Security In The Internet Of Things – A Systematic Mapping Study

Jari Porras
Lappeenranta University of
Technology
Jari.Porras@lut.fi

Jouni Pänkäläinen
Lappeenranta University of
Technology
Jouni.Pankalaine@gmail.com

Antti Knutas
Lappeenranta University of
Technology
Antti.Knutas@lut.fi

Jayden Khakurel
Lappeenranta University of Technology
Jayden.Khakurel@lut.fi

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 paper 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 systematic mapping study as the methodological approach. Based on the chosen search strategy, 38 articles (of close to 3500 articles in the field) 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. The mapping study identifies nine main concerns and 11 solutions. However, the findings also reveal challenges, such as secure privacy management and cloud integration that still require efficient solutions.

1. Introduction

The modern idea of the Internet of Things (IoT) was first introduced by Mark Weiser in 1991 [42]. Weiser wrote "*The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it*". In his article, Weiser talked about interconnected devices that disappear into the background of our everyday lives. Since the beginning of the 21st century, the Internet has spread everywhere. Gartner [14] has estimated that 6.4 billion devices will be connected to the Internet in 2016: 30 percent more than in 2015. A growing number of these devices are IoT devices. IoT is one of the biggest drivers of the other main trends of technology, such as 5G [33]. 5G and IoT are finally, after almost three decades, making the futuristic vision of Mark Weiser a reality.

The Global Standards Initiative defines [15] the 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". This means that besides the traditional Internet "things", such as desktop and laptop computers, the IoT definition contains elements such as cars, clothing and even buildings. By connecting all these devices necessary for everyday life to the Internet, new security concerns arise. 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.

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) [21] is used to collect data and analyse the literature. Using this approach, this research will attempt to answer the following research questions.

- RQ1: What kinds of **security related concerns** have been raised within IoT?
- RQ2: What kinds of **solutions** have been presented to improve the security of IoT?
- RQ3: 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 from 2000 to 2016.

The paper is organised as follows: Section 2 presents the research design and implementation, explaining the research methods and SMS. Sections 3 present the literature review results in respect to the research question emphasising the trends of the IoT security research, including focuses on the content of the research. Section 4 concludes the paper.

HICSS

2. Research design and implementation

An SMS is a secondary study to classify and thematically analyse earlier research [22, 29]. Such a study classifies and structures a field of interest in research by categorising publications and analysing their publication trends [29]. Additionally, mapping studies can analyse what kinds of studies have been done in the field, and the research methods and outcomes [7]. It is closely related to a wider secondary study, a systematic literature review (SLR), which aims at gathering and evaluating all the research results on a selected research topic [3, 20]. An SMS is more general in search terms and aims at classifying and structuring the field of research, while the target of SLR is to summarise and evaluate the research results. Kitchenham and Charters [20] 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. Both kinds of studies can be used to identify research gaps in the current state of research. For this study, an SMS approach was selected and a process developed by Petersen et al. [29] for the field of software engineering followed. The research process steps, adapted for the review process, are listed as follows.

a) Define the research questions based on the objectives of the research.
b) Define search queries based on the research questions. Finding proper search queries (terms) might require an iterative process. Tools like NAILS[1] and HAMMER [23] can be used for the first iterations.
c) Search articles on primary studies using search strings on scientific libraries and databases.
d) Screen the initial set of articles by applying inclusion and exclusion criteria to determine whether each potential article should be included or excluded from this study. 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.
e) Extract the predefined set of data from the selected set of articles.
f) Analyse the extracted data to answer the research questions. Various tools exist for the analysis, such as HAMMER[2] , KHCoder[3] or VOSviewer[4].
g) Present the acquired results.

The search string was kept rather open due to the aim for a broad perspective on security issues covered in the IoT: *(("Internet of Things" OR "IoT") AND "security")*

Searches were conducted via digital libraries such as ACM Digital Library, IEEE Xplore Digital Library and Science Direct. These libraries have been chosen because they are identified as relevant to the information technology field.

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 [19]. Thus, the following set of inclusion and exclusion criteria were used.

- *Published between 1.1.2006 and 31.7.2016*
- *Topic is IoT and information security*
- *Scientific and peer-reviewed articles*
- *Relevant to the research questions*
- *Articles written in English*

Information security is a vast field of research. To keep the number of articles reasonable, the following exclusion criteria were used:

- *Articles concerning specific technologies, such as protocols or identity management methods*
- *Editorials and non-peer reviewed articles*
- *Articles that are not fully available*
- *Duplicates of already included papers*

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.

