SECURITY AND PRIVACY IN IOT ENVIRONMENT: A SYSTEMATIC MAPPING STUDY

Moussa WITTI and Dimitri KONSTANTAS

Information Science Institute University of Geneva
Route de Drize 7, 1227 Carouge, Switzerland

ABSTRACT

Over the last decades, the rapid grow of Internet of Things or IoT connected to the Internet has accelerated sensitive and non-sensitive data exchange such as lifestyle, personal data (using we arables sensors, smart devices). A huge number of heterogeneous sensors may convey or collect and dispatch sensitive data from an endpoint to worldwide network on Internet. Privacy remain an important issues, therefore Internet of Things has developed significant attention in the research. In this paper, we aim to evaluate current research state related to privacy and security in IOT by identifying existing approaches and publications trends. Therefore, we have conducted a systematic mapping study using auto mated searches from selected relevant academics databases. The result of this mapping highlights research type and contribution in different facets and research activities trends in the topic of "security and privacy" in IoT edge, cloud and fog environment.

KEYWORDS

Internet of Thing, privacy, security, mapping study

1. INTRODUCTION

Recently we are witnessing the increase use of "Internet of Things" (IoT). According to Gartner's report on "IoT Technology Disruptions", IoT security market will grow from $547 million in 2018 to $841 million by the end of 2020. Gartner predicts that the use of the IoT will increase of 31% up. Approximately 67% of the use of IoT will be located in North America, Western Europe and China. From RFID technologies in supply chain management, to wearables devices in lifestyle or healthcare monitoring system, and smart sensors in automotive or in home automation, the use of "Internet of things" has led to change our life.

However, data collection raises privacy and security issues in Internet of Things (IoT) environment. Using heterogeneous protocols that are WiFi, Bluetooth, ZigBee, sub-GHz, Z- Wave, Thread and 2G/3G/4G cellular, along end-to-end communication how to ensure security and preserve privacy?

In this paper, we conducted a systematic mapping study to perform thematic analysis, trends and future works about security and privacy-preserving methods and models in IOT environment.

Dhinaharan Nagamalai et al. (Eds) : CSEN, NCWC - 2018
pp. 09–19, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81202

The paper is organized as follows: Section 2 presents related work in the research, Section 3 defines the research method, Section 4 provides the results of the systematic mapping and describes overview of included studies while Section 5 try to respond to the research questions and discussing main findings. Section 6, deal with the threats to research validity and Section 7 provides conclusions and directions for future work.

2. RELATED WORK

In the literature, privacy and security issues are challenged and several security models for IoT have been designed. The rapid growth of IoT has extended Internet to any small smart devices in distributed environment [11] thus has introduced a serious problematic. As IoT environment is more heterogeneous, more complex [17] and maintaining security is very critical in distributed system as well as cloud and fog environment [1] [2] [23] [32].

Most research studies [5] [8] [16] [17] [18] [27] are focused on how to integrate security among application, perception and transport layers level for distributed or cloud environment such as IaaS (Infrastructure as a Service), SaaS (Software as Service), and PaaS (Platform as Service). Except rare studies [12] [25] [33], focused on specific use, we found only one research paper using systematic mapping study on IOT and cloud computing [7].

To protect sensitive data a huge of privacy-preserving algorithms have been developed such as k-anonymity, l-diversity. The concept of k-anonymity has been introduced by L. Sweeney and P.Samarati [21] in order to preserve privacy. While l-diversity is a data anonymization technique based on generalization and suppression often with a loss of the quality of the information. L-diversity is defined as extension of the k-anonymity [30]. Another algorithm "t- closeness" [22] has been developed to anonymize data [8][20]. This technique is an extension of l-diversity and designed to preserve the confidentiality of sensitive data while reducing the granularity of data representation.

3. RESEARCH METHOD

In the experimental software engineering, there are two main approaches to conduct a literature reviews that are “Systematic Mapping Studies” and “Systematic Literature Reviews”. If a researcher aims to identify, classify, and evaluate result to respond for a specific research question “Systematic Literature Reviews” is the adequate approach but if he seeks to answer for multiples research questions “Systematic Mapping Study” is the best one. In this paper, we have conducted the formal guidelines of Systematic Mapping Study from Petersen et al. [25] performed in five steps. The outcome from each step gives the input for the next step. SMS start with the initial research questions built up to provide a general scope for the study used to find out research papers (step 2) from the selected digital libraries (according the research fields). In the next step, screening process start with a set of inclusion and exclusion criteria to select relevant papers (step 3). Finally, the keywording process (step 4) enable classification and data extraction (step 5) wich would have to answer the research questions (figure 1).

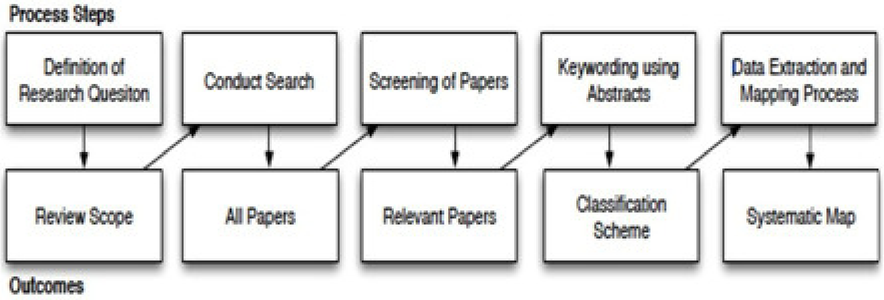


Figure 1: Systematic Mapping Process

3.1 OBJECTIVES

We aim to assess how privacy and security are managed in different context of use of IOT such as IOT edge, IOT cloud and fog environment. We aim to analyse and map research studies that deal with security and privacy concerns in the use of Internet of Thing. Thus, we conducted systematic mapping study to assess data securisation methods and privacy-preserving technique in the research field. We aim also to analyze research contributions and trends in IOT edge, IOT cloud and fog environment.

