this study, with all of them discussing the outcomes in the context of extracted and synthesized information.

## 7. Answers to Research Questions

In this paper, we raised multiple Research Questions (RQ) addressed throughout the previous sections. Next, we provided more concise answers to the RQs with back-references to the particular section content.

***RQ1*** *What is the taxonomy of security solutions?*

This question is answered through three taxonomy models of distinctions by publication year, goals, and categorization through extracted keywords in Section 4. In particular, Figure 2 details the publication year taxonomy, with the year 2019 being the most active year. The keyword taxonomy is highlighted in Figure 3, giving the proportions of research focus on authentication, context, services, authorization, cloud, attributes, roles, and health.

***RQ2*** *What topologies, communication types, and perspectives are most dominant in the authentication and authorization IoT research?*

We have identified that IoT solutions become more context-aware when considering the perspectives of past and present. There is no conclusion to be made whether centralized or distributed models dominate; both are used with the moderate majority for distributed models as described in Section 5.2. The user-to-machine communication model has a significantly greater scientific interest than machine-to-machine models, although a hybrid model accommodating both is also considered as Section 5.3 stated in detail. The great majority of research works are on established methods.

***RQ3*** *What are the applicability domains and requirements of identified solutions?*

We addressed this question through full-text analysis, which resulted in comprehensive answers available in Tables 4 and 5. A summary of the results is shown in Section 5.5.

## 8. Conclusions

This systematic review provides a practical overview of recent IoT authentication and authorization advancements. Using a systematic literature review approach, it assessed 1622 peer-reviewed publications to find evidence to provide security solution taxonomy and discuss recent efforts from other related perspectives. The provided details show that common practices and models are applied for authentication and authorization. Context-awareness can be a beneficial companion to aid authentication. While most security

solutions are distributed, still a significant proportion are centralized. Research directions are further fragmented by communication from the central perspective to users or devices, for which we provide a practical road map to existing works .

**Author Contributions:** Conceptualization, M.T. and T.C.; software, M.T.; validation, M.T. and A.S.; investigation, M.T., A.S.A., A.S., and M.C.; data curation, M.T., A.S.A., A.S., and M.C.; writing—original draft preparation, M.T., A.S.A., A.S., and M.C.; writing—review and editing, M.T., A.S., and T.C.; supervision, T.C.; project administration, T.C. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by National Science Foundation grant number 1854049 and a grant from Red Hat Research https://research.redhat.com (accessed on 9 February 2022). The APC has not been funded yet.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The authors declare no conflict of interest. The patrons had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

## Abbreviations

The following abbreviations are used in this manuscript:

| | |
|---|---|
| IoT | Internet of things |
| RQ | Research question |
| WoS | Web of Science |
| SCIE | Science Citation Index Expanded |
| ACM DL | Association for Computing Machinery digital library |
| M2M | Machine to machine |
| U2M | User to machine |
| ABAC | Attribute-based access control |
| RBAC | Role-based access control |
| JWT | JSON web token |
| GPS | Global positioning system |
| PC | Personal computer |
| CBAC | Capability-based access control |
| RFID | Radio-frequency identification |

## References

1. Loi, F.; Sivanathan, A.; Gharakheili, H.H.; Radford, A.; Sivaraman, V. Systematically Evaluating Security and Privacy for Consumer IoT Devices. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy (IoTS&P '17)*; Association for Computing Machinery: New York, NY, USA, 2017; pp. 1–6. [CrossRef]
2. Anderson, R.; Moore, T. The Economics of Information Security. *Science* **2006**, *314*, 610–613. [CrossRef] [PubMed]
3. Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805. [CrossRef]
4. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things security: A survey. *J. Netw. Comput. Appl.* **2017**, *88*, 10–28. [CrossRef]
5. binti Mohamad Noor, M.; Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. *Comput. Netw.* **2019**, *148*, 283–294. [CrossRef]
6. Trnka, M.; Cerny, T.; Stickney, N. Survey of Authentication and Authorization for the Internet of Things. *Secur. Commun. Netw.* **2018**, *2018*, 4351603. [CrossRef]
7. Miloslavskaya, N.; Tolstoy, A. Internet of Things: Information security challenges and solutions. *Clust. Comput.* **2019**, *22*, 103–119. [CrossRef]
8. Chanal, P.M.; Kakkasageri, M.S. Security and Privacy in IoT: A Survey. *Wirel. Pers. Commun.* **2020**, *115*, 1667–1693. [CrossRef]
9. Al-Naji, F.H.; Zagrouba, R. A survey on continuous authentication methods in Internet of Things environment. *Comput. Commun.* **2020**, *163*, 109–133. [CrossRef]

