Security Challenges and Solutions in the Internet of Things

Jari Porras*, Jayden Khakurel, Antti Knutas
and Jouni Pänkäläinen

Lapeenranta University of Technology, Finland
Email: Jari.Porras@lut.fi
**Corresponding Author*

Received 01 December 2018;
Accepted 10 December 2018

Abstract

The Internet of Things (IoT) concept is emerging and evolving rapidly. Various technical solutions for multiple purposes have been proposed for its implementation. The rapid evolution and utilization of IoT technologies has raised security concerns and created a feeling of uncertainty among IoT adopters. The purpose of this article is to examine the current research trends related to security concerns of the IoT concept and provide a detailed understanding of the topic. We thus applied two types of literature reviews as the methodological approach. The manual systematic mapping study was performed over 3500 articles, out of which 38 were selected for a closer examination. Out of these articles, the concerns, solutions and research gaps for the security in the IoT concept were extracted. This mapping study identified 9 main concerns and 11 solutions. The findings also revealed challenges, such as secure privacy management and cloud integration that still require efficient solutions. The results of the manual systematic mapping study were extended by using automatic content analysis tools on two datasets (–2016 and –2018) from Web of Science. This content analysis produces trends over the years on IoT security.

Keywords: Internet of things, Security, IoT threats, security solutions.

Journal of NBICT, Vol. 1, 177–206.
doi: 10.13052/nbjict1902-097X.2018.010

1 Introduction

The idea of connecting things has been discussed since 1982 when researchers at Carnegie Mellon University in Pittsburgh, Pennsylvania connected the vending machine to the university's computer network. This allowed them to determine the number of cans been dispensed, the number of remaining cans as well as to ensure the vending machines are restocked before visiting the location [36]. In 1991, Mark Weiser presented the idea of the interconnected devices that disappear into the background of our daily live [51]. In [51] he wrote "The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it" (p. 1). Nevertheless, the term "Internet of Things" or in the short "IoT" only appeared in 1999 when British technology entrepreneur Kevin Ashton used it as the title of a presentation at Procter & Gamble (P & G), and the term appeared in 2013, in the Oxford English Dictionary [6, 36].

Since, the beginning of the 21st century with the constant availability of the internet, cloud computing and the advancement of the technology, the IoT and its definition have evolved. For example, IEEE defines IoT in terms of small and complex systems [34] whereas the Global Standards Initiative [23] defines IoT as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies". Despite varying definitions of IoT, these devices have already found their way into our everyday lives with the rapid growth in the number of devices connected to the internet [32]. More will likely follow in upcoming years with the introduction of 5th generation wireless systems (5G). Ejaz et al. [18] point, "5th generation wireless systems (5G) are on the horizon and IoT is taking the center stage as devices are expected to form a major portion of this 5G network paradigm" (p. 10310). This means IoT will be one of the biggest drivers of the other main trends of technology, such as 5G. 5G and IoT are finally, after almost three decades, making the futuristic vision of Mark Weiser a reality. Statista forecast, the installed base of Internet of Things devices will continue to grow at an exponential rate: almost 75 billion will be installed worldwide by 2025 [22]. Similarly, Ericcson predicts by 2022, there will be 18 billion connected devices, which will be related to IoT [46]. Moreover, analyst firm, Gartner estimates that by 2020 there will be 20 billion internet-connected things, which includes dedicated-function objects, such as vending machines, jet engines, connected cars resulting new business models, improving efficiency [33].

As new IoT devices emerges and more businesses, governments, and citizens adopts and rely on these devices for everyday processes, new security concerns may arise. For example, it is no longer sufficient to secure the doors and windows of one's apartment; individuals also must consider the information security of their fridge or thermostat. Kouicem et al. [27] state, "IoT suffers from several security issues, which are more challenging than those from other fields regarding its complex environment and resources-constrained IoT devices" (p. 199).

The main aim of this research is to determine the status of the security research (concerns, solutions and research gaps) regarding the IoT. A systematic mapping study (SMS) also known as scoping study [14] is used to collect data and analyse the literature. Using this approach, this research will attempt to answer the following research questions.

- RQ1: How has the **research trends** of IoT domain changed in time?
- RQ2: What kinds of **security related concerns** have been raised within IoT?
- RQ3: What kinds of **solutions** have been presented to improve the security of IoT?
- RQ4: What kinds of **research gaps** within IoT security research have been identified?

The above presented RQs will provide insights into the security concerns, solutions and remaining challenges or research gaps based on the literature. This work has been done in two phases. First phase included literature up to 2016 and was reported in HICSS 2018. The second phase was performed in November 2018 and updated the literature and the analysis for this article as described in Section 2.

The paper is organized as follows: Section 2 presents the research design and implementation, explaining the research methods and SMS. This section also explains how the original paper presented in HICSS 2018 was updated for this article. Sections 3 present the literature review results in respect to the research question emphasizing the trends of the IoT security research, including focuses on the content of the research. We also present the changes based on the updated literature from 2016 to 2018. Section 4 concludes the article.

2 Research Design and Implementation

This article is an extended version of a paper [39] published at HICSS 2018 conference. We have used the data presented in HICSS 2018 as a basis and rerun the literature searches to include literature published after the data collection for that previous paper. Thus, this article consists of two-phase research process: In phase one (i.e. original HICSS literature study): i) Manual systematic mapping study on security related concerns, solutions in Internet of Things domain from a selected set of databases; and ii) automatic content analysis based on a dataset from web of science database was performed. Similarly, phase two (i.e. extended literature study), new automatic content analysis of a new dataset from web of science was performed. These phases will be shortly described in the following subsections:

2.1 Phase 1: Original HICSS Literature Study

An SMS is a secondary study to classify and thematically to identify and analyse earlier research [15, 38]. It's primary purpose is to classify and structure a field of interest in research by categorizing publications and analyzing their publication trends through a visual summary, often a map of its results [38]. Additionally, mapping studies can analyse what kinds of studies have been done in the field, and the research methods and outcomes [8]. Kitchenham and Charters [26] state that SMSs are suitable for fields where few literature reviews have been done on the topic and where there is a need to get a general overview of the field of interest. The focus of the remainder of the article is to discuss the research steps, which involves the manual SMS process in undertaking this study. Each of them, are listed as follows:

a) **Define the research questions:** Bryman [13] state, "formulating a research question has an important role in many accounts of the research process as a stage that helps to militate against undisciplined data collection and analysis" (p. 5). As mentioned in introduction section, research questions were defined following the objectives of the research.

b) **Search strategies and data sources:** Identifying relevant publications requires appropriate keywords and relevant digital libraries to apply this clause [52]. Cronin et al. [17] point "Keywords need carefully consideration in order to select terms that will generate the data being sought" (p. 40). Therefore, in this study, we defined the search queries *(("Internet of Things" OR "IoT") AND "security")* based on the research questions and utilized NAILS[1] and HAMMER [29] tools for the first iterations of the keywords. Search articles on primary studies using search strings on selected set of scientific libraries and databases i.e. ACM Digital Library, IEEE Xplore Digital Library and Science Direct. These libraries have been chosen because they are identified as relevant to the field of research in this paper.