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
ScienceDirect	1377	13
Total	**3454**	**38**

The template was used to register the relevant information from the final set of reviewed 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[5] was executed and the received data were then analysed with NAILS and KHCoder. The larger data from Web of Science was used for general topic modelling. The query produced 2143 articles, including only 27 of the selected articles; thus, the analysis of this material gives a bit different perspective to the topic.

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 the broader data from Web of Science related to this SMS are presented.

The analysis (see Figure 1) shows the number of articles published per year from the selected set of articles. The search was limited to 2006–2016, and relevant articles only started to appear around 2010. The Web of Science data show only one article in 2005 and others from 2006 onwards. Since 2010, there has been a steady increase in the number of articles in the targeted topic. Out of the selected 20 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.
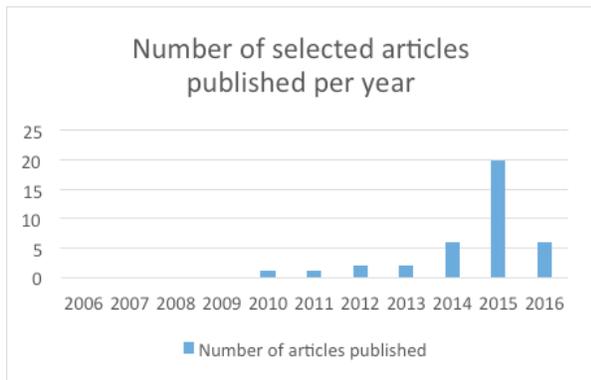

Figure 1. Number of selected articles published per year.

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.

The analysis of the larger dataset from Web of Science offers another perspective on IoT security research. NAILS uses the Latent Dirichlet Allocation (LDA) topic modelling algorithm [11] 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 [10]. It is commonly used for text analysis, and equivalent methods have been used to statistically analyse scientific texts in previous studies [38].
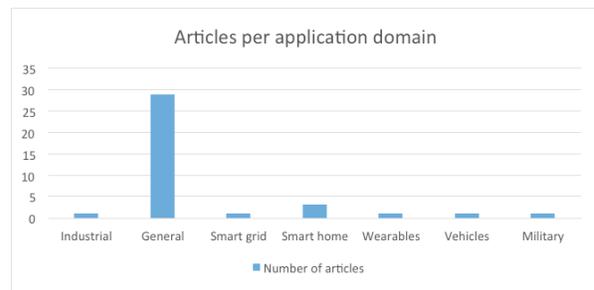

Figure 2. Number of selected articles published by application domain.

Table 2. LDA-based Web of Science data topics.

Topic 1 Networks	Topic 2 Smart systems	Topic 3 Security and IoT	Topic 4 Service
network	system	security	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

Table 2 presents the topics identified by the LDA modelling feature of NAILS (note that the authors have named these topics based on their content). Topics 1 and 4 seem to be related to technologies, such as networks, protocols and service models. Topics 2 and 3 seem to be close to the objectives of this paper. While

examining how the selected 38 articles are related to these topics, a clear category of papers under interest can be found (21 out of 27 papers are under topic 3, while only three under topic 2 and the rest in topics 1 and 4). Topic 3 is security and IoT-focused, while topic 2 contains papers on smart systems and technologies.

