Hindawi
Security and Communication Networks
Volume 2018, Article ID 4351603, 17 pages
https://doi.org/10.1155/2018/4351603

Review Article

Survey of Authentication and Authorization for the Internet of Things

Michal Trnka ,[1] **Tomas Cerny** ,[2] **and Nathaniel Stickney**[2]

[1]*Department of Computer Science, FEE, Czech Technical University in Prague, Prague, Czech Republic*
[2]*Department of Computer Science, Baylor University, Waco, TX, USA*

Correspondence should be addressed to Michal Trnka; trnkami1@fel.cvut.cz

Received 30 January 2018; Revised 20 April 2018; Accepted 10 May 2018; Published 12 June 2018

Academic Editor: Ilsun You

The Internet of Things is currently getting significant interest from the scientific community. Academia and industry are both focused on moving ahead in attempts to enhance usability, maintainability, and security through standardization and development of best practices. We focus on security because of its impact as one of the most limiting factors to wider Internet of Things adoption. Numerous research areas exist in the security domain, ranging from cryptography to network security to identity management. This paper provides a survey of existing research applicable to the Internet of Things environment at the application layer in the areas of identity management, authentication, and authorization. We survey and analyze more than 200 articles, categorize them, and present current trends in the Internet of Things security domain.

1. Introduction

Computer networks trace back to the early 1960s [1, 2]. TCP/IP, perhaps the most widely known protocol, was initially proposed in 1974 [3] and widely adopted in the early 1980s, allowing the widespread adoption of the Internet and its commercial use in the late 1980s [4]. In the beginning, the Internet connected only computers together, but in the 2000s, mobile devices began connecting to the Internet [5], and today network connection is available in more and more devices, which are called "smart objects" [6]. The current state is known as the "Internet of Things" (IoT) [7]. The forecast for the year 2020 is that the IoT will connect 20.5 billion devices with over three trillion US dollars spent on the hardware alone [8].

Security and privacy are considered the most crucial IoT challenges [7, 9]. Gartner [8] states, "security and risk concerns will continue to be the greatest impediment to IoT adoption. The market for IoT-specific security solutions will dramatically expand in 2017 as existing security providers aggressively retool existing capabilities to address IoT security risks."

This paper presents an overview of existing research in the areas of authentication, authorization, and identity management accomplished since 2013. The main focus areas in this work are security at the application layer, device management, and access rule enforcement. It excludes network and communications security. Candidate papers are identified not only by manual survey, but also by a systematic search [10] through multiple research indexing sites and portals. The resulting papers are analyzed to provide a survey and classification of existing work.

Other surveys of IoT security research exist. Sicari et al. [11] present existing solutions in seven categories: authentication, confidentiality, access control, privacy, trust, secure middleware, mobile security, and policy enforcement. Their survey summarizes state of the art in 2014 and does not include the most recent findings. Roman et al. [12] focus on security issues in a comparison of centralized and distributed architectures for IoT systems, both listing issues of the architectures, and outlining promising solutions to those issues as of 2013. Yang et al. [13] describe authentication and access control at the application layer, and security at the perception, network, and transport layers. We focus specifically on authentication and authorization at the application layer. Our survey employs a systematic search within the most prominent indexers. This way, our results are repeatable and not subjectively biased.

This paper provides an overview of basic authentication, authorization, and identity management techniques in Section 2. We define research goals and research questions to be answered in Section 3, and in Section 4 we describe our methods for paper discovery and selection, as well as the number of papers found. We categorize the research in Section 5 and further describe our categorization findings in Sections 5-8. In Section 10 we discuss threats to the validity of our survey.

2. Background

Initially computers were used as advanced machines to process various calculations or other processes without storing input or output data. While the systems supported multiple users, no data were stored, so security issues were not prevalent. However, when computers began to be used for data management and storage with multiple users accessing the system, the problem of access control emerged.

From the 1970s on, two predominant access control models were used: Mandatory Access Control (MAC) and Discretionary Access Control (DAC) [57]. MAC is predominantly used in applications with strict, centralized access control. Access rules are set by administrators and enforced by the system; users are not allowed to set or modify access policies for system resources. DAC is the opposite; no central element is needed and each user determines for the access policy for resources which they own.

As the complexity of applications increased, and they evolved into complex information systems with hundreds or thousands of users, a conceptual framework for easier access management was needed. Role-Based Access Control (RBAC) [58] allows grouping users together into groups, known as roles; each user may be assigned multiple roles. Access rules are further defined for the roles, and not single users. Roles often follow the organizational structure of the institution using the information system and are therefore easy to understand for business owners of the application. RBAC was introduced in the early 1990s and quickly became the predominant access control model.

As application user base sizes have continued to grow, the limitations of RBAC have become more apparent, including its unsuitability for context-aware applications [59] or for applications at a scale where the number of roles or role sets needed to cover different access right combinations is too extensive for manual management. Researchers have moved in two directions to address these issues. One direction is to extend the RBAC model in creative and numerous ways [60–65]. The other is to develop a more general access control model. Specifically, there is a growing interest in Attribute-Based Access Control (ABAC) [66]. It bases access rules on the user's attributes, rather than on predefined roles. ABAC can preserve all of the benefits of MAC, DAC, and RBAC while adding more flexibility; it can be used to support, or be implemented under, any of these access control paradigms.

The access control methods described above deal predominantly with authorizing users to access specific resources or take specific actions, rather than describing how the user should be authenticated; authentication is considered a prerequisite for authorization. This authentication may be accomplished using three basic credential categories. The first category, "Something I am", represents properties about the user, including their location or biometric characteristics. "Something I have" stands for credentials that were given to a user; the user possesses the credential. This category includes all types of keys, tokens, cards, or even personal devices like phones. The last and most familiar category is "Something I know", most often represented by passwords, but not limited to them; it also includes the user's knowledge of security questions, their interaction history, and other information.

Authorization credential categories may be combined together for increased security or to improve the user experience. Multifactor authentication is a common practice to increase security and prevent a breach in the event that a single credential is compromised. Some authentication frameworks provide single sign-on functionality where users sign into a trusted authentication provider using their credentials (often just a password) and receive provisional tokens which are then used to authenticate against other services. Subsequently, those services verify the token with authentication provider and log the user in. Often, the usage of the token is automated, and the user only needs to log in once.

Identity management is closely related to authentication and authorization. A virtual identity must exist against which users may authenticate and which stores user attributes (unique identification, attributes as understood in ABAC, RBAC roles, and other required information) used for authorization.

At the most basic level, applications each manage identity independently, using as little information as possible; generally this includes both a principal (identity unique identifier) and credentials used for authentication. As applications become more complex, the information required for user authorization grew to include roles or identity attributes. As the number of applications per user and the number of users per service increase, it becomes difficult both for the user and service administrators to manage the growing amount of identity information required. These developments led to the need for federated identity management—a way of providing identity services for multiple applications, often tied to authentication mechanisms. Currently, several implementations of federated identity management exist, including using LDAP [67] for identity management or using OpenID [68] as an identity service.

3. Goals

The motivation of this survey is to provide an overview of current progress on research in the domain of IoT security. This is a broad discipline and therefore we focus particularly on authorization, authentication, and identity management papers, specifically at the highest layer of the network stack, typically the application layer. While "network stack" is not the precise model used for the IoT, we use the term in lieu of a more standard vocabulary to describe the IoT technology and communication architecture; there does not yet appear to be common agreement on such a term. We are interested in architectures, projects, solutions, proposals, and frameworks dealing with user-to-machine and machine-to-machine authentication and authorization. We are also interested in identity management for IoT devices.

In this paper, we raise the following specific research questions:

RQ1 What is the taxonomy of security solutions?

RQ2 How does context-awareness extend security?

RQ3 Are existing approaches and standards adapted and extended for IoT security, or are novel methods proposed?

RQ4 Which approaches are applicable to distributed or centralized architectures?

RQ5 Does existing research focus on user-to-machine or machine-to-machine interactions?

The questions above are examined further in their respective sections. Each section provides a list of the research found, a summary of its content, and an answer to the particular question.

4. Search

In order to systematically review existing research and answer our research questions, we performed searches at the following indexing sites and portals: IEEE Xplore, ACM Digital Library (ACM DL), Web of Science (WoS), SpringerLink, and ScienceDirect.

To show that our search queries provide results relevant for this survey, we evaluated our search query results against a control set of papers identified as matching our scope through manual search before we performed the search queries. When a search query returned papers from the control set, this is evidence of the usefulness of the search query.

The search query consists of two parts. The first part targets terms and keywords to be included in the paper and the second part removes papers that contain terms we are not interested in. Naturally, we are interested in research about the IoT so we include "Internet of Things" or "IoT" as one of the main groups. Another crucial term is "Security" as we target only those papers that deal with security. Further restriction terms refine the results to include only papers with "Authentication", "Authorization", "Access Control", or identity management, which is shortened to "Identity". The second portion of the query is to limit the amount of the articles in the result set. We removed papers that deal with the security at the lower levels of the network stack. This translates to the terms "Network", "Hardware", "RFID", and "protocol". Cryptography is not a particular focus of this survey, so we also remove research with this keyword. Finally, we remove papers that are surveys themselves, containing "Survey" or "Study" in their title.

The query syntax differs for each indexing site, but we aim to search through abstracts or keywords/topics where applicable. The queries are constructed as similarly as possible. The exact queries used, including the general query we used as a template, are listed in Table 1.