10. Tange, K.; De Donno, M.; Fafoutis, X.; Dragoni, N. A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities. *IEEE Commun. Surv. Tutorials* **2020**, *22*, 2489–2520. [CrossRef]
11. Ibrahim, S.; Shukla, V.K.; Bathla, R. Security Enhancement in Smart Home Management Through Multimodal Biometric and Passcode. In Proceedings of the 2020 International Conference on Intelligent Engineering and Management (ICIEM), London, UK, 17–19 June 2020; pp. 420–424. [CrossRef]
12. Baruah, B.; Dhal, S. An Efficient Authentication Scheme for Secure Communication between Industrial IoT Devices. In Proceedings of the 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 1–3 July 2020; pp. 1–7. [CrossRef]
13. Zulkipli, N.H.N.; Wills, G.B. An Event-Based Access Control for IoT. In *Proceedings of the Second International Conference on Internet of Things, Data and Cloud Computing (ICC '17)*; Association for Computing Machinery: New York, NY, USA, 2017. [CrossRef]
14. Chen, Y.Y.; Chen, C.L.; Lin, C.L.; Chiang, C.T. Application of ECG Authentication in IoT-Based Systems. In Proceedings of the 2018 International Conference on System Science and Engineering (ICSSE), New Taipei City, Taiwan, 28–30 June 2018; pp. 1–6. [CrossRef]
15. Kashmar, N.; Adda, M.; Atieh, M.; Ibrahim, H. A New Dynamic Smart-AC Model Methodology to Enforce Access Control Policy in IoT Layers. In Proceedings of the 1st International Workshop on Software Engineering Research & Practices for the Internet of Things (SERP4IoT '19), Montreal, QC, Canada, 27 May 2019; pp. 21–24. [CrossRef]
16. Karimibiuki, M.; Aggarwal, E.; Pattabiraman, K.; Ivanov, A. DynPolAC: Dynamic Policy-Based Access Control for IoT Systems. In Proceedings of the 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC), Taipei, Taiwan, 4–8 December 2018; pp. 161–170. [CrossRef]
17. Chen, H.C.; Chang, C.H.; Leu, F.Y. Implement of agent with role-based hierarchy access control for secure grouping IoTs. In Proceedings of the 2017 14th IEEE Annual Consumer Communications Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2017; pp. 120–125. [CrossRef]
18. Olazabal, O.; Gofman, M.; Bai, Y.; Choi, Y.; Sandico, N.; Mitra, S.; Pham, K. Multimodal Biometrics for Enhanced IoT Security. In Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019; pp. 0886–0893. [CrossRef]
19. Terkawi, A.; Innab, N.; al Amri, S.; Al-Amri, A. Internet of Things (IoT) Increasing the Necessity to Adopt Specific Type of Access Control Technique. In Proceedings of the 2018 21st Saudi Computer Society National Computer Conference (NCC), Riyadh, Saudi Arabia, 25–26 April 2018; pp. 1–5. [CrossRef]
20. Hoang, N.M.; Son, H.X. A Dynamic Solution for Fine-Grained Policy Conflict Resolution. In *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy (ICCSP '19)*; Association for Computing Machinery: New York, NY, USA, 2019; pp. 116–120. [CrossRef]
21. Cattermole, T.; Docherty, S.; Pym, D.; Sasse, M.A. Asset-Oriented Access Control: Towards a New IoT Framework. In *Proceedings of the 9th International Conference on the Internet of Things (IoT 2019)*; Association for Computing Machinery: New York, NY, USA, 2019; [CrossRef]
22. Mathew, S.; Saranya, G. Advanced biometric home security system using digital signature and DNA cryptography. In Proceedings of the 2017 International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT), Coimbatore, India, 16–18 March 2017; pp. 1–4. [CrossRef]
23. Jain, P.; Pötter, H.; Lee, A.J.; Mósse, D. MAFIA: Multi-layered Architecture For IoT-based Authentication. In Proceedings of the 2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Atlanta, GA, USA, 28–31 October 2020; pp. 199–208. [CrossRef]
24. Guo, Y.; Zhang, Z.; Guo, Y. Fog-Centric Authenticated Key Agreement Scheme Without Trusted Parties. *IEEE Syst. J.* **2020**, *15*, 5057–5066. [CrossRef]
25. Renuka, K.M.; Kumari, S.; Zhao, D.; Li, L. Design of a Secure Password-Based Authentication Scheme for M2M Networks in IoT Enabled Cyber-Physical Systems. *IEEE Access* **2019**, *7*, 51014–51027. [CrossRef]
26. Kim, Y.; Nam, J.; Park, T.; Scott-Hayward, S.; Shin, S. SODA: A software-defined security framework for IoT environments. *Comput. Netw.* **2019**, *163*, 106889. [CrossRef]
27. Felde, N.g.; Grundner-Culemann, S.; Guggemos, T. Authentication in dynamic groups using identity-based signatures. In Proceedings of the 2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Limassol, Cyprus, 15–17 October 2018; pp. 1–6. [CrossRef]
28. Mahbub, T.N.; Reza, S.M.S.; Hossain, D.A.; Raju, M.H.; Arifeen, M.M.; Ayob, A. ANFIS Based Authentication Performance Evaluation for Enhancing Security in Internet of Things. In *Proceedings of the International Conference on Computing Advancements (ICCA 2020)*; Association for Computing Machinery: New York, NY, USA, 2020. [CrossRef]
29. Heydari, M.; Mylonas, A.; Katos, V.; Balaguer-Ballester, E.; Tafreshi, V.H.F.; Benkhelifa, E. Uncertainty-Aware Authentication Model for Fog Computing in IoT. In Proceedings of the 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC), Rome, Italy, 10–13 June 2019; pp. 52–59. [CrossRef]
30. Ning, Z.; Xu, G.; Xiong, N.; Yang, Y.; Shen, C.; Panaousis, E.; Wang, H.; Liang, K. TAW: Cost-Effective Threshold Authentication With Weights for Internet of Things. *IEEE Access* **2019**, *7*, 30112–30125. [CrossRef]