To further analyse the contents of topic 3 (Security and IoT) of the LDA analysis, the set of articles on topic 3 were further processed by KHCoder. KHCoder is a quantitative content analysis tool that allows text mining and analysis. The abstracts of all 549 articles of topic 3 were analysed, and the yearly trends were visualized. Figure 3 presents the topic's development by years (size of the bubble emphasises the importance of the keyword). The keywords for the search string used in this mapping study are all well represented by the research from 2014 to 2016.
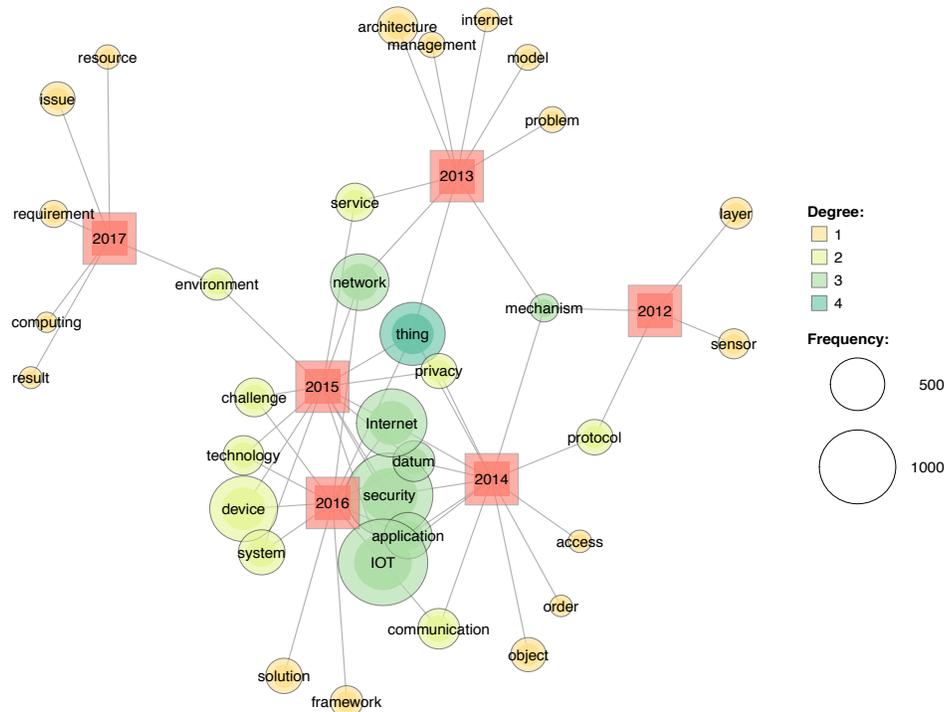

Figure 3. Word co-occurrences by year in topic 3 (security and IoT) articles

RQ1: *What kinds of security concerns have been raised within IoT?*

According to Wrum et al. [43], 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.

Environment constraints

One of the main challenges of IoT security is the constraint set by the environment. Hossain et al. [17] 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. [31] agree that the computational and network limitations are constraints to IoT security.

Vulnerable devices

According to many researchers [45, 47] an important aspect in IoT security is device security. Yu et al. [45] 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. [28] 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.

Data privacy

Many studies [2, 13, 16, 26, 32] 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 [26]. 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. [26] 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).

Enforcement mechanisms

According to Yu et al. [45], 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. [24] also worried about the IoT's lack of security updates.

Cross-device dependencies

Yu et al. [45] 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. They present a few examples: the NEST Protect home system has 188 cross-device policies, Wemo Plugin has 227 and Scout Alarm has 63.

Identification, authentication and authorisation

Many researchers [1, 2, 8, 12, 32, 47] 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. [27] 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.

Sources of threats

Atamli et al. [6] 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.

Attacker models

Based on the selected set of articles IoT has various attack vectors that need to be considered.
- *Denial of Service attacks* [5, 32, 46]
- *Physical attacks* [5, 32, 48]
- *Network attacks* [1, 2, 5, 9, 17, 24, 32]
- *Encryption attacks* [4]

Legislative issues

In 2010, Weber [40] 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 [41] Weber says, that an international regulatory framework is still missing. Suo et al. [36] 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.

RQ2: 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.

Trust management

Yan et.al. [44] and Hossain et al. [17] 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. [31] 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.

Authentication

Zhang et al. [47] 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. [25] also write about authentication schemes. They present a one-time, one-cipher method based on a request-reply mechanism.

Privacy solutions

Roman et al. [31] 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. [16] 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.

Policy enforcement

Yu et al. [45] 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.

Fault tolerance

Roman et al. [31] 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.

Secure communication

Kumar et al. [24] 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. [27] 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.

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).

DDoS protection

According to Zhang et al. [46], 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 neighbuoring 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 [46].

Spam prevention

Razzak [30] 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.

IoT architectures

Vasilomanolakis et al. [37] 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).

Regulatory solutions

Weber et al. [39] 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.