We encountered an issue with the search function in SpringerLink. The search system is not able to process a refined query such as the one we designed. We used a simpler query that returned 383 papers and processed these results by constructing a short script that opens the particular page for every exported paper, extracts the abstract, and performs the refined query locally on our machine.

Running the query across all five indexing services gives us a set of 387 papers, from which we exclude those that have less than 4 pages or are from year 2012 or earlier. Since WoS indexes papers that appear at other sites, it contains 16 duplicate papers, which we also remove. As a final filter, we read the abstract of each article and removed those papers not within the designed scope; this gives us 86 prefiltered candidate papers.

These remaining papers we read one by one, with some exceptions. The full text of one paper could not be downloaded; this was removed from the results set. Three of the papers were highly-similar extensions of another paper in the results set. In this case, we used the extended paper and discarded the shorter versions. We also removed papers that did not fit into the scope of this survey—those where the abstract initially indicated connection to our research questions but the full text did not. The complete statistics of papers found, prefiltered, and included for every indexing site can be seen in Table 2.

5. Taxonomy

To find candidate categories based on the most prevalent keywords we employ the RAKE [69] algorithm for keyword extraction. First, we transform the PDF documents using *pdftotxt* (5) and strip references or appendices. Then, we apply the RAKE algorithm with the following parameters for the keyword extraction: at least five characters, a maximum of two words for the keyword, and at least four occurrences in the text. For each keyword, we then find matching articles. Only keywords present in at least two papers are taken into consideration. We then group synonymous keywords into categories. As a consequence of this approach a paper may fall into multiple categories.

The results (excluding general terms) suggest the following categories of the papers. They are also illustrated in Figure 1.

(i) **authentication:** papers that address authentication [14–35]

(ii) **authorization:** articles dealing with authorization [18, 20, 21, 23, 26, 28, 30, 32–34, 36–45]

(iii) **service:** solutions that can be used in both IoT and SOA [15–17, 21–23, 25, 27, 30, 32, 35, 36, 46–49]

(iv) **token:** articles that use any form of token as an information bearer in their proposal [19, 21, 23, 29, 35–37, 40, 41, 43, 46, 50]

(v) **context:** papers using or proposing context-aware methods [14, 23, 33, 35, 36, 38, 46, 51–53]

(vi) **cloud:** research addressing security issues of cloud-based IoT devices [14, 16, 20, 41, 45, 51, 53, 54]

(vii) **identity management:** solutions discussing identity management [15, 18, 22, 34, 35, 46, 47, 50]

Table 1: 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 ”Abstract”: ”Identity” OR ”Abstract”:”Access Control”) AND ”Index Terms”: ”Security” AND NOT(Search_Index_Terms: ”Network” OR ”Abstract”: ”Hardware” OR ”Abstract”: ”Cryptography” OR ”Abstract”: ”Protocol” OR ”Document Title”: ”Survey” OR ”Abstract”: ”RFID” OR ”Document Title”:”Study”))
ACM DL	recordAbstract:(IoT ”Internet Of Things”) AND recordAbstract:(Authentication Authorization Identity ”Access Control” -Hardware -Cryptography -Protocol -RFID) AND acmdlTitle:(-Study -Survey) AND keywords.author.keyword:(-Hardware -Physical -Network)
WoS	(”internet of things” OR IoT) AND TOPIC: (Security) AND TOPIC: (Authentication OR Authorization OR Identity OR ”Access Control”) NOT TOPIC: (Hardware OR Cryptography OR Protocol OR RFID OR Physical OR Network) NOT TOPIC: (Study OR Survey)
SpringerLink	(Authentication OR Authorization OR Identity OR ”Access Control”) + title (”Internet of Things” OR IoT)
ScienceDirect	TITLE-ABSTR-KEY(”Internet of Things” OR ”IoT”) AND TITLE-ABSTR-KEY(Authentication OR Authorization OR Identity OR ”Access Control”) AND KEY(Security) AND NOT (TITLE-ABSTR-KEY(Hardware OR Cryptography OR Protocol OR RFID) OR title(study OR survey) OR key(Physical OR Network))

Table 2: Number of articles processed in the survey.

Indexer	Results	Prefiltered	Relevant
IEEE Xplore	120	29	15
ACM DL	84	9	7
WoS	67	31	13
SpringerLink	33	8	6
ScienceDirect	27	9	2
Total	331	86	43

(viii) **healthcare:** projects that specifically address the healthcare domain [18, 22, 28, 32, 41, 53]

(ix) **attribute-based** subset of authorization proposals that involve ABAC [15, 28, 32, 34, 38, 53]

(x) **roles:** subset of authorization proposals that involve RBAC [18, 28, 29]

Two of the papers do not fit into any of the above categories [55, 56]. One article [55] is likely too short for RAKE to perform any meaningful analysis; with the second article [56], we do not identify any obvious reason for not being categorized. Nevertheless, both of the papers address authentication and we have included them in this category.

In total, over 50% of the articles get two or three keywords. Significant number of research papers fit into one or four categories. Two papers did not fit any category, and another three fit to five categories. This statistic is shown at Figure 2. As illustrated in Figure 3, research covered by this survey shows evident increase of interest in IoT security based on the amount of articles published, from a single paper in year 2013 through 4 in 2014 up to 11 in the 2015. There is a small decrease to 10 research publications in 2016. Year 2017 exhibits again growth to 17 papers for only 3 quarters of the year.

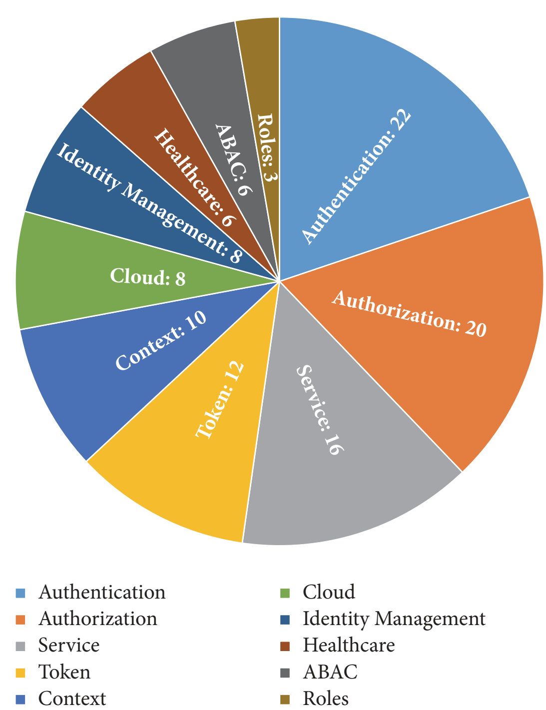

Figure 1: Number of keywords found across all articles.

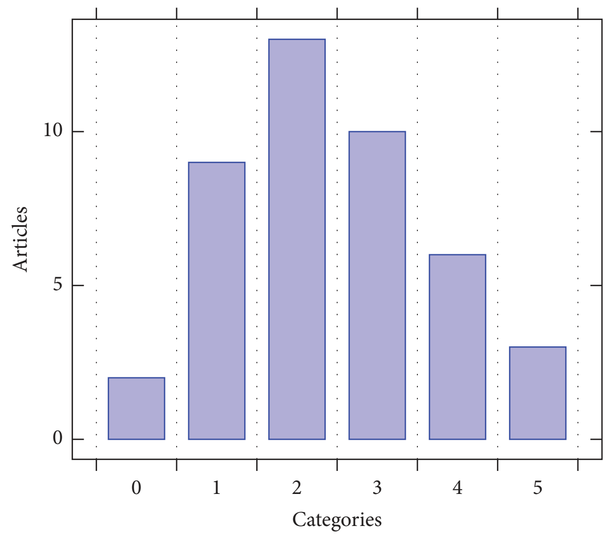

Figure 2: Number of categories suggested by RAKE per article.

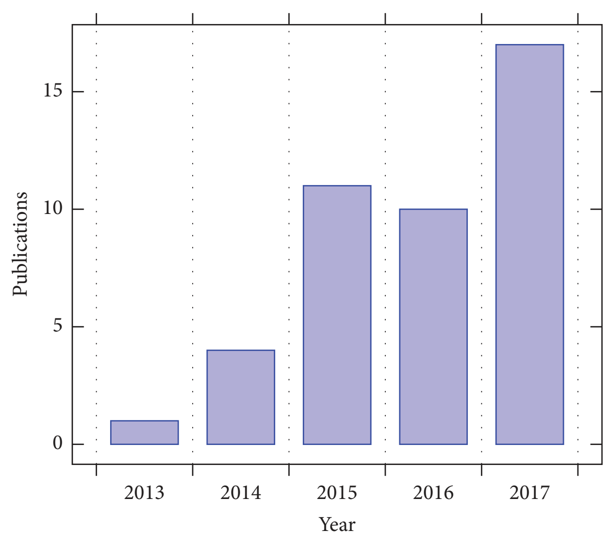

Figure 3: Number of publications per year. *Note that 2017 data is only through September*.

The authentication, authorization, identity management, and services categories are described in the subsequent subsections as they are the most populous categories. Articles with context-awareness elements are further described in their own section, which answers RQ2.

5.1. Authentication. Authentication is addressed by 22 papers from our pool—more than half of the articles in the survey. Authentication is the process of confirming an attribute claimed by an entity. In the vast majority of cases, it is confirmation of identity that the entity claims using credentials.