31. Leung, H.M.C.; Fu, C.W.; Heng, P.A. TwistIn: Tangible Authentication of Smart Devices via Motion Co-Analysis with a Smartwatch. In *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*; ACM: New York, NY, USA, 2018; Volume 2, pp. 1–24. [CrossRef]
32. Burakgazi Bilgen, M.; Bicakci, K. Extending Attribute-Based Access Control Model with Authentication Information for Internet of Things. In Proceedings of the 2020 International Conference on Information Security and Cryptology (ISCTURKEY), Ankara, Turkey, 3–4 December 2020; pp. 48–55. [CrossRef]
33. Oh, S.R.; Kim, Y.G.; Cho, S. An Interoperable Access Control Framework for Diverse IoT Platforms Based on OAuth and Role. *Sensors* **2019**, *19*, 1884. [CrossRef]
34. Dammak, M.; Boudia, O.R.M.; Messous, M.A.; Senouci, S.M.; Gransart, C. Token-Based Lightweight Authentication to Secure IoT Networks. In Proceedings of the 2019 16th IEEE Annual Consumer Communications Networking Conference (CCNC), Las Vegas, NV, USA, 11–14 January 2019; pp. 1–4. [CrossRef]
35. Nespoli, P.; Zago, M.; Celdran, A.H.; Perez, M.G.; Marmol, F.G.; Garcia Clernente, F.J. A Dynamic Continuous Authentication Framework in IoT-Enabled Environments. In Proceedings of the 2018 Fifth International Conference on Internet of Things: Systems, Management and Security, Valencia, Spain, 15–18 October 2018; pp. 131–138. [CrossRef]
36. Rothe, L.; Loske, M.; Gertler, D.G. Proposing Context-Aware Authentication for the Industrial Internet of Things. In Proceedings of the 2018 IEEE Global Conference on Internet of Things (GCIoT), Alexandria, Egypt, 5–7 December 2018; pp. 1–5. [CrossRef]
37. Ouaddah, A.; Mousannif, H.; Abou Elkalam, A.; Ait Ouahman, A. Access control in the Internet of Things: Big challenges and new opportunities. *Comput. Netw.* **2017**, *112*, 237–262. [CrossRef]
38. Yan, H.; Wang, Y.; Jia, C.; Li, J.; Xiang, Y.; Pedrycz, W. IoT-FBAC: Function-based access control scheme using identity-based encryption in IoT. *Future Gener. Comput. Syst.* **2019**, *95*, 344 – 353. [CrossRef]
39. Chiu, W.; Su, C.; Fan, C.Y.; Chen, C.M.; Yeh, K.H. Authentication with What You See and Remember in the Internet of Things. *Symmetry* **2018**, *10*, 537. [CrossRef]
40. Phoka, T.; Phetsrikran, T.; Massagram, W. Dynamic Keypad Security System with Key Order Scrambling Technique and OTP Authentication. In Proceedings of the 2018 22nd International Computer Science and Engineering Conference (ICSEC), Chiang Mai, Thailand, 21–24 November 2018; pp. 1–4. [CrossRef]
41. Heydari, M.; Mylonas, A.; Tafreshi, V.H.F.; Benkhelifa, E.; Singh, S. Known unknowns: Indeterminacy in authentication in IoT. *Future Gener. Comput. Syst.* **2020**, *111*, 278–287. [CrossRef]
42. Malavizhi, N.; Selarani, N.; Raj, P. Adaptive fuzzy genetic algorithm for multi biometric authentication. *Multimed Tools Appl.* **2020**, *79*, 9131–9144. [CrossRef]
43. Sharif, M.; Mercelis, S.; Van Den Bergh, W.; Hellinckx, P. Towards Real-Time Smart Road Construction: Efficient Process Management through the Implementation of Internet of Things. In *Proceedings of the International Conference on Big Data and Internet of Thing (BDIOT2017)*; Association for Computing Machinery: New York, NY, USA, 2017; pp. 174–180. [CrossRef]
44. Ashibani, Y.; Kauling, D.; Mahmoud, Q.H. A context-aware authentication framework for smart homes. In Proceedings of the 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE), Windsor, ON, Canada, 30 April–3 May 2017; pp. 1–5. [CrossRef]
45. Ulz, T.; Pieber, T.; Steger, C.; Holler, A.; Haas, S.; Matischek, R. Automated Authentication Credential Derivation for the Secured Configuration of IoT Devices. In Proceedings of the 2018 IEEE 13th International Symposium on Industrial Embedded Systems (SIES), Graz, Austria, 6–8 June 2018; pp. 1–8. [CrossRef]
46. Gebrie, M.T.; Abie, H. Risk-Based Adaptive Authentication for Internet of Things in Smart Home EHealth. In *Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings (ECSA '17)*; Association for Computing Machinery: New York, NY, USA, 2017; pp. 102–108. [CrossRef]
47. Wang, M.; Yan, Z. Privacy-Preserving Authentication and Key Agreement Protocols for D2D Group Communications. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3637–3647. [CrossRef]
48. Nespoli, P.; Zago, M.; Huertas Celdrán, A.; Gil Pérez, M.; Gómez Mármol, F.; García Clemente, F.J. PALOT: Profiling and Authenticating Users Leveraging Internet of Things. *Sensors* **2019**, *19*, 2832. [CrossRef] [PubMed]
49. Ghosh, N.; Chandra, S.; Sachidananda, V.; Elovici, Y. SoftAuthZ: A Context-Aware, Behaviour-Based Authorization Framework for Home IoT. *IEEE Internet Things J.* **2019**, *6*, 10773–10785. [CrossRef]
50. Gad, R.; Abd El-Latif, A.A.; Elseuofi, S.; Ibrahim, H.M.; Elmezain, M.; Said, W. IoT Security Based on Iris Verification Using Multi-Algorithm Feature Level Fusion Scheme. In Proceedings of the 2019 2nd International Conference on Computer Applications Information Security (ICCAIS), Riyadh, Saudi Arabia, 1–3 May 2019; pp. 1–6. [CrossRef]
51. Mbarek, B.; Buhnova, B.; Pitner, T. SeMLAS: An Efficient Secure Multi-Level Authentication Scheme for IoT-Based Smart Home Systems. In Proceedings of the 2019 15th International Wireless Communications Mobile Computing Conference (IWCMC), Tangier, Morocco, 24–28 June 2019; pp. 1373–1378. [CrossRef]
52. Hasan, A.; Qureshi, K. Internet of Things Device Authentication Scheme Using Hardware Serialization. In Proceedings of the 2018 International Conference on Applied and Engineering Mathematics (ICAEM), Taxila, Pakistan, 4–5 September 2018; pp. 109–114. [CrossRef]
53. Arfaoui, A.; Cherkaoui, S.; Kribeche, A.; Senouci, S.M.; Hamdi, M. Context-Aware Adaptive Authentication and Authorization in Internet of Things. In Proceedings of the ICC 2019—2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6. [CrossRef]