RQ3: 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. [34] 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. [26], 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. [32] 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. [35] 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.
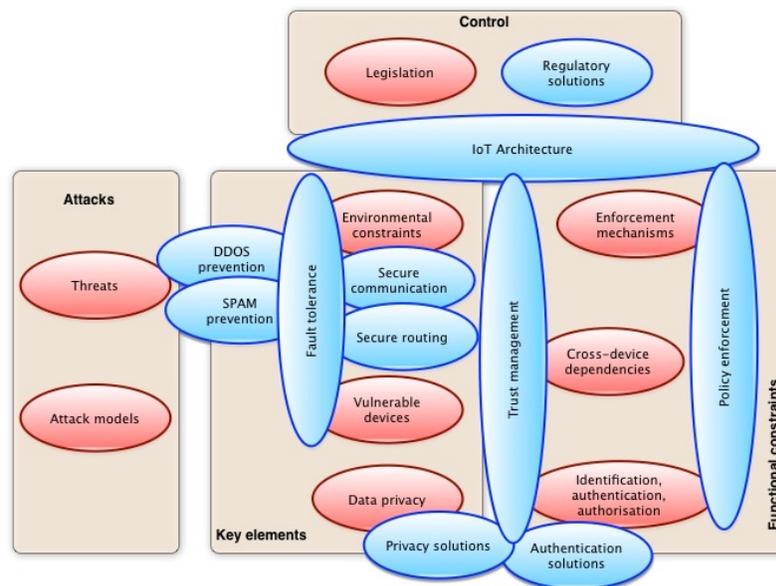

Figure 4. Challenges and solutions of IoT security research.

If mapping the challenges (red) and solutions (blue) presented in the selected articles (see Figure 4), one can see that environment constraints and vulnerable device challenges have been emphasised by many solutions (fault tolerance and trust management being the most influential ones). The highly distributed nature of the resource-limited IoT environment is still a challenge. The lack of proper methods for managing (enforcement, authorization, etc.) the environment remains a challenge. The trends of the IoT security research presented in Figure 3 show that these might be potential research topics for future studies (management has been one trend in 2013 while 2017 shows some signs of studying the resource limited environment).

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) [18]. 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.

6. References

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

[2] Airehrour, D., Gutierrez, J., and Ray, S.K. Secure routing for internet of things: A survey. JNCA66, (2016), 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 (2007), 133–151.

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

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

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

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

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

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

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

[11] Blei, D.M., Edu, B.B., Ng, A.Y., Edu, A.S., Jordan, M.I., and Edu, J.B. Latent Dirichlet Allocation. CrossRef Listing of Deleted DOIs 1, (2000), 993–1022.

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

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

[14] Gartner Inc. Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015. http://www.gartner.com/newsroom/id/3165317 (accessed Aug 8, 2016).

[15] Global Standards Initiative. Internet of Things Global Standards Initiative. http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx (accessed Aug 8, 2016).

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

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

[18] Ju, S., Seo, H., Han, S., Ryou, J., and Kwak, J. A Study on User Authentication Methodology Using Numeric Password and Fingerprint Biometric Information. BioMed Research International 2013, (2013), 1–7.

[19] Khakurel, J., Melkas, H., and Porras, J. Tapping into the wearable device revolution in the work environment: A systematic review. Information Technology and People, (2017), 1–17.

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

[21] Kitchenham, B. and Charters, S. Guidelines for performing Systematic Literature reviews in Software Engineering Version 2.3. Engineering 45, 4 (2007), 1051.

[22] Kitchenham, B. and Charters, S. Guidelines for performing Systematic Literature Reviews in Software Engineering. Engineering 2, (2007), 1051.

[23] Knutas, A., Hajikhani, A., Salminen, J., Ikonen, J., and Porras, J. Cloud-based Bibliometric Analysis Service for Systematic Mapping Studies. Proceedings of the 16th International Conference on Computer Systems and Technologies, (2015), 184–191.

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

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

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

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

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

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

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

[31] Roman, R., Najera, P., and Lopez, J. Securing the Internet of Things (IoT). IEEE Computer 44, (2011), 51–58.

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

[33] Rysavy, B.P. OR MOVE ? IoT & 5G : WAIT OR MOVE ? 2016, 1–10. http://www.rysavy.com/Articles/2016-09-IoT-5G.pdf. (accessed Aug 8, 2016).

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

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

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

[37] Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., and Kikiras, P. On the Security and Privacy of Internet of Things Architectures and Systems. International Workshop on Secure Internet of Things (SIoT), IEEE (2015), 49–57.

[38] Wang, C. and Blei, D.M. 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 (2011), 448.

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

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

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

[42] Weiser, M. The Computer for the 21st Century. Scientific American 265, 3 (1991), 94–104.

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

[44] Yan, Z., Zhang, P., and Vasilakos, A. V. A survey on trust management for Internet of Things. Journal of Network and Computer Applications 42, (2014), 120–134.

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

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

[47] Zhang, Z.-K., Cho, M.C.Y., and Shieh, S. Emerging Security Threats and Countermeasures in IoT. Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security - ASIA CCS '15, ACM Press (2015), 1–6.

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