Traditional authentication methods, enhanced with multifactor authentication based on a location, are described in [14]. Their system considers user location, and they develop an additional factor for multifactor authentication which ascertains the physical possibility of a user being in a particular location; e.g., a user cannot possibly be in Los Angeles if they just logged in from New York. This adds additional security without requiring the user to perform extra actions.

In [15], the authors suggest enhancing privacy during authentication by basing authentication on attributes, rather than identities. A trusted authority issues certificates which prove that an entity possesses a particular attribute; these certificates are used for authentication when communicating with other services. This scheme preserves both entity privacy and the advantages of centralized identity management.

The authentication model for cloud-based IoT is elaborated by Barreto et al. [16]. Their solution supports two stages of authentication: one for basic and a second one for advanced access, e.g., administrative purposes. They do not describe specifically how the authentication should be done; rather they specify methods that cloud services should provide for authentication.

To achieve efficient and smart authentication of IoT devices, Cagnazzo et al. [17] suggest using Quick Response (QR) codes, specifically XignQR [70]. Every device has a printed QR code that contains important information about it, e.g., an ID representing its service provider, authentication server address, and digital signature. Scanning the QR code and sending it to the authentication manager allow the manager to decide which authentication method it should enforce on the user. This approach can be useful when physically managing large amounts of devices at the same location, e.g., in a hospital or in a factory.

A security framework following the Architecture Reference Model (ARM) [71] is described in [21]. It bases authentication on the Extensible Authentication Protocol (EAP) over LAN [72]. EAP is widely used and recognized as a mechanism to provide flexible authentication through different EAP methods. Those methods allow an EAP peer to be authenticated by an EAP server through EAP authentication for network access. While their work proposes interesting solutions, they do not provide any case study or usability study.

Kumar et al. [22] assume that the best authentication method for wearables and nearables (devices which are not worn, but are generally close to the user) is the biometric information of their owner. The proposed solution requires the user to register their biometric characteristic(s) in person with the authentication provider. Later, access points close to the user—wearables or nearables—capture the user's biometric information and authenticate them by comparing those characteristics with the registered characteristics. However, there is an issue with privacy as many users are reluctant to share their personal information.

Two almost identical works proposed the OpenID protocol as the method of authentication in the IoT environment [23, 29]. They describe a central service issuing tokens and communicating through a RESTful API [73] over the HTTP(s) [74] protocol, allowing rapid development and acceptance among IoT devices as all technologies used are proven, well-documented, and widely supported. A downside is that the OpenID protocol was not designed with IoT usage in mind and can be more demanding of computation and network resources than specialized protocols.

Another framework [24] for authentication is formally described using process algebra, specifically CSP [75]. The framework contains three authentication forms. An *entity* authentication is the capability of verifying the identity that the entity claims. An *action* authentication refers to authentication of the actions of devices and whether they are allowed. A *claim* authentication verifies the authenticity of devices' claims about previous actions. It also has three strength levels for each form—weak level, noninjective level, and injective level. The paper does not provide any proof of concept or other kinds of demonstration of their solution.

A mechanism of HTTP(s)-based authentication for IoT devices using a hash-chain generated between server and the client is explained in [25]. This hash-chain is generated during the login process and serves as a One Time Password for the client to authenticate against services. If a device does not have the required capabilities (battery lifetime, computational power, network connection, etc.) to generate the hash-chain, or those capabilities are in use for other functions, another device acting as a proxy may be used to generate the hash-chain.

Continuous authentication of personal IoT devices is addressed by Shazad et al. [26]. Current practice is to authenticate an entity just once when a session is established and keep them authenticated until some timeout occurs, or the session is otherwise closed. This session persistence presents a potential security risk. The authors divide devices into two categories: those which maintain physical contact with the user and those which do not. Devices that keep contact can be authenticated using various biometric information, both direct (blood flow rhythm) and indirect (using inertia measurement unit to check a user's gait). For devices that are not in physical contact with the user, the authors propose using radio frequency signals. For example, Wi-Fi signals are reflected by the human body and the resulting distortions can be measured and used to determine users' walking speed, gait cycle, and other physical properties.

Advanced authentication methods better than the current approaches are suggested in [27]. Most of the traditional methods have flaws or were not designed to be frequently used (e.g., passwords—almost no one can memorize strong and unique passwords for every service or device they use, so users reuse their passwords). Their proposal is based on users' digitized memories. Users would authenticate themselves against their digitized memories based on date and time, place, people or pets, devices, habits, audio, or ownership recognition. They map different suitable methods, including choice selection, alphanumeric input, image part selection, or interactive categorization.

Wiseman et al. [31] present a niche but interesting problem along with a solution. They address the issue of pairing an IoT device with its "master" account. Connecting from devices using a password can be difficult or even impossible because of the lack of a proper input method. One method to avoid this is to let the device display an access code and add the access code to the master account. They examine this process from a user experience perspective and compare convenience between alphanumeric codes and codes generated from human-readable words.

A privacy-preserving, decentralized identity management framework for the IoT is presented in [35]. Identity in the IoT is extended not only to users but also to IoT devices themselves using an ARM-compliant, claims-based approach built on top of Identity Mixer technology [76]. They define partial identities as subsets of user or device virtual identities that preserve privacy while being sufficient to provide identity confirmation. They show a use of their framework with Distributed Capability-Based Access Control [21]. Identity attributes are disclosed by specific proof and are employed during authorization based on XACML rules to obtain capability tokens used to access a service.

Finally, there is a group of papers [18–20, 28, 30, 32–34] that address authentication tangentially either as part of a broader and more complex framework or project, or to solve authentication issues as a side effect of dealing with another problem.

Table 3 presents an overview of authentication research, reflecting the information we extracted from the papers. It shows which solutions support centralized and decentralized architectures, which are oriented for user-to-machine (U2M) or for machine-to-machine (M2M) communication, which possess at least some elements of context-awareness, the paper's primary domain, or which authentication factor is used for the primary authentication ("Inherence" is "Something I am"; "Possession" is "Something I have"; "Knowledge" is "Something I know").

5.2. Authorization. Authorization is the process of granting permissions on specific actions to given entities—in our scenario specifically to users, devices, or applications. There are a total of 20 articles in the identified pool addressing this topic. Authorization ties with services as the second most populous category.

Access control based on trust in an ARM-compliant model is proposed by [36]. It describes various levels of trust, a multidimensional attribute which describes various concerns in the network the authors call dimensions: quality of service (including network availability and throughput), security (authentication and authorization protocols, encryption, etc.), reputation (recommendations from other devices), and social relationship (the group or groups of IoT devices to which an individual device belongs, e.g., those made by a certain manufacturer or currently in a particular location). This trust is used for final authorization within the environment.

The authors of [18] describe a complex framework for use in the healthcare field. They employ a version of RBAC where a user, specifically a patient, grants permission to access his data based on a particular role—a group of doctors and nurses. A centralized authentication server enforces the resulting security rules.

Another paper [37] develops an authorization architecture based on IoT-OAS [77], authenticating users using tokens similar to those used in OpenID. Every device has a designated owner and a set of actions or permissions. Users may request and share permissions with one another; multiple operational cases are described in the paper.

Gerdes et al. [20] tackle the problem of authorization and authentication for devices with constrained computational

Table 3: Summary of authentication articles.

Article	Centralized	Decentralized	U2M	M2M	Context-aware	Factor	Domain	Specifics
[14]	Yes	Yes	Yes	No	Yes	Inherence	Any	Service answering whether user can be in the given location
[15]	Yes	Yes	Yes	Yes	No	Possession	Any	Use of attributes for authentication
[16]	Yes	No	Yes	Yes	No	N/A	Cloud	Authentication through cloud
[17]	Yes	Yes	Yes	No	No	N/A	Any	Reading QR codes physically present on a device
[18]	Yes	Yes	N/A	N/A	No	Knowledge	Healthcare	Framework designed to preserve patient privacy
[19]	Yes	No	Yes	Yes	No	Knowledge	Any	Adjustment of Web API management; OpenID Connect
[20]	No	Yes	Yes	Yes	No	Possession	Any	Authentication for devices with constrained computational power
[21]	Yes	No	No	Yes	No	Knowledge	Any	ARM compliant; EAPoL; RADIAL
[22]	No	Yes	Yes	No	No	Inherence	Healthcare	Biometric from wearable and nearables
[23]	Yes	No	Yes	Yes	No	N/A	Healthcare	OpenID Connect
[24]	Yes	No	Yes	Yes	No	N/A	Any	Authentication framework mathematical description using CSP algebra
[25]	Yes	No	Yes	Yes	No	N/A	Any	HTTPS-based device authentication using hash chain as One Time Password
[26]	N/A	N/A	Yes	No	Yes	Inherence	Any	Biometric; continuous authentication
[27]	Yes	No	Yes	No	Yes	Knowledge	Any	User's electronical history
[28]	Yes	No	Yes	Yes	No	N/A	Healthcare	Authentication based on attributes
[29]	Yes	No	Yes	Yes	No	Knowledge	Any	OpenID Connect
[30]	N/A	N/A	No	Yes	No	N/A	Any	WS-Security adaptation for IoT
[31]	N/A	N/A	Yes	No	No	Knowledge	Any	One time passwords using words chosen by a user
[32]	Yes	No	Yes	Yes	No	Possession	Healthcare	Full security framework
[33]	No	Yes	Yes	Yes	No	N/A	Any	Blockchain access control framework
[34]	N/A	N/A	No	Yes	No	Possession	No	Authentication on perception level
[35]	No	Yes	Yes	Yes	Yes	Knowledge	Any	Privacy preserving based on partial identities

power. The authors divide IoT devices into the categories "constrained" and "less-constrained" based on resource availability and allow less-constrained devices to perform some authorization functions on behalf of the constrained devices. The paper includes basic methods for these authorization management tasks, and "principal actors", which represent the person or company that owns the specific device or the data on the device, must set appropriate policies for each situation about which tasks can or cannot be offloaded.