54. Murphy, J.; Howells, G.; McDonald-Maier, K.D. Multi-factor authentication using accelerometers for the Internet-of-Things. In Proceedings of the 2017 Seventh International Conference on Emerging Security Technologies (EST), Canterbury, UK, 6–8 September 2017; pp. 103–107. [CrossRef]
55. Durand, A.; Gremaud, P.; Pasquier, J. Decentralized Web of Trust and Authentication for the Internet of Things. In *Proceedings of the Seventh International Conference on the Internet of Things (IoT '17)*; Association for Computing Machinery: New York, NY, USA, 2017. [CrossRef]
56. Pallavi, K.N.; Ravi Kumar, V. Authentication-based Access Control and Data Exchanging Mechanism of IoT Devices in Fog Computing Environment. *Wirel. Pers. Commun.* **2020**, *116*, 3039–3060. [CrossRef]
57. Saadeh, M.; Sleit, A.; Sabri, K.E.; Almobaideen, W. Hierarchical architecture and protocol for mobile object authentication in the context of IoT smart cities. *J. Netw. Comput. Appl.* **2018**, *121*, 1–19. [CrossRef]
58. Carnley, P.R.; Rowland, P.; Bishop, D.; Bagui, S.; Miller, M. Trusted Digital Identities for Mobile Devices. In Proceedings of the 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Calgary, AB, Canada, 17–22 August 2020; pp. 483–490. [CrossRef]
59. Chifor, B.C.; Bica, I.; Patriciu, V.V.; Pop, F. A security authorization scheme for smart home Internet of Things devices. *Future Gener. Comput. Syst.* **2018**, *86*, 740–749. [CrossRef]
60. Batool, S.; Hassan, A.; Saqib, N.A.; Khattak, M.A.K. Authentication of Remote IoT Users Based on Deeper Gait Analysis of Sensor Data. *IEEE Access* **2020**, *8*, 101784–101796. [CrossRef]
61. Gamundani, A.M.; Phillips, A.; MUYINGI, H.N. Privacy Preservation and Security Dilemma : Relationship proposition for IoT authentication. In Proceedings of the 2018 International Conference on Recent Innovations in Electrical, Electronics Communication Engineering (ICRIEECE), Bhubaneswar, India, 27–28 July 2018; pp. 363–367. [CrossRef]
62. Chauhan, J.; Rajasegaran, J.; Seneviratne, S.; Misra, A.; Seneviratne, A.; Lee, Y. Performance Characterization of Deep Learning Models for Breathing-Based Authentication on Resource-Constrained Devices. In *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*; ACM: New York, NY, USA, 2018; Volume 2, pp. 1–24. [CrossRef]
63. Sharaf Dabbagh, Y.; Saad, W. Authentication of Wireless Devices in the Internet of Things: Learning and Environmental Effects. *IEEE Internet Things J.* **2019**, *6*, 6692–6705. [CrossRef]
64. Ali, I.; Asif, M. Applying security patterns for authorization of users in IoT based applications. In Proceedings of the 2018 International Conference on Engineering and Emerging Technologies (ICEET), Lahore, Pakistan, 22–23 February 2018; pp. 1–5. [CrossRef]
65. Wallis, K.; Merzinger, M.; Reich, C.; Schindelhauer, C. A Security Model Based Authorization Concept for OPC Unified Architecture. In *Proceedings of the 10th International Conference on Advances in Information Technology (IAIT 2018)*; Association for Computing Machinery: New York, NY, USA, 2018. [CrossRef]
66. Krašovec, A.; Pellarini, D.; Geneiatakis, D.; Baldini, G.; Pejović, V. Not Quite Yourself Today: Behaviour-Based Continuous Authentication in IoT Environments. In *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*; ACM: New York, NY, USA, 2020; Volume 4, pp. 1–29. [CrossRef]
67. Yang, S.K.; Shiue, Y.M.; Su, Z.Y.; Liu, C.G. A Novel Authentication Scheme Against Node Captured Attack in WSN for Healthcare Scene. In Proceedings of the 2019 IEEE Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability (ECBIOS), Okinawa, Japan, 31 May–3 June 2019; pp. 39–42. [CrossRef]
68. Sahoo, S.; Sahoo, S.S.; Maiti, P.; Sahoo, B.; Turuk, A.K. A Lightweight Authentication Scheme for Cloud-Centric IoT Applications. In Proceedings of the 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 7–8 March 2019; pp. 1024–1029. [CrossRef]
69. Zhu, X.; Badr, Y.; Pacheco, J.; Hariri, S. Autonomic Identity Framework for the Internet of Things. In Proceedings of the 2017 International Conference on Cloud and Autonomic Computing (ICCAC), Tucson, AZ, USA, 18–22 September 2017; pp. 69–79. [CrossRef]
70. Das, A.K.; Wazid, M.; Kumar, N.; Vasilakos, A.V.; Rodrigues, J.J.P.C. Biometrics-Based Privacy-Preserving User Authentication Scheme for Cloud-Based Industrial Internet of Things Deployment. *IEEE Internet Things J.* **2018**, *5*, 4900–4913. [CrossRef]
71. Khan, R. Dynamically Configurable Architecture for User Identification and Authentication for Internet of Things Platform. In Proceedings of the 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox'sBazar, Bangladesh, 7–9 February 2019; pp. 1–8. [CrossRef]
72. Chien, H.Y. Group-Oriented Range-Bound Key Agreement for Internet of Things Scenarios. *IEEE Internet Things J.* **2018**, *5*, 1890–1903. [CrossRef]
73. Aski, V.J.; Gupta, S.; Sarkar, B. An Authentication-Centric Multi-Layered Security Model for Data Security in IoT-Enabled Biomedical Applications. In Proceedings of the 2019 IEEE 8th Global Conference on Consumer Electronics (GCCE), Osaka, Japan, 15–18 October 2019; pp. 957–960. [CrossRef]
74. Alkhresheh, A.; Elgazzar, K.; Hassanein, H.S. DACIoT: Dynamic Access Control Framework for IoT Deployments. *IEEE Internet Things J.* **2020**, *7*, 11401–11419. [CrossRef]
75. Ethelbert, O.; Moghaddam, F.F.; Wieder, P.; Yahyapour, R. A JSON Token-Based Authentication and Access Management Schema for Cloud SaaS Applications. In Proceedings of the 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud), Prague, Czech Republic, 21–23 August 2017; pp. 47–53. [CrossRef]