c) **Article selection process:** The aim of the article selection process in this study was to extract publications relevant to the objective of this SMS based on certain inclusion and exclusion criteria [25]. Inclusion and exclusion happen in multiple stages, starting from the screening of titles and abstracts and ending to the analysis of the whole document. Secondary articles can be added by manually browsing cited articles in the selected set of primary articles, i.e. by using backward snowballing like presented in [58]. Thus, the following set of inclusion (IC) and exclusion criteria (EC) were applied:

- IC1: Published between 1.1.2006 and 31.7.2016 (these are the original dates for the queries for the manual SMS and not changed for this article)
- IC2: Topic is IoT and information security
- IC2: Scientific and peer-reviewed articles written in English and relevant to RQ's
- EC1: Articles concerning specific technologies, such as protocols or identity management methods
- EC2: Duplicates of already included papers and are not fully available

The defined search query resulted in 3454 articles from digital libraries, as presented in Table 1. After refining the results based on the above-mentioned predefined exclusion and inclusion criteria, 38 articles were selected for detailed data extraction and analysis in the latter phase. These articles were

Table 1 The number of search results and selected articles per database

Library	Number of Articles Found by Search Query	Number of Articles Selected
ACM Digital Library	266	4
IEEE Xplore	1811	23
Science Direct	1377	13
Total	3454	38

[1] nailsproject.net

also used as "selection criteria" for the automatic content analysis in the next phase.

d) Data extraction and analysis: The template was used to register the relevant information from the selected set of articles. The data extraction process included the following input from each selected article: Basic information: ID, Author(s), Year of Publication, Title, Publication type (workshop, conference, journal), Keywords, Abstract, Database in which study was found; Specific information: Application domain, main concerns, proposed solutions and identified research gaps.

For validation purposes, a similar query on Web of Science[2] was executed and the received data were then analysed with NAILS and KHCoder. The query (with the original 10 year publication timeline 2006–2016) produced 2143 articles, a bit less than the query on selected databases. It should be noticed that this dataset included only 27 of the selected 38 articles. This data from Web of Science was used for general topic modelling and then those 27 included articled were mapped to the generated groups of articles (topics). The group(s) with most articles could then be run through automatic content analysis tools.

2.2 Phase 2: Extended Literature Study

For this article the original query on Web of Science was rerun including the publications up to 20.11.2018 and this dataset was analyzed using NAILS and KHCoder as explained in the phase 1B. The query produced close to 5200 articles including 29 of the original 38 selected articles. The number of articles in the field has thus more than doubled in two years. These results are compared to the results achieved in phase 1B.

3 Results

In this section, the analysed results from both the primary literature review data, i.e. 38 articles from 2006 to 2016, as well as from both datasets (2006–2016 and 2006–2018) from Web of Science related to this SMS are presented.

3.1 Articles in the Manual SMS

The analysis (see Figure 1) shows the number of articles published per year of the selected set of 38 articles. The database searches were limited to

[2] webofknowledge.com

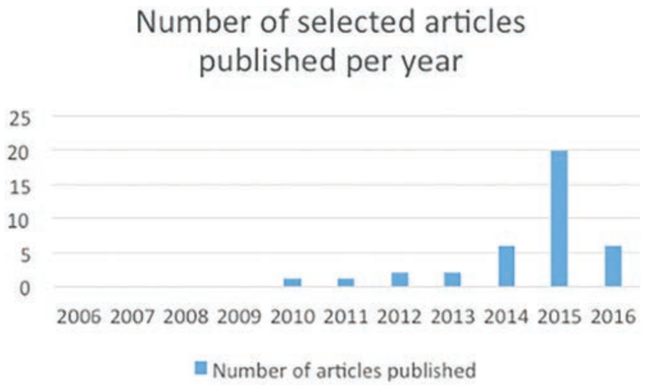

Figure 1 Number of selected articles published per year.

2006–2016, but relevant articles only started to appear around 2010. Since 2010, there has been a steady increase in the number of articles in the targeted topic. Out of the selected 38 articles, more than half were published in 2015. By the end of July of 2016, there were nearly as many articles published as in all of 2014. As such the interest in the topic is growing (though the emphasis is changing, as shown later by NAILS and KHCoder data). The small set of selected articles does not reveal any special journals or conferences for IoT security research. The larger dataset from Web of Science reveals, in general, that International Journal of Distributed Sensor Networks, Security, and Communication Networks, as well as IEEE IoT journal are among the most appropriate journals and the IEEE World Forum on the IoT and IndiaCom the most popular conferences for this research topic.

Further, the selected 38 articles were analysed according to the application domains of the targeted solution. Figure 2 shows the number of selected articles per application domain. Most had a rather general perception of IoT security. Only a small fraction of them specifically focused on security in some application domain, e.g. smart homes. This clearly shows that the security field in IoT solutions was just evolving by the time of the original article searches.

To further analyze the security on the IoT domain the Web of Science datasets were analysed by NAILS and KHCoder. The authors wanted to see if the rather large dataset (2143 and 5178 articles) contains some general trends or themes and if the larger dataset could be divided in more focused but still revealing sets of articles. The automatic content analysis features of the mentioned tools were used for categorization (topic modelling) and for finding yearly research themes (trending).

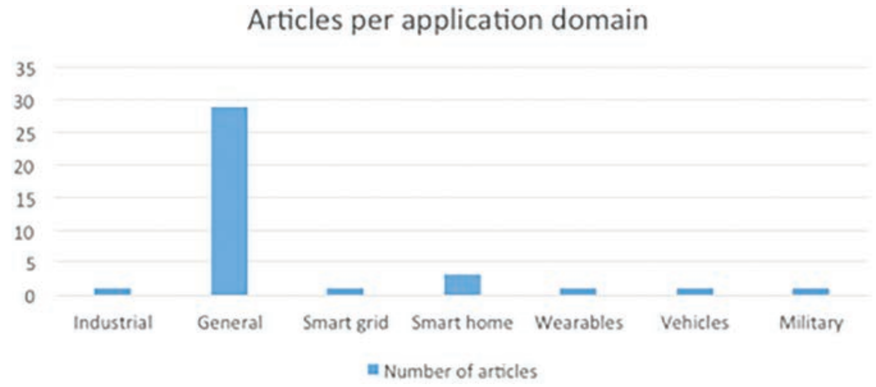

Figure 2 Number of selected articles published by application domain.

3.2 Topic Modelling and Keywords

The analysis of the dataset from Web of Science offers another perspective on IoT security research. NAILS uses the Latent Dirichlet Allocation (LDA) topic modelling algorithm [12] for categorisation of articles into groups. LDA can be used as a statistical text mining method for assigning documents into topics, which are detected using word association and distributions [11]. It is commonly used for text analysis, and equivalent methods have been used to statistically analyse scientific texts in previous studies [48]. Figures 3 and 4 present the results of topic models in 2016 and 2018 respectively. The dataset of 2016 (2143 articles) is included in the dataset of 2018 (5191 articles). In general, the terms used within these articles are approximately the same as shown by Figures 3 and 4.

Like with LDA analysis with the NAILS tool the KHCoder tool was used to analyze the entire 2018 Web of Science dataset in sense of the keywords used in the abstracts. Figure 5 presents the dentogram of all groups of keywords in the set of 5200 articles. One can find the same words as in topic modelling but categorized in another way.

The topic modelling of the larger 2018 dataset divides the articles into 5 topics while the 2016 dataset was divided in 4 topics (Note that the authors have named the topics based on their content). When comparing the specific keywords for each topic presented in these tables one can see that the Topic 1 – Networks of the 2016 dataset is divided in two, namely networks and protocols, in 2018 dataset. Otherwise, the topics have remained quite constant, although the number of articles has more than doubled in each topic. For example the topic of our interest, Topic 4 – IoT security, has doubled its articles in just 2 years.