One solution to the problem of data access control across a shared network is developed in [38]. The authors use Ciphertext-Policy Attribute-Based Encryption [78] and enhance it with a set of policy descriptions in a XML file. Access policies are based on entity attributes and structured as a binary tree with "And" and "Or" operations available. Entities present a keyserver with a list of their attributes, and the keyserver generates a key which can only decrypt data to which the listed attributes allow access.

A framework introduced in [21] supports not only authentication but also authorization, enabled by creating an Authorization Server which issues access tokens according to security rules stored in XACML [79], an XML schema for representing authorization and entitlement policies. Entities request authorization tokens based on their attributes and then use the tokens to access services provided by or data stored on another server or device.

Kurniawan et al. find classic security strategies unsuitable because they are centralized and scale poorly in the IoT environment. They propose a trust-based model [39] based on Bayesian decision theory. The authors compute Bayesian trust values based on three inputs: experience (the history of interactions between the actors), knowledge (what is already known about the entity and the context), and recommendation (how much trusted peers trust the entity in question) and use these trust values as input to a loss function that determines the cost of an action. Access control decisions are made based on the output of the loss function, given a particular trust value.

Two proposals based on the existing OAuth protocol [80] use tokens that encode the access rights (e.g., roles or attributes) of the token owner and a configurable lifespan. The first method [41] uses JSON Web Tokens [81]; the second proposal [23] uses a special token format which allows a limited number of accesses. Both proposals communicate through a RESTful API.

Another framework for securing API-enabled IoT devices in smart buildings [43] is also inspired by OAuth and uses JSON Web Tokens. The proposed security manager is split into two services to enable better scalability. The first service is an authentication manager which authenticates users or services with a process similar but not identical to OAuth and issues a JSON Web Token. The second service is an access control manager that verifies whether the access is allowed, based on XACML rules set by the system administrator and the identity of the requesting side (which is provided by the token).

Blockchain technology is used in [40] to store, distribute, and verify authorization rules. Every node in the network has a full database of all access control policies for each resource-requester pair in the form of transactions. Access is granted by giving a token to the requester entity and propagating it in the blockchain. The blockchain also serves as an auditing and logging tool. Trust in the network is based on the distributed nature and large size of that network; it is very difficult to gain unauthorized access or disable the network by attacking a central element. A slightly different approach using blockchain is presented in [33]. Rules based on OrBAC [82] are distributed through a block chain, and based on the history of the communication, the rules are updated with reinforced learning algorithms.

Tasali et al. [28] discuss current standards for healthcare devices, including Integrated Clinical Environment (ICE) [83] and Medical Application Platform (MAP) [84]. The conclusion is that they barely address authorization and authentication (if they address it at all). Their solution is based on ABAC, enhanced with attribute inheritance inspired by RBAC. Attribute inheritance allows "plug-and-play" configuration of new devices based on device types represented as attributes preset on the devices.

Another option is to isolate each function of the device and provide access just to that functionality [28]. Functionalities are slightly similar to the concept of micro services. The proposed functionality-centric access control framework also reduces application level attacks on "misused functionality" or "reduced functionality".

A proposal for energy constrained devices called Time Division Multiple Access is described in [44]. The schema is well suited for sensors with known communication patterns, such as a repeating communication schedule in which sensors periodically report data. The proposed communication scheme optimizes the tradeoff between device lifetime and distortion of the data transmitted. Another different application of ABAC focused on reducing storage and communication overhead is described in [34].

Sicari et al. provide a full specification for a security framework for smart healthcare [32]. It describes three main points (locations) for policy enforcement, a policy administration point, a policy enforcement point, and a policy decision point. The access roles are described using XML in a format inspired by ABAC.

Another access control model for IoT running in the cloud [45] secures data using hierarchical attribute-based encryption. The encryption is done in two steps. The first part of encryption is done on the device; the secondary encryption is done on the gateway. This reduces the load on the device. Decryption is likewise split between the cloud and the device in order to save application resources. The hierarchical nature of the encryption scheme allows updating security policies using an update key based on information from the data source, without the device itself needing to reencrypt the data.

Two of the reviewed papers [26, 30] discuss authorization only tangentially. The complete overview of authorization research can be seen in Table 4.

5.3. Identity Management. Identity can be viewed as a set of user's attributes, both virtual or real. Identity management is the mechanism of storing and retrieving user identities. Typically, users are forced to have more unconnected identities for

Table 4: Summary of authorization articles.

Article	Centralized	Decentralized	U2M	M2M	Context-aware	Policies creator	Domain	Policies based on	Specifics
[18]	Yes	Yes	N/A	N/A	No	Data creator	Healthcare	Roles	Rules tied to the data
[20]	No	Yes	Yes	Yes	No	Resource owner	Any	N/A	Constrained devices
[21]	Yes	No	No	Yes	No	Administrator	Any	N/A	ARM compliant; describes access control generally
[23]	Yes	No	Yes	Yes	No	Administrator	Any	N/A	OAuth; tokens
[26]	N/A	N/A	Yes	No	Yes	N/A	Any	Data itself	Biometric information used
[28]	Yes	No	Yes	Yes	Yes	Administrator	Healthcare	Attributes	Supports with attribute inheritance
[30]	N/A	N/A	No	Yes	No	Administrator	Any	N/A	WS-Security adaptation for IoT
[32]	Yes	No	Yes	Yes	Yes	Administrator	Healthcare	Attributes	Full security framework
[33]	No	Yes	Yes	Yes	No	Resource owner	Any	OrBAC	Reinforced learning to update rules
[36]	Yes	Yes	Yes	Yes	No	N/A	Any	Attributes	ARM compliant; Attributes extended with trust based on various concerns in the network
[37]	No	Yes	Yes	No	No	Resource owner	Any	Direct grants	Tokens; Possible to share permissions
[38]	No	Yes	N/A	N/A	Yes	Data creator	Any	Attributes	Data decryption only with correct attributes
[39]	No	Yes	N/A	Yes	Yes	System	Any	Bayesian decision	Bayesian decision theory for authorization
[40]	No	Yes	Yes	Yes	No	Resource owner	Any	Direct grant	Propagation through blockchain
[41]	Yes	No	Yes	Yes	No	N/A	Healthcare	N/A	OAuth; tokens
[34]	N/A	N/A	Yes	Yes	Yes	Resource owner	Any	Attributes	Perception layer framework
[42]	Yes	Yes	Yes	Yes	No	Resource owner	Any	Direct grant	Access control specified for functionalities
[43]	Yes	Yes	No	Yes	No	Resource owner	Smart building	Attributes	OAuth; XACML; tokens
[44]	N/A	N/A	No	Yes	No	N/A	Any	N/A	Constrained devices
[45]	Yes	Yes	No	Yes	No	Data creator	Cloud	Attributes	Gateway, device and cloud share data encryption

various services. In the IoT environment, the identity should be available for the whole IoT network, while preserving user's privacy, although it does not mean that each user must have single identity. The identity concept is also extended from users to include sensor identities in the IoT. Identity management is closely connected to authentication, which is process of verifying that a user (or a device) actually is the owner of that identity, as well as to authorization, which is the process of granting access to a resource based on user attributes (i.e., identity). Eight of the articles address identity or identity management at least partially.

Traditionally, user identity contains the principal along with credentials used for authentication. This renders a privacy risk, especially if the identity is shared with multiple services whose operators are not known in advance, and that might appear on and disappear from the network at any time in the dynamic IoT concept. Many of the articles tackle the problem of privacy by limiting a user's identity to only their attributes, without any unique information that could lead to disclosure of their identity. One of the proposals is for a trusted party to issue cryptographic containers containing user attributes [15]. It is not specified that the trusted party must be single entity in a network, so we can assume that multiple trusted parties can exist simultaneously. Also [50] proposes using attributes instead of identity for authorization. Gusmeroli et al. propose a slightly different approach with using capabilities instead of attributes [46]. This proposal also supports anonymous capabilities which allows authentication without disclosing identity.

The problem of assigning identity to devices is described in [47]. An IoT device inherits the identity of its user through various methods based on a relationship between the user and the device. They formulate methods for devices that are strictly connected to a single user, as well as identity extensions from users to devices that change users frequently.

A complete framework for decentralized identity management to enhance user privacy is introduced in [35]. It defines partial identities as the least sufficient subsets of full identities for a requesting service that do not disclose any unnecessary information about a user.

The principle of storing a user's biometric information in access points, serving like identity servers, and thus linking a real user's identity with his virtual identity through wearables is described in [22]. Two final articles [18, 34] deal partially with privacy and data transmission encryption.

5.4. Services. This section presents an overview of the solutions that either support IoT-as-a-service or provide security-as-a-service. This means that at a minimum the security client (an entity) or security provider follows the principles of Service Oriented Architecture (SOA) [85]. Frequently, both of the actors can be viewed as services. In this survey we have 16 research publications that include SOA compatibility, although not every paper in this category uses the term SOA or "service"; instead, they are frequently called by synonyms, e.g., "central entity", "authorization or authentication server", and so forth. Most of the centralized security approaches can be viewed as a service.