76. Sun, F.; Mao, C.; Fan, X.; Li, Y. Accelerometer-Based Speed-Adaptive Gait Authentication Method for Wearable IoT Devices. *IEEE Internet Things J.* **2019**, *6*, 820–830. [CrossRef]
77. Shayan, M.; Naser, M.; Hossein, G. IoT-Based Anonymous Authentication Protocol Using Biometrics in Smart Homes. In Proceedings of the 2019 16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC), Mashhad, Iran, 28–29 August 2019; pp. 114–121. [CrossRef]
78. Elganzoury, H.S.; Abdelhafez, A.A.; Hegazy, A.A. A new secure one-time password algorithm for mobile applications. In Proceedings of the 2018 35th National Radio Science Conference (NRSC), Cairo, Egypt, 20–22 March 2018; pp. 249–257. [CrossRef]
79. Oh, S.R.; Kim, Y.G. Development of IoT security component for interoperability. In Proceedings of the 2017 13th International Computer Engineering Conference (ICENCO), Cairo, Egypt, 27–28 December 2017; pp. 41–44. [CrossRef]
80. Zhou, L.; Su, C.; Chiu, W.; Yeh, K.H. You Think, Therefore You Are: Transparent Authentication System with Brainwave-Oriented Bio-Features for IoT Networks. *IEEE Trans. Emerg. Top. Comput.* **2020**, *8*, 303–312. [CrossRef]
81. Oh, S.R.; Kim, Y.G. AFaaS: Authorization framework as a service for Internet of Things based on interoperable OAuth. *Int. J. Distrib. Sens. Netw.* **2020**, *16*, 1550147720906388, [CrossRef]
82. Belk, M.; Fidas, C.; Pitsillides, A. FlexPass: Symbiosis of Seamless User Authentication Schemes in IoT. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems (CHI EA '19)*; Association for Computing Machinery: New York, NY, USA, 2019; pp. 1–6. [CrossRef]
83. Hassan, M.; Mansoor, K.; Tahir, S.; Iqbal, W. Enhanced Lightweight Cloud-assisted Mutual Authentication Scheme for Wearable Devices. In Proceedings of the 2019 International Conference on Applied and Engineering Mathematics (ICAEM), Taxila, Pakistan, 27–29 August 2019; pp. 62–67. [CrossRef]
84. Kaliya, N.; Hussain, M. Framework for privacy preservation in iot through classification and access control mechanisms. In Proceedings of the 2017 2nd International Conference for Convergence in Technology (I2CT), Mumbai, India, 7–9 April 2017; pp. 430–434. [CrossRef]
85. Wazid, M.; Das, A.K.; Khan, M.K.; Al-Ghaiheb, A.A.D.; Kumar, N.; Vasilakos, A.V. Secure Authentication Scheme for Medicine Anti-Counterfeiting System in IoT Environment. *IEEE Internet Things J.* **2017**, *4*, 1634–1646. [CrossRef]
86. Shah, R.H.; Salapurkar, D.P. A multifactor authentication system using secret splitting in the perspective of Cloud of Things. In Proceedings of the 2017 International Conference on Emerging Trends Innovation in ICT (ICEI), Pune, India, 3–5 February 2017; pp. 1–4. [CrossRef]
87. Amoon, M.; Altameem, T.; Altameem, A. RRAC: Role based reputed access control method for mitigating malicious impact in intelligent IoT platforms. *Comput. Commun.* **2020**, *151*, 238–246. [CrossRef]
88. Yazdanpanah, H.; Azizi, M.; Pournaghi, S.M. A Secure and Improved Authentication Scheme for Heterogeneous Wireless Sensor Networks in the Internet of Things Environment. In Proceedings of the 2020 17th International ISC Conference on Information Security and Cryptology (ISCISC), Tehran, Iran, 9–10 September 2020; pp. 36–43. [CrossRef]
89. Barbareschi, M.; De Benedictis, A.; La Montagna, E.; Mazzeo, A.; Mazzocca, N. PUF-Enabled Authentication-as-a-Service in Fog-IoT Systems. In Proceedings of the 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Napoli, Italy, 12–14 June 2019; pp. 58–63. [CrossRef]
90. Loske, M.; Rothe, L.; Gertler, D.G. Context-Aware Authentication: State-of-the-Art Evaluation and Adaption to the IIoT. In Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 15–18 April 2019; pp. 64–69. [CrossRef]
91. Shahzad, M.; Singh, M.P. Continuous Authentication and Authorization for the Internet of Things. *IEEE Internet Comput.* **2017**, *21*, 86–90. [CrossRef]
92. Rattanalerdnusorn, E.; Thaenkaew, P.; Vorakulpipat, C. Security Implementation For Authentication In Iot Environments. In Proceedings of the 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS), Singapore, 23–25 February 2019; pp. 678–681. [CrossRef]
93. Prathibha, L.; Fatima, K. Exploring Security and Authentication Issues in Internet of Things. In Proceedings of the 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 14–15 June 2018; pp. 673–678. [CrossRef]
94. Whaiduzzaman, M.; Oliullah, K.; Mahi, M.J.N.; Barros, A. AUASF: An Anonymous Users Authentication Scheme for Fog-IoT Environment. In Proceedings of the 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 1–3 July 2020; pp. 1–7. [CrossRef]
95. Liu, H.; Li, J.; Gu, D. Understanding the security of app-in-the-middle IoT. *Comput. Secur.* **2020**, *97*, 102000. [CrossRef]
96. El Kalam, A.A.; Outchakoucht, A.; Es-Samaali, H. Emergence-Based Access Control: New Approach to Secure the Internet of Things. In *Proceedings of the 1st International Conference on Digital Tools & Uses Congress (DTUC '18)*; Association for Computing Machinery: New York, NY, USA, 2018. [CrossRef]
97. Genç, D.; Tomur, E.; Erten, Y.M. Context-Aware Operation-Based Access Control for Internet of Things Applications. In Proceedings of the 2019 International Symposium on Networks, Computers and Communications (ISNCC), Istanbul, Turkey, 18–20 June 2019; pp. 1–6. [CrossRef]
98. Ashibani, Y.; Kauling, D.; Mahmoud, Q.H. A context-aware authentication service for smart homes. In Proceedings of the 2017 14th IEEE Annual Consumer Communications Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2017; pp. 588–589. [CrossRef]