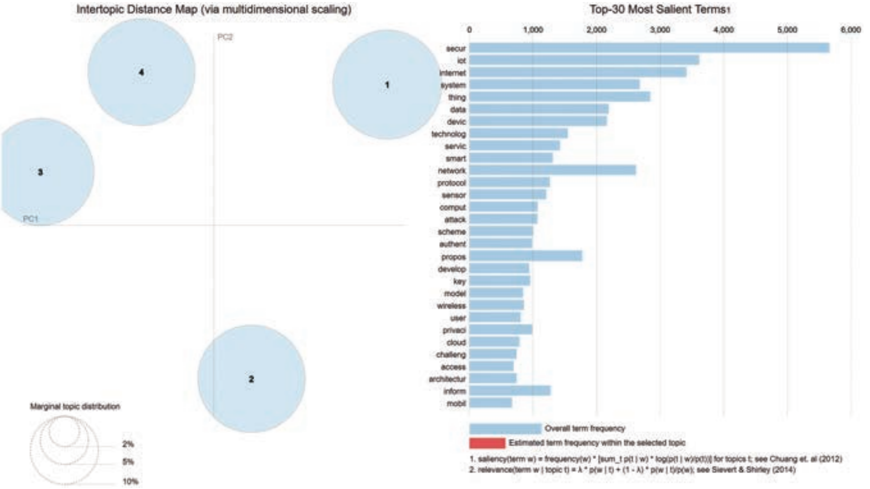

Figure 3 Topic modelling of Web of Science articles in 2016.

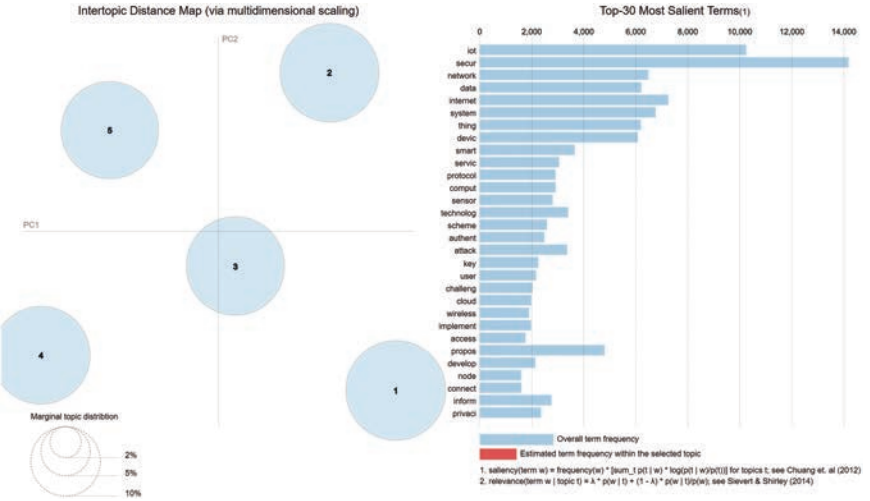

Figure 4 Topic modeling of Web of Science articles in 2018.

Tables 2 and 3 present the topics identified by the LDA modelling feature of NAILS. The topics have been named by the authors based on their content and there seems to be a clear separation of the topics. Topic 2 (of 2018 dataset) emphasizes the holistic system view while Topics 1 and 5 are present network and protocol levels. Topic 3 emphasizes data and service and the Topic 4 seems

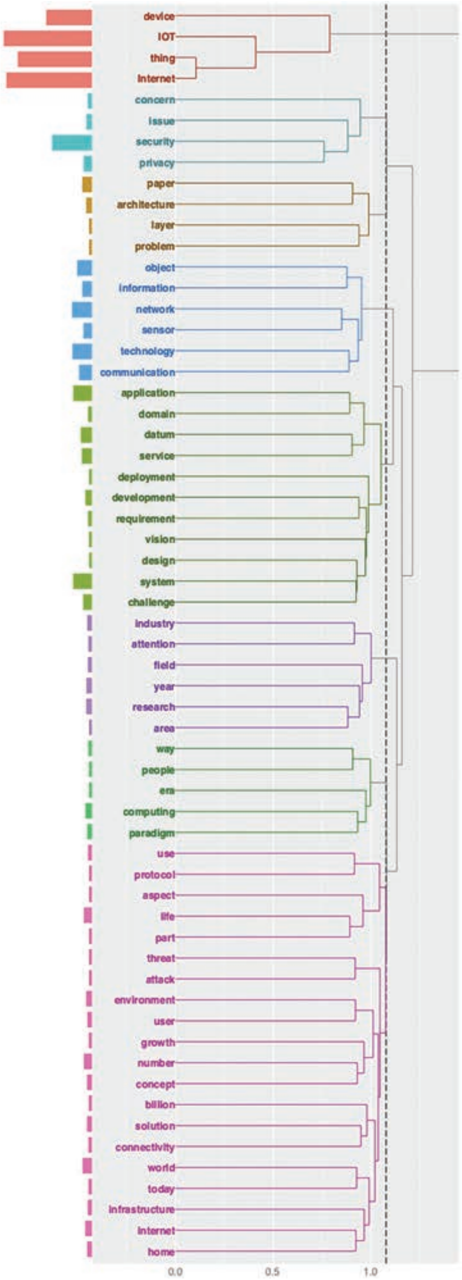

Figure 5 Keywords of all articles of 2018 Web of Science dataset as categorized by KHCoder.

Table 2 LDA-based Web of Science data topics and number of articles in each topic until July 2016

Topic 1 Networks	Topic 2 Systems	Topic 3 loT Security	Topic 4 Service
network	system	secur	data
protocol	technolog	iot	servic
propos	smart	internet	comput
sensor	develop	thing	privaci
attack	inform	devic	model
scheme	home	network	user
authent	manag	applic	cloud
key	monitor	challeng	access
secur	intellig	architectur	mobil
wireless	research	communic	provid
639	533	574	397

Table 3 LDA-based Web of Science data topics and number of articles in each topic until November 2018

Topic 1 Networks	Topic 2 Systems	Topic 3 Service	Topic 4 loT Security	Topic 5 Protocols
network	system	data	iot	secur
attack	smart	servic	secur	protocol
sensor	technolog	com put	internet	scheme
wireless	develop	user	thing	authent
node	inform	cloud	devic	propos
result	home	privaci	challeng	key
detect	industri	access	applic	devic
propos	monitor	control	connect	implement
method	intellig	mobil	architectur	communic
energi	manag	provid	paper	base
904	1165	915	1129	1065

to be the one of our interest (although all the articles were collected by the rather broad search query). This is also supported by the distribution of the 38 manually picked articles as 23 of them are included in Topic 4, 3 in Topic 3, 2 in Topic 2, 1 in Topic 5 and none in Topic 1. Thus, the automatic analysis will be focused to Topic 4.