Most of the surveyed proposals contain an identity management, authentication, or authorization service. An application in the IoT environment may offload the authentication process to such a security service [16, 17, 21, 23, 27, 32, 35, 47]. A few proposals also allow the distribution of access rights or other properties used for authorization from the service to its clients [15, 21, 46]. Some of the services also provide additional features like enhanced user privacy [15, 25, 46]. They anonymize entity identities by hiding identity details from the service provider and guarantee the entity's identity by the trustworthiness of the identity management service itself.

Two of the papers in this category stand out. The first adapts the Web Service (WS) Security specification [86], which is intended for loosely coupled distributed systems, to the IoT environment by extending it to allow identity management functions to be offloaded from computationally "weak" devices to "strong" ones [30]. The proposed method, termed DPWSec, also simplifies the original WS-Security specification by removing unneeded portions: multihop security, statelessness, hosting and hosted devices, and the device profile communication model. The second paper describes a security framework within the scope of the Device Profile for Web Services using the XACML standard for rule description [49]. It describes three parts of the framework—the policy enforcement point (where the policies are enforced), policy decision points (where the policies are evaluated), and policy information points (where the audit logs are kept).

6. Context-Awareness

One trend in contemporary application development is a movement towards context-awareness. Context is defined by Abowd [59] as any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and the application themselves. In the context of the IoT it can be extended to not only interaction between a user and an application but also between two applications.

Solutions using context-aware security can provide a much better user experience as well as increased security [87]; often both can be achieved at the same time. Nevertheless, the level of interest in context-awareness from a security perspective has not reached the same level as interest from the user experience perspective, likely because computer security is traditionally a more conservative domain of computer science. In this section we focus on research that does speak to an interest in context-aware security.

Most common approach to achieve context-aware security is using ABAC. It differs from RBAC in that an entity (a user or a device) performing an action is not authorized based on matching the roles it is assigned to roles which allow certain actions. In ABAC, every action is mapped to a specific set of attributes an entity must possess in order to take that action. An example of such a rule for reading a document is that the entity must be from the same department as the creator of the document, must be employed in a management position, and must be located in the same building or complex.

One option is to specify access rules using ABAC for every piece of data at creation time and join those rules with the data so that during network transportation, updates, or copying, the rules stay consistent. In order to manipulate the data, an entity must possess the specified attributes [38]. Another method is to use a three-module architecture. The first module, a policy enforcement point, is responsible for invoking checks on access rules. The second, a policy information point, gathers information about an entity's attributes, including their context. Finally, a policy decision point compares security rules with the information gathered about the entity and decides whether the action is allowed or declined [28, 53]. Security rules can be written in XML using XACML [28] or using the Ontology Web Language [53]. While [32, 34, 48, 50] do not mention context information specifically, the ABAC implementations in those papers could also utilize context-aware attributes.

Instead of extending ABAC, another option is to adapt the well-described Capability-Based Access Control (CBAC) [88] architecture. A capability (known in some systems as a key) is a communicable, unforgeable token of authority. It refers to a value that references an object along with an associated set of access rights. This token may contain additional contextual rules, defined in XACML format, which must be satisfied for the token to be valid [46]. Variation on this is using Distributed Capability-Based Access Control [21] as described in [35].

A novel authorization architecture based on Bayesian decision theory [39] also considers context. The trust parameters of history, knowledge, and reputation (described in the Authorization section) may include contextual elements which are either acquired directly by the device itself or provided indirectly by a peer device. Machine learning techniques used to enhance access rights [33] also consider context in terms of a history of the previous interaction.

Biometric information may be considered "contextual" by definition, so biometric authorization is context-aware [22, 26]. Many devices, especially wearables, directly measure the user's physical traits (e.g., heart rhythm or body temperature). Other "nearable" devices can provide additional information such as weight or gait, both of which can be measured by video sensors. All of this information can be compared to a user's known physical or kinesiological properties.

Beyond simple biometric data, a user's digital life may be considered as context for identity management. A user's photos, videos, blog posts, and browsing history can be used to authenticate that user [27]. Given sufficient digital history, security questions can be devised which no one but the authentic user can answer. This has the benefit that the user does not need to memorize passwords or carry other credential material; their own memories are sufficient. Another similar proposal, which restricts context to information from network traffic, authenticates using contextual information provided by a smart home [51].

7. Existing versus Novel Approaches

Existing research projects in IoT security that propose an actual solution or method can be roughly aligned to two categories: those which extend or adjust existing architectures or programs to better suit the IoT environment and those which propose entirely new ideas to solve environment-specific problems. However, the classification is not strictly binary, and it is often difficult to judge the novelty of any particular proposal. The reader will note that all research is meant to be "novel"; we use the word here in a narrower sense to mean an entirely new approach which does not make use of existing technologies or standards.

The works we considered that apply or adapt existing technologies and methods from other security domains to the IoT environment often consider OAuth 2 technology [19, 24, 29, 41, 43]. Two proposals also adopt the WS-Security specification to IoT devices and communication between them [30, 49].

The most innovative solutions share some common properties. All of them are suitable for distributed use and none require administrator interaction. They can handle device connection and disconnection as well as security rule distribution and validation. Often the responsibility for creation of access rules is moved from administrators to data owners. Two papers show operation with trust between devices and dynamic calculation of trust among various communication partners [36, 39, 50]. One proposal adjusts ABAC to be more dynamic and allow a device to pick its own attributes; other devices must subsequently confirm that the device really does possess the claimed attribute. Security rules are set during data creation using ABAC and then connected to those data for its whole life-cycle [48]. Other innovative approaches suggest propagating all security rules through a blockchain in the network [40] and possibly update them based on reinforced learning algorithms [33]. Access would be granted for a specific entity to a given resource and distributed using blockchain as described earlier. One of the researches proposes access control based not on roles or attributes, but rather on functionalities of the IoT node [42]. Access control for cloud applications based on attributes [45] using computational power of sensor gateways and the cloud itself is suitable for constrained devices.

In summary, there are various novel proposals [33, 36, 39, 40, 42, 45, 48, 50], especially focusing on distributed solutions [33, 39, 40, 45, 48, 50], that potentially suit the IoT environment better in terms of scalability, maintainability, and flexibility, but due to their novelty it is difficult or impossible to predict which ideas might be adopted or see wide use. A significant amount of research [19, 23, 29, 30, 34, 41, 43, 49] is focused on adoption of existing technologies; all exhibit promising results.

8. Distribution versus Centralization

The IoT is a diverse, complex, and fast changing environment. It comprises a large number of devices that interact autonomously. Objects also appear and disappear autonomously and with high frequency. Given these differences from a more standard network environment, we focus in this section on what paradigms are used in the security solutions.

A conventional, centralized approach is very easy to set up, maintain, and audit for system administrators. It also

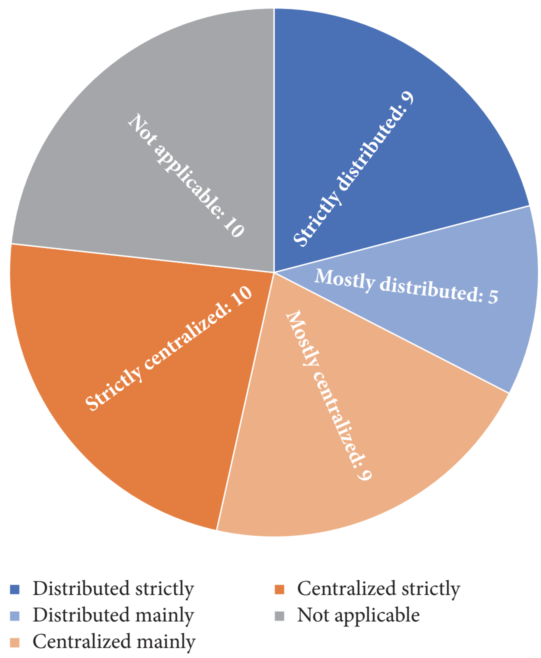

FIGURE 4: Categorization of distributed and centralized solutions.

presents a stable point in the network from which users and application can build trust. Implementing centralized solutions is simpler both for the central server and for applications using it. Many of the existing centralized solutions for networks and application can be extended to operate in the IoT environment without overly costly adjustments. However, using a centralized architecture in the IoT presents several drawbacks, including limited flexibility and scalability.

By contrast, the attributes of distributed architectures are completely opposite. They scale well and are built with flexibility as a main goal. However, synchronization, maintenance, and auditing present serious difficulties. There is also the issue that no single trusted central entity stands behind them, which may be required by business users, legal entities, or others.

To further complicate matters, the line between distributed and centralized solution is often not clear. While some solutions can be considered exclusively in one category, there are a significant number of proposals that may work under both paradigms. Figure 4 shows a chart of distributed and centralized solutions.

Requiring a central server for identity management prevents distributed operation for obvious reasons. Sometimes this limitation is imposed for domain-specific reasons (e.g., in the healthcare domain [18, 22, 32, 41]); other times it arises simply as a function of the technologies or methods employed [19, 23, 29, 51, 52]. In one proposal, the authentication method requires having as much historical data about an entity as possible, to the point that authentication data storage requirements make it impractical to host such data at multiple locations [27].

At the other end of the spectrum, the technologies used in some proposals specifically preclude centralization. For instance, methods which rely on the creators of data to specify security rules, or which grant access selectively, do not operate with a central server [20, 35, 37, 39, 48, 55]. Blockchain-based access rule verification [33, 40] also can not be centralized, and the same applies to extensions of the ABAC system which rely on peer devices to confirm an entity's attributes over the network [50].