99. Bhatt, S.; Sandhu, R. ABAC-CC: Attribute-Based Access Control and Communication Control for Internet of Things. In *Proceedings of the 25th ACM Symposium on Access Control Models and Technologies (SACMAT '20)*; Association for Computing Machinery: New York, NY, USA, 2020; pp. 203–212. [CrossRef]
100. Pal, S.; Hitchens, M.; Varadharajan, V.; Rabehaja, T. On Design of A Fine-Grained Access Control Architecture for Securing IoT-Enabled Smart Healthcare Systems. In *Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous 2017)*; Association for Computing Machinery: New York, NY, USA, 2017; pp. 432–441. [CrossRef]
101. Miettinen, M.; Nguyen, T.D.; Sadeghi, A.R.; Asokan, N. Revisiting Context-Based Authentication in IoT. In *Proceedings of the 55th Annual Design Automation Conference (DAC '18)*; Association for Computing Machinery: New York, NY, USA, 2018. [CrossRef]
102. Lu, C.X.; Li, Y.; Xiangli, Y.; Li, Z. Nowhere to Hide: Cross-Modal Identity Leakage between Biometrics and Devices. In *Proceedings of The Web Conference 2020 (WWW '20)*; Association for Computing Machinery: New York, NY, USA, 2020; pp. 212–223. [CrossRef]
103. Gupta, M.; Benson, J.; Patwa, F.; Sandhu, R. Dynamic Groups and Attribute-Based Access Control for Next-Generation Smart Cars. In *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy (CODASPY '19)*; Association for Computing Machinery: New York, NY, USA, 2019; pp. 61–72. [CrossRef]
104. Salama, U.; Yao, L.; Wang, X.; Paik, H.Y.; Beheshti, A. Multi-Level Privacy-Preserving Access Control as a Service for Personal Healthcare Monitoring. In Proceedings of the 2017 IEEE International Conference on Web Services (ICWS), Honolulu, HI, USA, 25–30 June 2017; pp. 878–881. [CrossRef]
105. Blue, L.; Abdullah, H.; Vargas, L.; Traynor, P. In *2MA: Verifying Voice Commands via Two Microphone Authentication (ASIACCS '18)*; Association for Computing Machinery: New York, NY, USA, 2018; pp. 89–100. [CrossRef]
106. Islam, S.M.R.; Hossain, M.; Hasan, R.; Duong, T.Q. A conceptual framework for an IoT-based health assistant and its authorization model. In Proceedings of the 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 8–10 January 2018; pp. 616–621. [CrossRef]
107. Srinivas, J.; Das, A.K.; Wazid, M.; Kumar, N. Anonymous Lightweight Chaotic Map-Based Authenticated Key Agreement Protocol for Industrial Internet of Things. *IEEE Trans. Depend. Secur. Comput.* **2020**, *17*, 1133–1146. [CrossRef]
108. Pal, S.; Hitchens, M.; Varadharajan, V. Towards the Design of a Trust Management Framework for the Internet of Things. In Proceedings of the 2019 13th International Conference on Sensing Technology (ICST), Sydney, NSW, Australia, 2–4 December 2019; pp. 1–7. [CrossRef]
109. Atlam, H.F.; Wills, G.B. An efficient security risk estimation technique for Risk-based access control model for IoT. *Internet Things* **2019**, *6*, 100052. [CrossRef]
110. Khalil, A.; Mbarek, N.; Togni, O. IoT-MAAC: Multiple Attribute Access Control for IoT environments. In Proceedings of the 2020 IEEE 17th Annual Consumer Communications Networking Conference (CCNC), Las Vegas, NV, USA, 10–13 January 2020; pp. 1–6. [CrossRef]
111. Djilali, H.B.; Tandjaoui, D.; Khemissa, H. Enhanced dynamic team access control for collaborative Internet of Things using context. *Trans. Emerg. Telecommun. Technol.* **2020**, *32*, e4083. [CrossRef]
112. Van hamme, T.; Preuveneers, D.; Joosen, W. A Dynamic Decision Fusion Middleware for Trustworthy Context-Aware IoT Applications. In *Proceedings of the 4th Workshop on Middleware and Applications for the Internet of Things (M4IoT '17)*; Association for Computing Machinery: New York, NY, USA, 2017; pp. 1–6. [CrossRef]
113. Schuster, R.; Shmatikov, V.; Tromer, E. Situational Access Control in the Internet of Things. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18)*; Association for Computing Machinery: New York, NY, USA, 2018; pp. 1056–1073. [CrossRef]
114. Aliane, L.; Adda, M. HoBAC: Toward a Higher-order Attribute-Based Access Control Model. *Procedia Comput. Sci.* **2019**, *155*, 303–310. [CrossRef]
115. Nakouri, I.; Hamdi, M.; Kim, T.H. A Key Management Scheme for IoT-Based Video Surveillance Systems Based on Fingerprints. In Proceedings of the 2018 IEEE 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Paris, France, 27–29 June 2018; pp. 100–105. [CrossRef]
116. Ranaweera, P.; Imrith, V.N.; Liyanag, M.; Jurcut, A.D. Security as a Service Platform Leveraging Multi-Access Edge Computing Infrastructure Provisions. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6. [CrossRef]
117. Selvarani., P.; Suresh, A.; Malarvizhi, N. Secure and optimal authentication framework for cloud management using HGAPSO algorithm. *Clust. Comput.* **2019**, *22*, 4007–4016. [CrossRef]
118. Aski, V.; Dhaka, V.S.; Kumar, S.; Parashar, A.; Ladagi, A. A Multi-Factor Access Control and Ownership Transfer Framework for Future Generation Healthcare Systems. In Proceedings of the 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC), Waknaghat, India, 6–8 November 2020; pp. 93–98. [CrossRef]
119. Ahmed, S.; Mahmood, Q. An authentication based scheme for applications using JSON web token. In Proceedings of the 2019 22nd International Multitopic Conference (INMIC), Islamabad, Pakistan, 29–30 November 2019; pp. 1–6. [CrossRef]
120. Lupascu, C.; Lupascu, A.; Bica, I. DLT Based Authentication Framework for Industrial IoT Devices. *Sensors* **2020**, *20*, 2621. [CrossRef] [PubMed]