3.3 Analysis of Trends in IoT Security Domain

3.3.1 RQ1: How has the research trends of IoT domain changed in time?

The 2018 Web of Science dataset was analysed by using KHCoder to find general trends (all papers) and evolution of the more focused set of papers

(Topic 4 – IoT Security). KHCoder is a quantitative content analysis tool that allows text mining and analysis. First, the abstract of all 5178 articles were analysed and co-occurrence of the key terms were calculated and visualised (see Figure 6). This figure shows the main keywords of articles by year and, thus, the research emphasis and trends of each year. Note that the size of the bubble emphasises the importance of the keyword. Figure 7 illustrates the trends within the Topic 4 that was selected as our focus by topic modelling.

The analysis of the trends presented in Figure 6 reveals some general evolution of research emphasis on IoT field. Early years were emphasizing the nodes (2009) and communication technologies like RFID (2010) while the focus of the last years have been more on data (2015, 2017), services (2015)

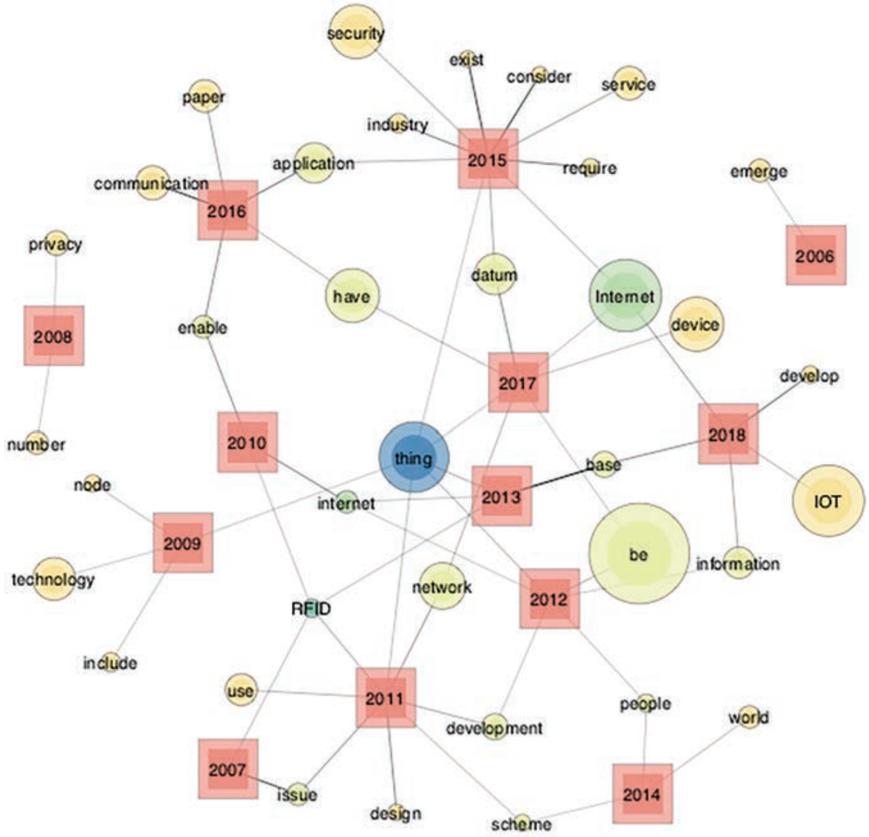

Figure 6 Co-occurrence of all keywords of 2018 Web of Science dataset as categorized by KHCoder.

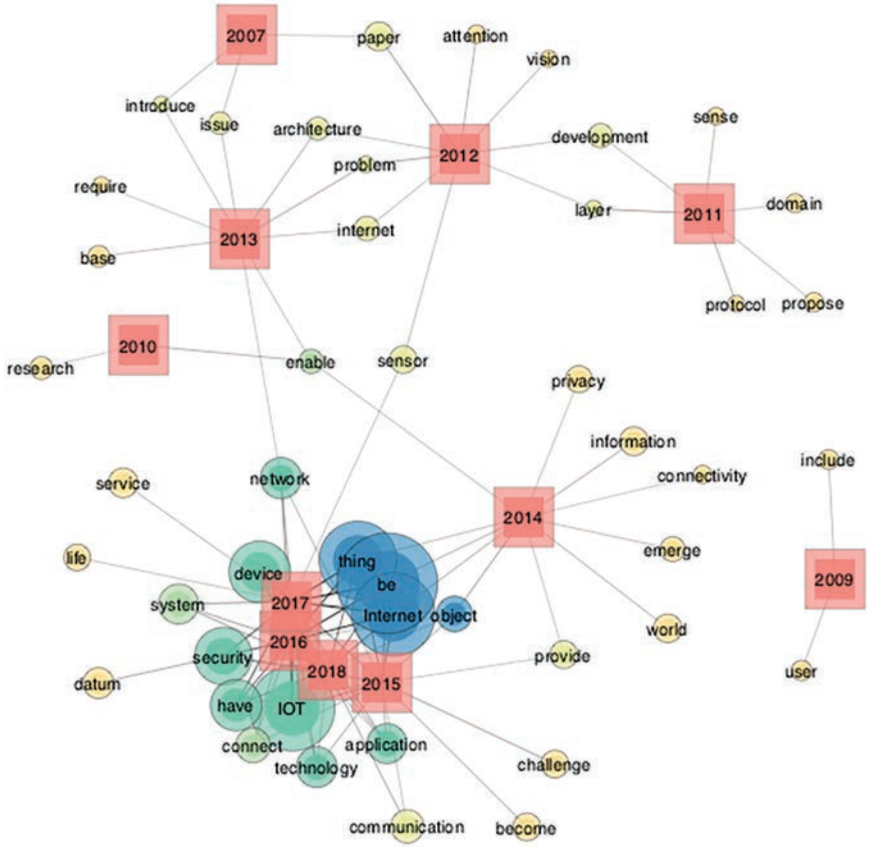

Figure 7 Co-occurrence of Topic 4 keywords of 2018 Web of Science dataset as categorized by KHCoder.

and applications (2015, 2016). Privacy and security issues are not so visible in this holistic picture. If looking at the trends in Topic 4 co-occurrence graph the security is a key component of the research since 2015.

3.3.2 Analysis of the contents of the manual dataset

The originally collected manual SMS dataset of 38 papers was analysed more deeply by looking answers to the research questions of this article.

3.3.3 RQ2: What kinds of security concerns have been raised within IoT?

According to Wrum et al. [53], some of the current commercially off the shelf (COTS) IoT devices do have software-level security solutions, but insufficient to secure entire IoT environments. They further state that the software level security is simply fundamentally flawed when an IoT environment is considered due to the different usage patterns. Airehrour et al. [2] point out that IoT are the fusion of heterogeneous of network, which transmits ultra-sensitive information across the IoT and poses numerous challenges to mobile communications sensor networks in today's society.

Therefore, it is necessary to obtain better overview on security concerns while implementing the IoT devices. The main objective of this research question was to identify the range of security concerns that has been raised by the research community in recent years and how have they been categorised. Primary studies had nine categories of concerns. For this SMS, they were further classified into four sub groups better understand the topic (**Key elements** – Environment constraints, Vulnerable Devices, Data privacy; **Functional constraints** – Enforcement mechanisms, Cross device dependencies, Identification, authentication and authorization; **Control** – Legislation; **Attacks** – Threats, Modes). The categories are linked to each other and other groupings could have been made.