Most of the ideas in the papers surveyed can be used in both centralized and decentralized architectures. Centralized solutions can be often decentralized by multiplying central elements [14–16, 21, 25, 28, 36, 42, 43], and decentralized proposals can be centralized by limiting the number of security control elements to single node [17, 38, 45, 46, 50]. Similarly, some of the research we reviewed [26, 30, 31, 34, 36, 44, 49, 52, 54, 56] cannot be categorized in either category. They work equally well for either architecture without modification and can be seen as complementary extensions for complex security solutions, helping with particular issues (e.g., authentication, auditing, context-awareness).

9. User versus Device-Centrism

In IoT two basic communication patterns exist: either users interact with devices, or devices interact among themselves. The first type is designated U2M category. The other scheme of communication is designated M2M. Some of the proposals fit both patterns; this section explains how the security models support particular communication models, and the limitations of those models.

One important restrictive factor is the need for human input to the interaction. In some cases, various information about the actual user is required for security reasons: biometric information [22, 26, 56], a user's digital history [27], or a user's location [14]. Other approaches require direct user interaction such as scanning QR codes [17] or using words to generate a password which connects a master account with the particular device [31]. Any of these cases requires U2M communication.

Generally a device is capable of constant and repetitive tasks, but its decision capabilities are limited: goals or objectives can only be set by a user. Users, on the other hand, may find monotonous or continual-load requirements onerous at best and impossible at worst. Given these differences in capability, the adaptation of existing M2M security technologies [21, 30, 34, 43, 55] works well for IoT scenarios where a user is not required. Proposals exist for M2M authentication even with low-resource devices [20, 44, 45].

Finally, many of the solutions described in U2M research can be used for M2M identity management with little to no modification [14, 18, 24, 32, 35, 37, 53] and vice versa [15, 28, 33, 36, 39, 40, 42, 49, 50]. Some of the research even includes existing U2M technologies being used for M2M purposes [23, 29, 41], and many of the papers surveyed are useful for either communication model [16, 19, 25, 38, 46–48, 51, 52, 54].

Figure 5 shows that research contributions in the U2M communication model occur with similar frequency to those in the M2M model. The vast majority of projects can be used for either communication scheme, which demonstrates the versatility of the security solutions and proposals.

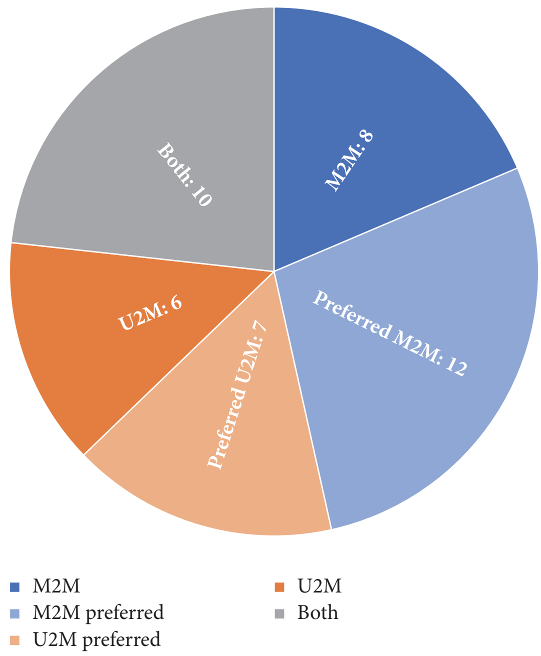

Figure 5: Categorization of U2M and M2M solutions.

10. Threats to Validity

Surveys are a highly subjective type of research and therefore suffer from threats to validity. We have identified several threats that need to be addressed or at least mentioned. In order to eliminate most of them, we have followed recommended guidelines for conducting systematic studies [10].

Our evidence selection is based on professional indexing sites. We could miss some articles published in other sources (e.g., journals not indexed in WoS). Also, the queries we use to search for articles explore only abstracts. This means that articles which should have been included may not have been because they contained some of the excluded words or because they did not contain any of the included words. We tried to eliminate this by testing our queries against the manually selected control set.

Data extraction bias is another possible threat to validity. We addressed this primarily by ensuring that each paper received several individual reviews focused on each research question. Using the RAKE algorithm to extract paper keywords also mitigated data extraction bias somewhat because the same extraction method was applied to each paper, apart from any human factors.

Exclusion and inclusion of the papers due to their scope are also potential threat. To mitigate this threat we followed methods for the selection criteria suggested in [10]. We have read numerous related works and spent considerable time reading the selected papers to assure they fit within our considered scope. We removed papers that focus specifically on cryptography, networking, and low level device security. We have also excluded papers that do not provide specific results, that list only suggestions or opinions without solution proposals.

All of the papers were treated equally in the survey, although not all of the published research has the same quality or impact on the community. We provide some overview of each article's impact in Table 5, including metadata about the impact of the paper and possible quality of the source of the publication. To measure community impact we have chosen two sources: data from publishers and Google Scholar [89]. Publishers generally provide their own list of citing works and a number of downloads (or views) of the work. One disadvantage of using this publisher-provided data is that it may often miss citations from sources unknown to it. Therefore, Google Scholar was chosen as a universal, most fully populated article aggregator. It provides its own list of citations, but they include self-citations and it may take up to few months for articles or citations to appear there. To quantify quality of the publishing media we chose two methods. For journals we use Impact Factor [90] from Web of Science as it is the most prominent and possibly oldest journal indexing tool. Ranking conferences proves to be more difficult. The most appropriate measure for our needs seems to be the Computing Research Education (CORE) Association of Australasia conference ranking [91] as it presents independent rankings of conferences with any sponsor. It ranks conferences with letters C, B, A, and A∗ for its quality (A∗ is the best, C is the worst). A disadvantage is that not all conferences are included in the ranking and the ranking itself is managed by a small group of scientists from a particular geographic area.

11. Conclusion

This paper provides an overview of the accomplished research and challenges in the security domain of IoT, especially for authentication and authorization. It contains the most recent research and categorizes it from multiple perspectives. It shows how context-awareness extends security and what approaches exist to incorporate context-awareness into IoT security. It shows how existing and current, widely adopted technologies are adapted for the IoT and surveys new security proposals designed specifically for that environment. We discussed whether security solutions for centralized or distributed architectures are favored and analyzed whether machine-to-machine or user-to-machine security is more prevalent in the current research.

To our best knowledge there is no similar study or survey of IoT security or any other study containing the latest IoT security research. We believe that this overview will help readers gain an overall picture about the state of IoT security research, allowing them to reapply existing knowledge and deal with the security issues that are preventing IoT popularity and adoption from increasing among end users.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the Fulbright Program and the Grant Agency of the Czech Technical University in Prague, Grant no. SGS16/234/OHK3/3T/13.

Table 5: Community impact of articles.

Article	Published in	IF or CORE ranking	Year	Source citations	Source citations per year	Google citations	Google citations per year	Views	Views per year
[14]	Conference	A	2016	0	0	2	1	244	122
[15]	Conference	N/A	2016	0	0	6	3	342	171
[16]	Conference	N/A	2015	3	1	15	5	246	82
[17]	Journal	N/A	2016	2	1	1	0.5	409	204.5
[18]	Journal	1.405	2017	0	0	0	0	374	374
[19]	Conference	A	2015	1	0.33	7	2.33	766	255.33
[20]	Book chapter	N/A	2015	0	0	N/A	N/A	N/A	N/A
[21]	Journal	8.085	2015	45	15	57	19	1701	567
[22]	Conference	B	2017	0	0	4	4	207	207
[23]	Journal	1.239	2017	0	0	0	0	355	355
[24]	Conference	B	2014	4	1	0	0	945	236.25
[25]	Conference	N/A	2016	2	1	0	0	359	179.5
[26]	Journal	1.521	2017	2	2	1	1	1269	1269
[27]	Conference	C	2015	3	1	6	2	183	61
[28]	Conference	C	2017	0	0	0	0	160	160
[29]	Journal	N/A	2017	0	0	0	0	407	407
[30]	Conference	N/A	2015	0	0	2	0.67	195	65
[31]	Conference	A∗	2016	1	0.5	1	0.5	252	126
[32]	Journal	N/A	2017	0	0	5	5	N/A	N/A
[33]	Journal	N/A	2017	N/A	N/A	2	2	N/A	N/A
[34]	Journal	1.232	2014	N/A	N/A	73	18.25	N/A	N/A
[35]	Journal	0.849	2017	1	1	1	1	313	313
[36]	Journal	2.472	2016	17	8.5	30	15	1100	550
[37]	Conference	N/A	2015	1	0.33	4	3.33	180	60
[38]	Conference	C	2015	0	0	4	1.33	164	54.66
[39]	Conference	N/A	2015	1	0.33	1	0.33	297	99
[40]	Conference	N/A	2017	2	2	12	12	359	359
[41]	Conference	N/A	2016	0	0	0	0	394	197
[42]	Conference	C	2017	0	0	1	1	165	165
[43]	Conference	B	2016	2	1	3	1.5	253	126.5
[44]	Journal	4.951	2017	0	0	1	1	N/A	N/A
[45]	Journal	1.405	2017	2	2	5	5	370	370
[46]	Journal	2.02	2013	65	4.33	111	22.2	N/A	N/A
[47]	Conference	N/A	2017	1	1	0	0	511	511
[48]	Conference	N/A	2016	0	0	1	0.5	732	366
[49]	Conference	N/A	2014	5	1.25	10	2.5	97	24.25
[50]	Journal	10.435	2017	2	2	4	4	693	693
[51]	Conference	B	2015	11	3.67	43	14.33	1638	548
[52]	Conference	C	2015	2	1.67	1	0.33	272	90.67
[53]	Conference	N/A	2014	1	0.25	3	0.75	337	84.25
[54]	Conference	B	2017	1	1	1	1	238	238
[55]	Conference	N/A	2017	0	0	0	0	363	363
[56]	Conference	N/A	2016	0	0	1	0.5	315	157.5

References

[1] P. Baran, "On distributed communications networks," *IEEE Transactions on Communications*, vol. 12, no. 1, pp. 1–9, 1964.