121. Krishnan, K.N.; Jenu, R.; Joseph, T.; Silpa, M.L. Blockchain Based Security Framework for IoT Implementations. In Proceedings of the 2018 International CET Conference on Control, Communication, and Computing (IC4), Thiruvananthapuram, India, 5–7 July 2018; pp. 425–429. [CrossRef]
122. Jonnada, S.; Dantu, R.; Shrestha, P.; Ranasinghe, I.; Widick, L. An OAuth-Based Authorization Framework for Access Control in Remote Collaboration Systems. In Proceedings of the 2018 National Cyber Summit (NCS), Huntsville, AL, USA, 5–7 June 2018; pp. 38–44. [CrossRef]
123. Gebresilassie, S.K.; Rafferty, J.; Morrow, P.; Chen, L.; Abu-Tair, M.; Cui, Z. Distributed, Secure, Self-Sovereign Identity for IoT Devices. In Proceedings of the 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2–16 June 2020; pp. 1–6. [CrossRef]
124. Martínez, J.A.; Hernández-Ramos, J.L.; Beltrán, V.; Skarmeta, A.; Ruiz, P.M. A user-centric Internet of Things platform to empower users for managing security and privacy concerns in the Internet of Energy. *Int. J. Distrib. Sens. Netw.* **2017**, *13*, 1550147717727974. [CrossRef]
125. Colombo, P.; Ferrari, E. Access Control Enforcement within MQTT-Based Internet of Things Ecosystems. In *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies (SACMAT '18)*; Association for Computing Machinery: New York, NY, USA, 2018; pp. 223–234. [CrossRef]
126. Rech, A.; Pistauer, M.; Steger, C. A Novel Embedded Platform for Secure and Privacy-Concerned Cross-Domain Service Access. In Proceedings of the 2019 IEEE Intelligent Vehicles Symposium (IV), Paris, France, 9–12 June 2019; pp. 1961–1967. [CrossRef]
127. Lee, S.; Choi, J.; Kim, J.; Cho, B.; Lee, S.; Kim, H.; Kim, J. FACT: Functionality-Centric Access Control System for IoT Programming Frameworks. In *Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies (SACMAT '17 Abstracts)*; Association for Computing Machinery: New York, NY, USA, 2017; pp. 43–54. [CrossRef]
128. Hazra, S. Smart ATM Service. In Proceedings of the 2019 Devices for Integrated Circuit (DevIC), Kalyani, India, 23–24 March 2019; pp. 226–230. [CrossRef]
129. Tandon, L.; Fong, P.W.L.; Safavi-Naini, R. HCAP: A History-Based Capability System for IoT Devices. In *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies (SACMAT '18)*; Association for Computing Machinery: New York, NY, USA, 2018; pp. 247–258. [CrossRef]
130. Wen Shieng, P.S.; Jansen, J.; Pemberton, S. Fine-grained Access Control Framework for Igor, a Unified Access Solution to The Internet of Things. *Procedia Comput. Sci.* **2018**, *134*, 385–392. [CrossRef]
131. Xiong, S.; Ni, Q.; Wang, L.; Wang, Q. SEM-ACSIT: Secure and Efficient Multiauthority Access Control for IoT Cloud Storage. *IEEE Internet Things J.* **2020**, *7*, 2914–2927. [CrossRef]
132. Wu, F.; Li, X.; Xu, L.; Sangaiah, A.K.; Rodrigues, J.J. Authentication Protocol for Distributed Cloud Computing: An Explanation of the Security Situations for Internet-of-Things-Enabled Devices. *IEEE Consum. Electron. Mag.* **2018**, *7*, 38–44. [CrossRef]
133. Han, Z.; Liu, L.; Liu, Z. An Efficient Access Control Scheme for Smart Lock Based on Asynchronous Communication. In *Proceedings of the ACM Turing Celebration Conference—China (ACM TURC '19)*; Association for Computing Machinery: New York, NY, USA, 2019. [CrossRef]