3.3.4 Environment constraints

One of the main challenges of IoT security is the constraint set by the environment. Hossain et al. [21] enumerate them. First, they emphasise the hardware limitations: devices are constrained by computational power, memory and battery. Computationally complex memory intensive operations are therefore not well suited for the IoT. Next, they focus on software limitations. The operating systems in IoT devices have thin network stacks and may not be remotely reprogrammable. This limits the design of security modules and the ability to deliver security patches to these systems. Finally, they mention network-based constraints. The mobility, size and heterogeneity of the networks all add their own constraints and challenges to the security design. Roman et al. [41] agree that the computational and network limitations are constraints to IoT security.

3.3.5 Vulnerable devices

According to many researchers [55, 57] an important aspect in IoT security is device security. Yu et al. [55] present multiple known vulnerable devices, with issues such as hardcoded administrative usernames and passwords and open DNS resolvers, which could be used to mount Distribute Denial of Service (DDoS) attacks. Airehrour et al. [2] write about a case in 2012, where live footage from TRENDNET IP cameras was available to web users without requiring a password. Finally, Patton et al. [37] performed an extensive study on the vulnerable IoT devices, including 35,737 different devices. The vast majority were publicly accessible via the Internet, requiring no identification.

3.3.6 Data privacy

Many studies [2, 19, 20, 31, 42] indicate that data privacy is one of the main concerns in the IoT due to the high possibility of security risks, such as eavesdropping, unauthorized access, data modification, data forgery and unauthorized remote tampering with devices [31]. For example, Airehrour et al. [2] point out that collected data, such as names, addresses and insurance policy numbers, are often sensitive in nature and even more problems arise when such data are transferred to cloud environments. Similarly, Malina et al. [31] noted “many IoT services and applications provide sensitive and personal information that are exposed, and can be misused by an attacker. Unsecured sensitive data can leak to third parties” (pp. 83–84).

3.3.7 Enforcement mechanisms

According to Yu et al. [55], the enforcement mechanisms of IoT are either broken or lacking. There are no host-based defences, such as antiviruses, due to a lack of resources on the devices and the heterogeneous nature of the IoT environment. IoT devices also lack the automated software updates of traditional networked devices. The current vulnerability patching happens via firmware updates, which is done per manufacturer and per device. Third, the current network security mechanisms largely rely on strong static perimeter defences, such as firewalls. When vulnerable IoT devices are embedded deep inside the network, this approach will no longer be effective. Kumar et al. [28] also worried about the IoT’s lack of security updates.

3.3.8 Cross-device dependencies

Yu et al. [55] claim that the interconnected nature of the IoT presents additional security risks. They present an example of an attacker disabling an air conditioning unit, which would cause the temperature in a room to rise, which would then trigger another system to open the windows of the room, thus presenting a physical security risk. These interconnected devices are not uncommon. [55] presents a few examples: the NEST Protect home system has 188 cross-device policies, Wemo Plugin has 227 and Scout Alarm has 63.

3.3.9 Identification, authentication and authorisation

Many researchers [1, 2, 9, 16, 42, 57] argue that one of the main IoT security concerns is device identification and authentication. The massive number of devices in the IoT makes uniquely identifying and authenticating a single device extremely difficult. Without authentication, it is not possible to ensure that the data flow produced by an entity contains what it is supposed to contain. Related to authentication, there is also a problem of authorisation. Some sort of access control is required so that everyone is not enabled to access everything in a network. Nguyen et al. [35] observe that very few current security protocols offer access control or privacy protection properties. They argue that the access control service is key in the IoT. They note, that server-based protocols often offer this service with the help of an authorization server.

3.3.10 Sources of threats

Atamli et al. [7] list sources of threats for the IoT. According to them, the threats are malicious users, bad manufacturers and external adversaries. Malicious users are owners of IoT devices with the potential to perform attacks to learn the manufacturer's secrets and gain access to restricted functionality. Bad manufacturers produce devices with the ability to exploit technology to gain information about users or other IoT devices. Finally, external adversaries are outside parties, which have no access to the system.

3.3.11 Attacker models

Based on the selected set of articles IoT has various attack vectors that need to be considered.

- Denial of Service attacks [5, 42, 56]
- Physical attacks [5, 42, 58]
- Network attacks [1, 2, 5, 10, 21, 28, 42]
- Encryption attacks [4]

3.3.12 Legislative issues

In 2010, Weber [50] argued that new regulatory frameworks will become necessary to protect consumers' privacy; much of the IoT industry was largely self-regulated in that year. Weber argued, that this kind of regulation may be insufficient to ensure effective security or privacy. Weber stated that an international regulation would be necessary due to the global nature of the IoT. However, in his later paper [51] Weber says, that an international regulatory framework is still missing. Suo et al. [45] also note the need for security law and regulations to note the IoT, stating that the IoT is related to national security, business secrets and personal privacy and thus needs the legislative point of view to promote its development.

3.3.13 RQ3: What kinds of solutions have been presented to improve IoT security?

In addition to challenges, many researchers have also suggested solutions for the IoT security problems. The proposed solutions were grouped into 10 categories. These categories are first explained and later mapped against the challenges.

3.3.14 Trust management

Yan et al. [54] and Hossain et al. [21] claim that trust management plays a critical role in the IoT. Having trust management helps people overcome the uncertainty and risks attached to the IoT. Trust as a concept covers both security and privacy. Roman et al. [41] agree that trust is essential for the IoT. They state that trust is also about how users feel when interacting in the IoT. Users must be able to control their own services and have tools to describe their interactions with the systems. They also state that good governance can increase trust in the IoT.

Andrea et al. [4] and Abomhara et al. [1] also identify some trust relationships. There needs to be trust between each of the layers of the IoT. Communication and transitions between the layers need to be secure and private. For each layer, there also needs to be trust for security and privacy, meaning that each IoT layer must be preserved under any circumstance. Finally, there needs to be trust between the user and the IoT system.

Abomhara et al. [1] also discuss other aspects of trust management in the IoT, stating that the main objectives of trust research in the IoT are the conception of new models for decentralised trust, implementation of trust mechanisms for cloud computing and the development of applications based on node trust. They state that trust evaluation should be autonomous and automated.

3.3.15 Authentication

Zhang et al. [57] present multiple authentication models for the IoT. The models they suggest are authentication-by-gateway, authentication by security token, authentication by trust chain and authentication by global trust tree.

Each model has its own advantages and disadvantages. Mahmoud et al. [30] also write about authentication schemes. They present a one-time, one-cipher method based on a request-reply mechanism.

3.3.16 Privacy solutions

Roman et al. [41] offer several solutions for the privacy issues. One principle is privacy by design, which means that users would have the tools to manage their own data. Another principle is transparency. Transparency in the context of IoT means that users should know which entities are managing their data and how and when they are using them. The third solution they present is data management. This means deciding who is managing the secrets. There must be various data management policies and a policy-enforcement mechanism. Henze et al. [20] present a solution to handle IoT data in cloud environments called User-driven Privacy Enforcement for Cloud-based Services in the IoT (UPECSI). With UPECSI, users can control their sensitive data before they are transferred to the cloud.

3.3.17 Policy enforcement

Yu et al. [55] present a software-based approach to IoT security. Their solution is a security architecture consisting of micro security functions called µmboxes. The architecture has a centralised IoTSec controller, that monitors the environment and generates a global view for cross-device policy enforcement. Administrators can configure and instantiate new µmboxes and their routing mechanisms from this view.