[2] J. C. R. Licklider, "Memorandum for members and affiliates of the intergalactic computer network, Technical report," Tech. Rep., Advanced Research Projects Agency, April 1963.

[3] V. G. Cerf and R. E. Kahn, "A Protocol for Packet Network Intercommunication," *IEEE Transactions on Communications*, vol. 22, no. 5, pp. 637–648, 1974.

[4] B. M. Leiner, V. G. Cerf, D. D. Clark et al., "A brief history of the internet," *Computer Communication Review*, vol. 39, no. 5, p. 22, 2009.

[5] C.-L. Hsu, H.-P. Lu, and H.-H. Hsu, "Adoption of the mobile Internet: an empirical study of multimedia message service (MMS)," *Omega*, vol. 35, no. 6, pp. 715–726, 2007, Special Issue on Telecommunications Applications.

[6] G. Wu, S. Talwar, K. Johnsson, N. Himayat, and K. D. Johnson, "M2M: from mobile to embedded internet," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 36–43, 2011.

[7] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[8] Gartner Inc., "Hype cycle for the internet of things 2017," Technical report, July 2017.

[9] G. Jayavardhana, B. Rajkumar, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," in *Future Generation Computer Systems*, vol. 29 of *Including Special sections: Cyber-enabled Distributed Computing for Ubiquitous Cloud and Network Services & Cloud Computing and Scientific Applications - Big Data, Scalable Analytics, and Beyond*, pp. 1645–1660, 7 edition, 2013.

[10] K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: an update," *Information and Software Technology*, vol. 64, pp. 1–18, 2015.

[11] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: the road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[12] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[13] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[14] I. Agadakos, P. Hallgren, D. Damopoulos, A. Sabelfeld, and G. Portokalidis, "Location-enhanced authentication using the IoT because you cannot be in two places at once," in *Proceedings of the 32nd Annual Computer Security Applications Conference, ACSAC 2016*, pp. 251–264, USA, December 2016.

[15] G. Alpár, L. Batina, L. Batten et al., "New directions in IoT privacy using attribute-based authentication," in *Proceedings of the ACM International Conference on Computing Frontiers, CF 2016*, pp. 461–466, NY, USA, May 2016.

[16] L. Barreto, A. Celesti, M. Villari, M. Fazio, and A. Puliafito, "An authentication model for IoT clouds," in *Proceedings of the IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2015*, pp. 1032–1035, August 2015.

[17] M. Cagnazzo, M. Hertlein, and N. Pohlmann, *An Usable Application for Authentication, Communication and Access Management in the Internet of Things*, Springer International Publishing, Cham, Switzerland, 2016.

[18] F. Chen, Y. Luo, J. Zhang et al., "An infrastructure framework for privacy protection of community medical internet of things: Transmission protection, storage protection and access control," *World Wide Web*, pp. 1–25, 2017.

[19] P. Fremantle, J. Kopecký, and B. Aziz, *Web API Management Meets the Internet of Things*, Springer International Publishing, Cham, Switzerland, 2015.

[20] S. Gerdes, C. Bormann, and O. Bergmann, "Chapter 11 - keeping users empowered in a cloudy internet of things," in *The Cloud Security Ecosystem*, R. Ko and K.-K. R. Choo, Eds., pp. 231–247, Syngress, Boston, MA, USA, 2015.

[21] J. L. H. Ramos, M. P. Pawlowski, A. J. Jara, A. F. Skarmeta, and L. Ladid, "Toward a lightweight authentication and authorization framework for smart objects," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 4, pp. 690–702, 2015.

[22] T. Kumar, A. Braeken, M. Liyanage, and M. Ylianttila, "Identity privacy preserving biometric based authentication scheme for Naked healthcare environment," in *Proceedings of the IEEE International Conference on Communications, ICC*, May 2017.

[23] S.-H. Lee, K.-W. Huang, and C.-S. Yang, "TBAS: Token-based authorization service architecture in Internet of things scenarios," *International Journal of Distributed Sensor Networks*, vol. 13, no. 7, 2017.

[24] L. Liu, B. Fang, and B. Yi, *A General Framework of Nonleakage-Based Authentication Using CSP for the Internet of Things*, Springer International Publishing, Cham, Switzerland, 2014.

[25] A. Pinto and R. Costa, *Hash-Chain Based Authentication for IoT Devices and REST Web-Services*, Springer International Publishing, Cham, Switzerland, 2016.

[26] M. Shahzad and M. P. Singh, "Continuous authentication and authorization for the internet of things," *IEEE Internet Computing*, vol. 21, no. 2, pp. 86–90, 2017.

[27] N. Shone, C. Dobbins, W. Hurst, and Q. Shi, "Digital memories based mobile user authentication for IoT," in *Proceedings of the IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, pp. 1796–1802, October 2015.

[28] Q. Tasali, C. Chowdhury, and E. Y. Vasserman, "A flexible authorization architecture for systems of interoperable medical devices," in *Proceedings of the 22nd ACM Symposium on Access Control Models and Technologies, SACMAT 2017*, pp. 9–20, USA, June 2017.

[29] M. Trnka and T. Cerny, "Authentication and authorization rules sharing for internet of things," *Software Networking*, no. 1, pp. 35–52, 2017.

[30] S. Unger and D. Timmermann, "DPWSec: devices profile for web services security," in *Proceedings of the 10th IEEE International Conference on Intelligent Sensors, Sensor Networks and Information Processing, ISSNIP 2015*, pp. 1–6, April 2015.

[31] S. Wiseman, G. S. Mino, A. L. Cox, S. J. J. Gould, J. Moore, and C. Needham, "Use your words: Designing one-time pairing codes to improve user experience," in *Proceedings of the 34th Annual Conference on Human Factors in Computing Systems, CHI 2016*, USA, May 2016.

[32] S. Sicari, A. Rizzardi, L. Grieco, G. Piro, and A. Coen-Porisini, "A policy enforcement framework for Internet of Things applications in the smart health," *Smart Health*, vol. 3-4, pp. 39–74, 2017.

[33] A. Outchakoucht, H. Es-samaali, and J. Philippe, "Dynamic access control policy based on blockchain and machine learning

for the internet of things," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 1, 2017.

[34] N. Ye, Y. Zhu, R.-C. Wang, R. Malekian, and Q.-M. Lin, "An efficient authentication and access control scheme for perception layer of internet of things," *Applied Mathematics & Information Sciences*, vol. 8, no. 4, pp. 1617–1624, 2014.

[35] J. B. Bernabe, J. L. Hernandez-Ramos, and A. F. S. Gomez, "Holistic privacy-preserving identity management system for the internet of things," *Mobile Information Systems*, vol. 2017, 2017.

[36] J. Bernal Bernabe, J. L. Hernandez Ramos, and A. F. Skarmeta Gomez, "Taciot: multidimensional trust-aware access control system for the internet of things," *Soft Computing*, vol. 20, no. 5, pp. 1763–1779, 2016.

[37] S. Cirani and M. Picone, "Effective authorization for the Web of Things," in *Proceedings of the 2nd IEEE World Forum on Internet of Things, WF-IoT 2015*, pp. 316–320, December 2015.

[38] W. Han, Y. Zhang, Z. Guo, and E. Bertino, "Fine-grained business data confidentiality control in cross-organizational tracking," in *Proceedings of the 20th ACM Symposium on Access Control Models and Technologies, SACMAT 2015*, pp. 135–145, June 2015.

[39] A. Kurniawan and M. Kyas, "A trust model-based Bayesian decision theory in large scale Internet of Things," in *Proceedings of the 10th IEEE International Conference on Intelligent Sensors, Sensor Networks and Information Processing, ISSNIP 2015*, April 2015.

[40] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in IoT," *Advances in Intelligent Systems and Computing*, vol. 520, pp. 523–533, 2017.

[41] P. Solapurkar, "Building secure healthcare services using OAuth 2.0 and JSON web token in IOT cloud scenario," in *Proceedings of the 2nd International Conference on Contemporary Computing and Informatics, IC3I 2016*, pp. 99–104, December 2016.

[42] S. Lee, J. Choi, J. Kim et al., "FACT: Functionality-centric access control system for IoT programming frameworks," in *Proceedings of the 22nd ACM Symposium on Access Control Models and Technologies, SACMAT 2017*, pp. 43–54, USA, June 2017.

[43] S. Bandara, T. Yashiro, N. Koshizuka, and K. Sakamura, "Access control framework for API-enabled devices in smart buildings," in *Proceedings of the 22nd Asia-Pacific Conference on Communications, APCC 2016*, pp. 210–217, August 2016.

[44] A. Biason, C. Pielli, A. Zanella, and M. Zorzi, "Access control for IoT nodes with energy and fidelity constraints," *IEEE Transactions on Wireless Communications*, vol. 17, no. 5, pp. 3242–3257, 2018.