134. Fremantle, P.; Aziz, B. Cloud-based federated identity for the Internet of Things. *Ann. Telecommun.* **2018**, *73*, 415–427. [CrossRef]
135. Ben Daoud, W.; Meddeb-Makhlouf, A.; Zarai, F. A Trust-based Access Control Scheme for e-Health Cloud. In Proceedings of the 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), Aqaba, Jordan, 28 October–1 November 2018; pp. 1–7. [CrossRef]
136. Cui, J.; Wang, F.; Zhang, Q.; Xu, Y.; Zhong, H. An Anonymous Message Authentication Scheme for Semi-trusted Edge-enabled IIoT. *IEEE Trans. Ind. Electron.* **2020**, *68*, 12921–12929. [CrossRef]
137. Vorakulpipat, C.; Takahashi, T.; Rattanalerdnusorn, E.; Thaenkaew, P.; Inoue, D. Usable and Secure Cloud-based Biometric Authentication Solution for IoT Devices. In Proceedings of the 2018 IEEE Symposium on Computers and Communications (ISCC), Natal, Brazil, 25–28 June 2018; pp. 274–277. [CrossRef]
138. Li, G. Security Architecture of Computer Communication System Based on Internet of Things. In *Proceedings of the 2020 International Conference on Aviation Safety and Information Technology (ICASIT 2020)*; Association for Computing Machinery: New York, NY, USA, 2020; pp. 693–697. [CrossRef]
139. Gur, S.; Demir, S.; Simsek, S.; Levi, A. Secure and Privacy-Aware Gateway for Home Automation Systems. In *Proceedings of the 13th International Conference on Security of Information and Networks (SIN 2020)*; Association for Computing Machinery: New York, NY, USA, 2020. [CrossRef]
140. Gong, B.; Wang, Y.; Liu, X.; Qi, F.; Sun, Z. A trusted attestation mechanism for the sensing nodes of Internet of Things based on dynamic trusted measurement. *China Commun.* **2018**, *15*, 100–121. [CrossRef]
141. Gwak, B.; Cho, J.H.; Lee, D.; Son, H. TARAS: Trust-Aware Role-Based Access Control System in Public Internet-of-Things. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 74–85. [CrossRef]
142. Chen, H.C. Collaboration IoT-Based RBAC with Trust Evaluation Algorithm Model for Massive IoT Integrated Application. *Mob. Netw. Appl.* **2019**, *24*, 839–852. [CrossRef]
143. Foundation, P.S. Pdftotext. 2021. Available online: https://pypi.org/project/pdftotext/ (accessed on 12 July 2021).
144. Foundation, P.S. Rake-Nltk. 2021. Available online: https://pypi.org/project/rake-nltk/ (accessed on 12 July 2021).

145. Jin, X.; Krishnan, R.; Sandhu, R. A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC. In *Data and Applications Security and Privacy XXVI*; Cuppens-Boulahia, N., Cuppens, F., Garcia-Alfaro, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 41–55.
146. Ferraiolo, D.; Kuhn, R. Role-Based Access Control. In Proceedings of the 15th National Computer Security Conference, Baltimore, MD, USA, 13–16 October 1992; pp. 554–556.
147. Rosslin, J.; Robles, R.; Kim, T.H. Review: Context Aware Tools for Smart Home Development. *Int. J. Smart Home* **2010**, *4*, 1–12.
148. Jones, M.; Bradley, J.; Sakimura, N. JSON Web Token (JWT). RFC 7519, RFC Editor. 2015. Available online: http://www.rfc-editor.org/rfc/rfc7519.txt (accessed on 12 July 2021).
149. Wohlin, C.; Runeson, P.; Höst, M.; Ohlsson, M.C.; Regnell, B.; Wesslén, A. *Experimentation in Software Engineering*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2012.