3.3.18 Fault tolerance

Roman et al. [41] list several requirements for IoT systems to be fault tolerant. Achieving fault tolerance in the IoT requires three things. First, all devices must be secure by default. The second requirement is to give all IoT objects the ability to know the state of the network and its services. Finally, all objects should be able to defend themselves against network failures and attacks. Once an attack affects the services, the elements should be able to act quickly and recover from any damage.

3.3.19 Secure communication

Kumar et al. [28] state that the IoT protocol stack will try to match that of the classical Internet hosts to create an extended internet. According to them, this enables the IoT to utilise many of the existing security solutions. Nguyen et al. [35] also examine secure communication protocols in the context of the IoT. They examine two different categories of security solutions: solutions based on asymmetric keys and those based on symmetric pre-distributed keys.

3.3.20 Secure routing

Airehrour et al. [2] write about secure routing protocols to prevent routing attacks: a secure multi-hop routing protocol (SMRP), a trust-aware secure routing framework (TSFR), two-way acknowledgment-based trust (2-ACKT), a group-based trust management scheme (GTMS) and a collaborative lightweight trust-based routing protocol (CLT).

3.3.21 DDoS protection

According to Zhang et al. [56], a Learning Automata (LA) has been presented as a solution to DDoS attacks in IoT networks. The LA would intelligently determine the packet sampling rate from the environment. In the detection phase, the DDoS prevention component in each device would monitor the requests the device receives and once a pre-set maximum capacity is exceeded, it would issue out a DDoS alert to neighbouring nodes. Once the alert is issued, the devices would sample the IP addresses and try to detect the attacker. Once the attacker is identified, other nodes would be notified of this attacker and would drop any packets arriving from the attacker IP. Based on this approach, Zhang et al. present their own algorithm for detecting and preventing a DDoS attack in an IoT network. Another approach is to back up the sink node (a node that receives the data collected by sensors). This new node would be a redundant channel to hold a portion of the responsibilities of the sink node. This approach is considered a cost-effective one [56].

3.3.22 Spam prevention

Razzak [40] suggest that a solution to prevent IoT spam is to use digital signatures to sign the content in 2D barcodes. The barcode would contain the original content, digitally signed content and the barcode creator’s public key. The certificates verifying the identity of the creator would be placed in the URL to which the barcode points. An application would then check the QR code’s integrity and verify the certificate chain.

3.3.23 IoT architectures

Vasilomanolakis et al. [47] present multiple architectures for the IoT. The purpose of an IoT architecture is to bridge the gap between the actual devices and virtual entities, which produce services etc. The four presented architectures are IoT architecture (IoT-A), Building the environment for the Things as a Service (BeTaaS), open source cloud solutions for the IoT (OpenIoT) and IoT at Work (IoT@Work).

3.3.24 Regulatory solutions

Weber et al. [49] write about the regulatory action taken on the IoT. In Europe, the concept of the IoT was officially accepted in 2007. In 2009, a 14-point strategic action plan for the IoT was established. In 2012, it was established that there is significant disagreement between the users and the industry about the data-protection issues. In 2013, a European company called RAND was entrusted by the European Commission to establish guidelines for the IoT. It concluded, that the best regulatory approach for the IoT is “soft law”, which includes standards, supervision and ethical character, but at the same time ensures freedom for the industry.

On the other hand, the situation in America is not as clear. Most debates take place within several federal agencies that are only concerned about specific parts of the IoT. The first serious discussion was initiated in 2013, with the Federal Trade Commission (FTC) asking for comments on IoT privacy and security. Out of the 27 replies received, more than 60% were against regulation. Later in 2013, a workshop on IoT was held by the FTC. The conclusion was that regulation would depend on whether the companies would earn revenue from exclusively selling the IoT devices or if they would profit also from selling the user data.

3.3.25 RQ4: What kinds of research gaps within IoT security research have been identified?

The selected articles of this SMS contributed, in addition to the challenges and solutions, to a set of research gaps. Naturally, each article emphasises those topics under its focus, but some point out more general research gaps.

Sadeghi et al. [43] note that currently there are at least two topics that need further research. The next generation of IoT devices will consist of device swarms. The attestation of these systems, called swarm attestation, is still an open topic. Secure device management for IoT devices is another topic requiring further research. Current security solutions do not scale well with the growing number of devices. According to Malina et al. [31], there is still a need for a secure privacy preserving solution for the IoT. The current solutions are too computationally heavy for the resource-constrained devices that largely comprise the IoT. They argue that IoT applications need a solution that is not based on expensive bilinear pairing, produces short signatures and is easy to deploy in memory constrained devices.

Roman et al. [42] state that there have been very few advances in the management of access control policies in the distributed IoT. The existing access control policies cannot be applied to the distributed environments due to scalability and consistency issues. Role-based access control policies using certificates also require an infrastructure to validate the certificates in a cross-domain environment. There are, however, some workarounds for these problems.

Singh et al. [44] list multiple research areas that are still relatively unexplored. They mainly focus on the combination of the IoT and cloud environments. They claim that things like in-cloud data sharing, data combination, auditing cloud security, composite service responsibility and the impact of cloud decentralisation are still areas requiring more research to provide a more secure IoT.

Figure 8 presents a clustering the identified challenges in RQ2 (red) and solutions in RQ3 (blue). The clustering was done by the authors of this paper and it merely illustrates the links between various topics. Vast amount of work has been done with environmental constraints and with vulnerable devices and

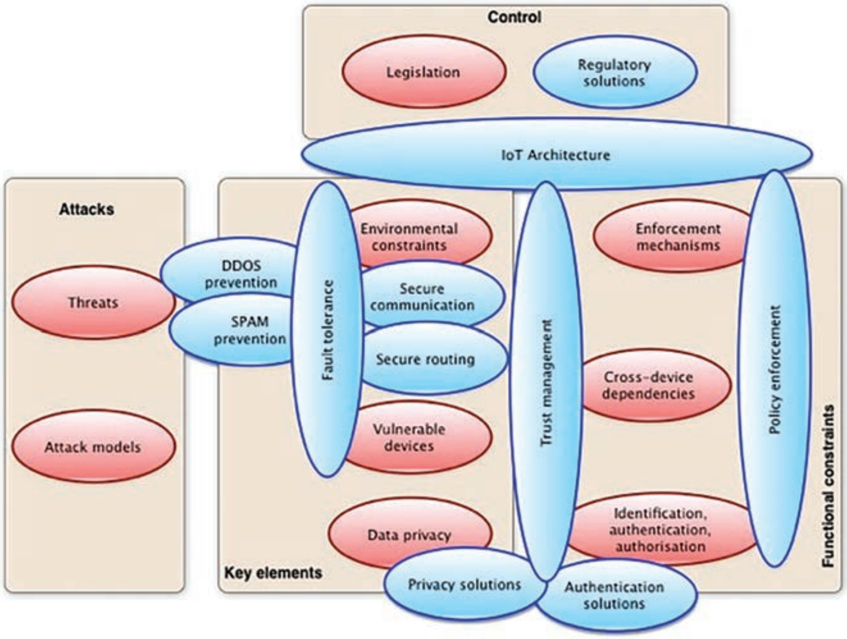

Figure 8 Challenges and solutions of IoT security research.

many of the solution categories link to these. If looking at the Figures 6 and 7 one can see some general trends in keywords. In general (Figure 6) the field has evolved from nodes and communication technologies to networks of devices, services and applications and more effort is put to data and its protection. Figure 7 presents similar tendencies among the more tightly focused set of papers. Both services and data are emphasized.