[45] Q. Huang, L. Wang, and Y. Yang, "DECENT: Secure and fine-grained data access control with policy updating for constrained IoT devices," *World Wide Web*, pp. 1–17, 2017.

[46] S. Gusmeroli, S. Piccione, and D. Rotondi, *A Capability-Based Security Approach to Manage Access Control in the Internet of Things*, vol. 58 of *Mathematical and Computer Modelling*, 5 edition, 2013, The Measurement of Undesirable Outputs: Models Development and Empirical Analyses and Advances in mobile, ubiquitous and cognitive computing.

[47] A. Majeed and A. Al-Yasiri, *Formulating A Global Identifier Based on Actor Relationship for the Internet of Things*, Springer International Publishing, Cham, Switzerland, 2017.

[48] D. Schreckling, J. David Parra, D. Charalampos, and J. Posegga, *Data-Centric Security for the IoT*, Springer International Publishing, Cham, Switzerland, 2016.

[49] K. Fysarakis, I. Papaefstathiou, C. Manifavas, K. Rantos, and O. Sultatos, "Policy-based access control for DPWS-enabled ubiquitous devices," in *Proceedings of the 19th IEEE International Conference on Emerging Technologies and Factory Automation, ETFA 2014*, September 2014.

[50] D. Hussein, E. Bertin, and V. Frey, "A community-driven access control approach in Distributed IoT environments," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 146–153, 2017.

[51] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, "Network-level security and privacy control for smart-home IoT devices," in *Proceedings of the 11th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob 2015*, pp. 163–167, October 2015.

[52] I. Bouij-Pasquier, A. Ait Ouahman, A. Abou El Kalam, and M. Ouabiba De Montfort, "SmartOrBAC security and privacy in the Internet of Things," in *Proceedings of the 12th IEEE/ACS International Conference of Computer Systems and Applications, AICCSA 2015*, November 2015.

[53] M. Poulymenopoulou, F. Malamateniou, and G. Vassilacopoulos, "A virtual PHR authorization system," in *Proceedings of the 2014 IEEE-EMBS International Conference on Biomedical and Health Informatics, BHI 2014*, pp. 73–76, June 2014.

[54] J. Wilson, R. S. Wahby, H. Corrigan-Gibbs, D. Boneh, P. Levis, and K. Winstein, "Trust but verify: Auditing the secure Internet of Things," in *Proceedings of the 15th ACM International Conference on Mobile Systems, Applications, and Services, MobiSys*, USA, 2017.

[55] C.-Y. Chen, *Efficient Authentication for Tiered Internet of Things Networks*, Springer International Publishing, Cham, Switzerland, 2017.

[56] H. Ren, Y. Song, S. Yang, and F. Situ, "Secure smart home: A voiceprint and internet based authentication system for remote accessing," in *Proceedings of the 11th International Conference on Computer Science and Education, ICCSE 2016*, pp. 247–251, August 2016.

[57] R. Sandhu, "Access control: The neglected frontier," in *Information Security and Privacy*, J. Pieprzyk and J. Seberry, Eds., vol. 1172, Springer, Berlin, Heidelberg, Germany, 1996.

[58] D. Ferraiolo and R. Kuhn, "Role-based access control," in *Proceedings of the 15th National Computer Security Conference*, pp. 554–556, April 1992.

[59] D. Gregory, K. Abowd Anind, J. Peter, N. Davies, M. Smith, and P. Steggles, *Towards a Better Understanding of Context and Context-Awareness*, Springer, Berlin, Heidelberg, Germany, 1999.

[60] M. Trnka and T. Cerny, "On security level usage in context-aware role-based access control," in *Proceedings of the the 31st Annual ACM Symposium*, NY, USA, April 2016.

[61] M. A. Al-Kahtani and R. Sandhu, "A model for attribute-based user-role assignment," in *Proceedings of the 18th Annual Computer Security Applications Conference, ACSAC 2002*, pp. 353–362, USA, December 2002.

[62] M. Ge and S. L. Osborn, "A design for parameterized roles," in *Research Directions in Data and Applications Security XVIII*, C. Farkas and P. Samarati, Eds., Springer, Boston, MA, USA, 2004.

[63] J. Fischer, D. Marino, R. Majumdar, and T. Millstein, "Fine-grained access control with object-sensitive roles," in *ECOOP 2009 – Object-Oriented Programming*, S. Drossopoulou, Ed., Springer, Berlin, Heidelberg, Germany, 2009.

[64] M. J. Covington, W. Long, S. Srinivasan, A. K. Dey, M. Ahamad, and G. D. Abowd, "Securing context-aware applications using

environment roles," in *Proceedings of the sixth ACM Symposium on Access Control Models and Technologies (SACMAT 2001)*, pp. 10–20, USA, May 2001.

[65] G. Sladić, B. Milosavljević, and Z. Konjović, "Context-sensitive access control model for business processes," *Journal of Organizational Computing and Electronic Commerce*, vol. 10, no. 6, pp. 939–972, 2013.

[66] X. Jin, R. Krishnan, and R. Sandhu, "A unified attribute-based access control model covering dac, mac and rbac," in *Data and Applications Security and Privacy XXVI*, N. Cuppens-Boulahia, F. Cuppens, and J. Garcia-Alfaro, Eds., pp. 41–55, Springer, Berlin, Heidelberg, Germany, 2012.

[67] K. Zeilenga, "Lightweight directory access protocol (ldap): technical specification road map," RFC 4510, RFC Editor, 2006, http://www.rfc-editor.org/rfc/rfc4510.txt.

[68] M. Jones, B. de Medeiros, C. Mortimore, N. Sakimura, and J. Bradley, "Openid connect core," OpenID Community, 2014.

[69] S. Rose, D. Engel, N. Cramer, and W. Cowley, "Automatic keyword extraction from individual documents," *Text Mining: Applications and Theory*, pp. 1–20, 2010.

[70] N. Pohlmann, M. Hertlein, and P. Manaras, *Bring Your Own Device For Authentication (BYOD4A) – The Xign–System*, Springer Fachmedien Wiesbaden, Germany, 2015.

[71] A. Bassi, M. Bauer, M. Fiedler et al., *Enabling Things to Talk: Designing IoT Solutions with the IoT Architectural Reference Model*, Springer Publishing Company, Incorporated, 1st edition, 2016.

[72] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (eap)," RFC 3748, RFC Editor, June 2004, http://www.rfc-editor.org/rfc/rfc3748.txt.

[73] R. T. Fielding, *Architectural Styles and the Design of Network-Based Software Architectures*, chapter Representational State Transfer (REST), University of Californi, 2000.

[74] E. Rescorla, "Http over tls," RFC 2818, RFC Editor, May 2000, http://www.rfc-editor.org/rfc/rfc2818.txt.

[75] A. W. Roscoe, *The Theory and Practice of Concurrency*, Prentice Hall PTR, Upper Saddle River, NJ, USA, 1997.

[76] J. Camenisch and E. V. Herreweghen, "Design and implementation of the idemix anonymous credential system," in *Proceedings of the 9th ACM Conference on Computer and Communications Security CCS '02*, pp. 21–30, ACM, New York, NY, USA, November 2002.

[77] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari, "IoT-OAS: an oauth-based authorization service architecture for secure services in IoT scenarios," *IEEE Sensors Journal*, vol. 15, no. 2, pp. 1224–1234, 2015.

[78] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the IEEE Symposium on Security and Privacy (SP '07)*, pp. 321–334, IEEE Computer Society, Washington, DC, USA, 2007.

[79] "The extensible access control markup language (xacml) version 3.0. OASIS Standard," 2017.

[80] D. Hardt, "The oauth 2.0 authorization framework," RFC 6749, RFC Editor, October 2012, http://www.rfc-editor.org/rfc/rfc6749.txt.

[81] M. Jones, J. Bradley, and N. Sakimura, "Json web token (jwt)," RFC 7519, RFC Editor, May 2015, http://www.rfc-editor.org/rfc/rfc7519.txt.

[82] A. A. E. Kalam, R. E. Baida, P. Balbiani et al., "Organization based access control," in *Proceedings of the 4th IEEE International Workshop on Policies for Distributed Systems and Networks*, pp. 120–131, 2003.

[83] Astm f2761-09, *Medical Devices And Medical Systems - Essential Safety Requirements for Equipment Comprising The Patient-Centric Integrated Clinical Environment (Ice) - Part 1: General Requirements And Conceptual Model*, ASTM International, PA, USA, 2009.

[84] J. Hatcliff, A. King, I. Lee et al., "Rationale and architecture principles for medical application platforms," in *Proceedings of the 2012 IEEE/ACM 3rd International Conference on Cyber-Physical Systems, ICCPS 2012*, pp. 3–12, April 2012.

[85] T. Cerny, M. J. Donahoo, and M. Trnka, "Contextual understanding of microservice architecture: Current and future directions," *Applied Computing Review*, vol. 17, no. 4, 2018.

[86] Web services security: Soap message security 1.1. OASIS Standard, 2006.

[87] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: a survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 414–454, 2014.

[88] B. C. Neuman, "Proxy-based authorization and accounting for distributed systems," in *Proceedings of the 1993 IEEE 13th International Conference on Distributed Computing Systems*, pp. 283–291, May 1993.

[89] "Google scholar," https://scholar.google.com/.

[90] E. Garfield, "The history and meaning of the journal impact factor," *Journal of the American Medical Association*, vol. 295, no. 1, pp. 90–93, 2006.

[91] "Core conference ranking," http://portal.core.edu.au/conf-ranks/.