4 Discussion and Conclusion

This paper has shown how the security concerns in the IoT domain have evolved. The systematic mapping process of this study reveals how the evolution has happened, what kinds of concerns and solutions exist, and what gaps remain.

The present findings indicate that IoT security still needs significant work before it is ready for widespread public acceptance. Many security concerns persist. The most prevalent are privacy concerns, identification, authentication and authorisation concerns and lack of management (i.e. enforcement) methods. Privacy in the IoT is of the utmost importance, as the devices used often collect private, personal data, such as health information. Much has been done to secure sensitive users' data, such as personal information and physical characteristics, through authentication methods, such as: i) knowledge-based authentication (i.e. a way of authenticating with information that a user remembers, e.g. a password), ii) users' own knowledge-based authentication with smart cards or access cards and iii) physical characteristics (i.e. fingerprints) [24]. However, they do not adapt very well to the heterogeneous and resource-constrained environment of the IoT. In addition, considerable work has been done to either adapt the current protocols for IoT purposes or construct completely new ones for lightweight encryption and secure network transmission. Based on this study's outcomes, the most lacking aspect of the IoT security is currently authentication and authorisation. The increasing number of IoT devices in users' daily lives make authentication and security critical. After authentication, the access control problem must be solved, as not everyone accesses everything. Many researchers present this as a key issue to solve, but these findings suggest a universal, efficient and scalable solution for IoT authentication issues is missing.

Finally, the multiple attack vectors of the IoT are worrisome. In addition to the current Internet threats, there are multiple new vectors presented. The open and public nature of many IoT systems makes them especially vulnerable to malicious attacks. This is further emphasised by the often-poor security deployed into the devices themselves. Communication by radio waves is susceptible to many types of attacks, ranging from eavesdropping to outright DoS attacks. The lacking enforcement methods makes this even more severe, creating extra pressure for the systems to be as error-tolerant as possible. If security continues to be a severe issue in IoT, it might eventually prevent technology adoption by end users and thus slow down the field's development. Further, research and review efforts are needed in assisting device manufactures, regulators, and implementers to prioritise efforts while developing IoT security strategies.

References

[1] Abomhara, M., and Koien, G. M. (2014). Security and privacy in the Internet of Things: Current status and open issues, *International Conference on Privacy and Security in Mobile Systems (PRISMS)*, 1–8, IEEE.

[2] Airehrour, D., Gutierrez, J., and Ray, S. K. (2016). Secure routing for internet of things: A survey, *Journal of Network and Computer Applications* 66, 198–213.

[3] de Almeida Biolchini, J. C., Mian, P. G., Natali, A. C. C., Conte, T. U., and Travassos, G. H. Scientific research ontology to support systematic review in software engineering, *Advanced Engineering Informatics*, 21(2), 133–151.

[4] Andrea, I., Chrysostomou, C., and Hadjichristofi, G. (2016). Internet of Things: Security vulnerabilities and challenges, *Proceedings – IEEE Symposium on Computers and Communications*, 180–187.

[5] Ashraf, Q. M., and Habaebi, M. H. (2015). Autonomic schemes for threat mitigation in Internet of Things, *Journal of Network and Computer Applications* 49, 112–127.

[6] Ashton, K. (2009). That 'Internet of Things' Thing, *Rfid Journal*, https://www.rfidjournal.com/articles/view?4986

[7] Atamli, A. W., and Martin, A. (2014). Threat-Based Security Analysis for the Internet of Things, *International Workshop on Secure Internet of Things*, 35–43.

[8] Bailey, J., Budgen, D., Turner, M., Kitchenham, B., Brereton, P., and Linkman, S. (2007). Evidence relating to object-oriented software design: A survey, *Proceedings – 1st International Symposium on Empirical Software Engineering and Measurement, ESEM 2007*, 482–484.

[9] Basu, S. S., Tripathy, S., and Chowdhury, A. R. (2015). Design challenges and security issues in the Internet of Things, *IEEE Region 10 Symposium, IEEE*, 90–93.

[10] Benabdessalem, R., Hamdi, M., and Kim, T.-H. (2014). A Survey on Security Models, Techniques, and Tools for the Internet of Things, In *7th International Conference on Advanced Software Engineering and Its Applications, IEEE*, 44–48.

[11] Blei, D., Carin, L., and Dunson, D. (2010). Probabilistic topic models, *IEEE Signal Processing Magazine* 27(6), 55–65.

[12] Blei, D. M., Ng, A. Y., and Jordan, M. I. (2000). Latent Dirichlet Allocation, *Journal of machine Learning research*, 993–1022.

[13] Bryman, A. (2007). The research question in social research: What is its role? *International Journal of Social Research Methodology*, 10(1), 5–20.

[14] Budgen, D., and Brereton, P. (2006). Performing systematic literature reviews in software engineering, In *Proceedings of the 28th international conference on Software engineering*, 1051–1052, ACM.

[15] Budgen, D., and Brereton, P. (2006). Performing systematic literature reviews in software engineering, In *Proceedings of the 28th international conference on Software engineering*, 1051–1052, ACM.

[16] Cisar, P., and Cisar, S. M. (2016). General vulnerability aspects of Internet of Things, *CINTI 2015 – 16th IEEE International Symposium on Computational Intelligence and Informatics, Proceedings*, 117–121.

[17] Cronin, P., Ryan, F., and Coughlan, M. (2008). Undertaking a literature review: a step-by-step approach. *British journal of nursing*, 17(1), 38–43.

[18] Ejaz, W., Anpalagan, A., Imran, M. A. et al. (2016). Internet of Things (IoT) in 5G Wireless Communications, *IEEE Access* 4, pp. 10310–10314.

[19] Fink, G. A., Zarzhitsky, D. V., Carroll, T. E., and Farquhar, E. D. (2015). Security and privacy grand challenges for the Internet of Things”, *International Conference on Collaboration Technologies and Systems (CTS), IEEE*, 27–34.

[20] Henze, M., Hermerschmidt, L., Kerpen, D., Häußling, R., Rumpe, B., and Wehrle, K. (2016). A comprehensive approach to privacy in the cloud-based Internet of Things. *Future Generation Computer Systems*, 56, 701–718.

[21] Hossain, M. M., Fotouhi, M., and Hasan, R. (2015). Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things, *IEEE World Congress on Services*, 21–28.

[22] IHS, (2018). Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions), *Statista*, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[23] Intenational Telecommunication Union, (2012). *Next Generation Networks – Frameworks and functional architecture models, Overview of the Internet of things*.

[24] Ju, S. H., Seo, H. S., Han, S. H., Ryou, J. C., and Kwak, J. (2013). A study on user authentication methodology using numeric password and fingerprint biometric information. *BioMed research international, 2013*, Chicago.

[25] Khakurel, J., Melkas, H., and Porras, J. (2018). Tapping into the wearable device revolution in the work environment: a systematic review, *Information Technology & People* 31(3), 791–818.

[26] Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., and Linkman, S. (2009). Systematic literature reviews in software engineering – A systematic literature review, *Information and Software Technology*, 51(1), 7–15.

[27] Kouicem, D. E., Bouabdallah, A., and Lakhlef, H. (2018). Internet of things security: A top-down survey, *Computer Networks*.

[28] Kumar, S. A., Vealey, T., and Srivastava, H. (2016). Security in Internet of Things: Challenges, Solutions and Future Directions, *49th Hawaii International Conference on System Sciences (HICSS)*, IEEE, 5772–5781.

[29] Leppanen, M., Lahtinen, S., and Ihantola, P. (2016). Hammer and Nails – Crucial Practices and Tools in Ad Hoc Student Teams, *IEEE 29th International Conference on Software Engineering Education and Training (CSEET)*, IEEE, 142–146.

[30] Mahmoud, R., Yousuf, T., Aloul, F., and Zualkernan, I. (2015). Internet of things (IoT) security: Current status, challenges and prospective measures, *10th International Conference for Internet Technology and Secured Transactions (ICITST)*, IEEE, 336–341.

[31] Malina, L., Hajny, J., Fujdiak, R., and Hosek, J. (2016). On perspective of security and privacy-preserving solutions in the internet of things. *Computer Networks*, 102, 83–95.

[32] Maple, C. (2017). Security and privacy in the internet of things, *Journal of Cyber Policy*, 2(2), 155–184.

[33] Hung, M. (2017). *Leading the IoT*.

[34] Minerva, R., Biru, A., and Rotondi, D. (2015). Towards a definition of the Internet of Things (IoT), *IEEE Internet of Things*, 1, 1–86.

[35] Nguyen, K. T., Laurent, M., and Oualha, N. (2015). Survey on secure communication protocols for the Internet of Things. *Ad Hoc Networks*, 32, 17–31.

[36] Ornes, S. (2016). Core Concept: The Internet of Things and the explosion of interconnectivity, *Proceedings of the National Academy of Sciences*, 113(40), 11059–11060.

[37] Patton, M., Gross, E., Chinn, R., Forbis, S., Walker, L., and Chen, H. (2014). Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things (IoT), *IEEE Joint Intelligence and Security Informatics Conference*, IEEE, 232–235.

[38] Petersen, K., Feldt, R., Mujtaba, S., and Mattsson, M. (2008). Systematic mapping studies in software engineering, *EASE'08 Proceedings of the 12th international conference on Evaluation and Assessment in Software Engineering*, pp. 68–77.

[39] Porras, J., Pänkäläinen, J., Knutas, A., and Khakurel, J. (2018). Security In The Internet Of Things – A Systematic Mapping Study, *Proceedings of the 51st Hawaii International Conference on System Sciences*, 3750–3759.

[40] Razzak, F. (2012). Spamming the Internet of Things: A possibility and its probable solution, *Procedia Computer Science*, 658–665.

[41] Roman, R., Najera, P., and Lopez, J. Securing the Internet of Things (IoT), *IEEE Computer*, 44, 51–58.

[42] Roman, R., Zhou, J., and Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things, *Computer Networks*, 57(10), 2266–2279.

[43] Sadeghi, A.-R., Wachsmann, C., and Waidner, M. (2015). Security and privacy challenges in industrial internet of things, *Proceedings of the 52nd Annual Design Automation Conference on – DAC '15*, 1–6.

[44] Singh, J., Pasquier, T., Bacon, J., Ko, H., and Eyers, D. (2016). Twenty Security Considerations for Cloud-Supported Internet of Things, *IEEE Internet of Things Journal*, 3(3), 269–284.

[45] Suo, H., Wan, J., Zou, C., and Liu, J. (2012). Security in the Internet of Things: A Review, *International Conference on Computer Science and Electronics Engineering*, IEEE, 648–651.

[46] Telefonaktiebolaget LM Ericsson, "Internet of Things forecast", 2018. https://www.ericsson.com/en/mobility-report/internet-of-things-forecast

[47] Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., and Kikiras, P. (2015). On the Security and Privacy of Internet of Things

Architectures and Systems, *International Workshop on Secure Internet of Things (SIoT)*, IEEE, 49–57.

[48] Wang, C., and Blei, D. M. (2011). Collaborative topic modeling for recommending scientific articles, *Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining – KDD '11*, ACM Press, 448.

[49] Weber, M., and Boban, M. (2016). Security challenges of the internet of things, *39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, IEEE, 638–643.

[50] Weber, R. H. (2010). Internet of Things – New security and privacy challenges, *Computer Law & Security Review*, 26(1), 23–30.

[51] Weber, R. H. (2015). Internet of Things: Privacy issues revisited, *Computer Law and Security Review*, 31(5), 618–627.

[52] Wortmann, A., Combemale, B., and Barais, O. (2017). A Systematic Mapping Study on Modeling for Industry 4.0, *Proceedings – ACM/IEEE 20th International Conference on Model Driven Engineering Languages and Systems, MODELS*.

[53] Wurm, J., Hoang, K., Arias, O., Sadeghi, A.-R., and Jin, Y. (2016). Security analysis on consumer and industrial IoT devices, *21st Asia and South Pacific Design Automation Conference (ASP-DAC)*, IEEE, 519–524.

[54] Yan, Z., Zhang, P., and Vasilakos, A. V. (2014). A survey on trust management for Internet of Things, *Journal of Network and Computer Applications*, 120–134.

[55] Yu, T., Sekar, V., Seshan, S., Agarwal, Y., and Xu, C. (2015). Handling a trillion (unfixable) flaws on a billion devices, *Proceedings of the 14th ACM Workshop on Hot Topics in Networks – HotNets-XIV*, ACM Press, 1–7.

[56] Zhang, C., and Green, R. (2015). Communication Security in Internet of Thing: Preventive Measure and Avoid DDoS Attack over IoT Network, *Proceedings of the 18th Symposium on Communications & Networking*, 8–15.

[57] Zhang, Z. K., Cho, M. C. Y., and Shieh, S. (2015). Emerging security threats and countermeasures in IoT. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, 1–6. ACM.

[58] Zhao, K., and Ge, L., (2013). A Survey on the Internet of Things Security, *Ninth International Conference on Computational Intelligence and Security*, IEEE, 663–667.

[59] Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. In *Proceedings of the 18th international conference on evaluation and assessment in software engineering*, (p. 38). ACM.

Biographies

Jari Porras D.Sc (Tech) is Professor of Software Engineering (especially Distributed Systems) at the Lappeenranta University of Technology (LUT). He has conducted research on parallel and distributed computing, wireless and mobile systems and services as well as sustainable ICT. In last years he has focused his research on human and sustainability aspects of software engineering. He is actively working in international projects and organizations.

Jayden Khakurel received his Ph.D. degree under the supervision of Prof. Jari Porras and Prof. Helinä Melkas at the LUT University. His thesis focused on understanding the needs for acceptance and continued use of quantified self-tracking wearable devices, from a device characteristic perspective. His research focuses on Artificial Intelligence, Wearable Devices and Behavioral Science in the areas of human-computer interactions. Jayden Khakurel received a M.Sc. in Computer Science (2013) from the Lappeenranta University of Technology, MBA (2013) from the Kouvola University of Applied Science (Current XAMK).

Antti Knutas D.Sc. (Tech) is an Assistant Professor of Software Engineering (especially software construction) at the Lappeenranta University of Technology (LUT). His research interests involve computer-supported cooperative work (CSCW), non-traditional software engineering processes of digital services, and the design of community-driven socio-technical systems from a software engineering perspective.

Jouni Pänkäläinen M.Sc was a Master's student in Lappeenranta University of Technology. His thesis work was on security and usability challenges in IoT infrastructures. He graduated in December 2016.