3.2 RESEARCH QUESTIONS

“How security and privacy are provided and maintained in IOT enabled-technologies?”

We have decomposed this main research question into four specific questions as show in the table 1.

Table 1. Research questions

N°	Questions	Motivation
RQ1	What are security and privacy issues in IOT environment?	Find out an overview of studies about security and privacy in IOT.
RQ2	What are the field of the studies?	Find out the context of the related studies.
RQ3	How provide security and privacy in IOT environment?	Explore the state of the related research activities and their evolution.
RQ4	What are research trends in IOT environment about security and privacy concerns?	Assess future trend of the research activities about security and privacy in IOT.

3.3 SEARCH STRATEGY

According to our research questions, we have built up our Search Strings formulated using general terms with **AND** clause as **“IOT AND (security and privacy)”**. We adopted use of boolean operator such as **“AND”** to focus our search only on specific subjects. Therefore, we have restricted our search items to select from digital libraries only scientific papers, with as the specified keywords related to security and privacy in IOT. Then we used that search string above in the major search engines for academic studies, which are **ACM**, **DBLP**, **Google Scholar**, **iEEE**, **Science Direct**, **Springer**. For each digital libraries, according to their search rules, we did some customization in order to adapt our generic search string.

3.4 INCLUSION-EXCLUSION CRITERIA

We filtered out the result of the automatic search; in the relevant academic libraries as explain in the previous subsection, by applying inclusion and exclusion criteria detailed in table 2. The main selection criteria are:

- Selection by **"title"** and by **"abstract"**: we first selected papers only with **"IOT"** and **"privacy"** or **"security"** terms in the title or in the **"abstract"**.

- Selection by full paper reading: we selected paper in English and with a research contribution in IOT environment related to security or privacy.

Table 2. Inclusion / Exclusion Criteria

Inclusion	**Exclusion**
Studies with title related to IOT.	Paper in other language than English.
Studies related to security in IOT.	Paper without Abstract.
Studies related to privacy concern in IOT.	Paper from workshop.
Studies presenting security and privacy concerns in IOT environments	Books.
Studies about security and privacy in IOT cloud environment.	Studies about other issues in IOT environment.
Studies about security and privacy in IOT fog environment.	Paper out of our scope

4. EXECUTION

The search is executed using automated search engines. During screening process of relevant studies according to our inclusion-exclusion criteria defines previously, we examined firstly title, then abstract and keyword. For those without sufficient details in this part, we did full reading of the content of paper.

4.1 CONDUCTING THE SEARCH

We adapted the search string to each databases and obtained relevant studies in four steps as shown in figure 2:

Step 1: We obtained 3205 studies by putting our search string into the search engines of ACM,DBLP, Google Scholar, iEEE, Science Direct, Springer databases.

Step 2: We remove duplicated studies from more than one source and we obtained 2807 papers.

Step 3: We obtained 522 potentially relevant studies after removing all studies that not matching with research questions.

Step 4: Finally, after applying selection criteria, we obtained 54 relevant papers.

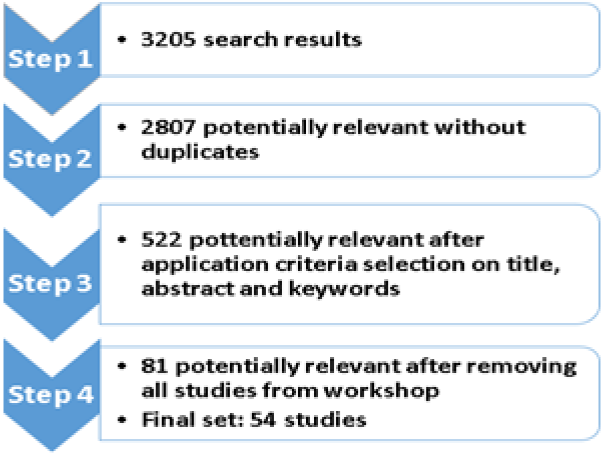

Step 1
• 3205 search results
Step 2
• 2807 potentially relevant without duplicates
Step 3
• 522 pottentially relevant after application criteria selection on title, abstract and keywords
Step 4
• 81 potentially relevant after removing all studies from workshop
• Final set: 54 studies

Figure 2: Main steps for selecting relevant studies

4.2 ANALYSIS AND CLASSIFICATION

Keywording phase remains important in the systematic mapping process: after reading firstly title, then abstract and when it is necessary we did full paper reading to search terms and concepts reflecting the research contribution. During abstract or full paper reading process, we categorized relevant papers into one facet or research contribution. Selected studies may be mapped according to their research focus and the context. Then, we can build-up a cluster from classification scheme.
We regrouped all relevant publications into three contributions research type facets such as:

- **Security facet**: IAM (or identity and access management), AAA (or Authentication Authorization Accounting), privacy, K.E.M or (Key Exchange and Management) , trust, confidentiality, integrity, cryptography, availability, I.A.A (or Identification Authentication and Authorization), Anonymity

- Application context or application field facet which are: medical, industrial, public

- Environment facet: IOT Edge, IOT Distributed, IOT cloud, IOT Fog.

In addition, we have obtained flowing research type such as:

- **Opinion papers** : the author gives his views about technical solutions or approach given by others.

- **Survey papers**: In a survey paper, data and results are taken from other papers, the authors draw out some new conclusion.

- Solution proposal

- **Evaluation research papers**

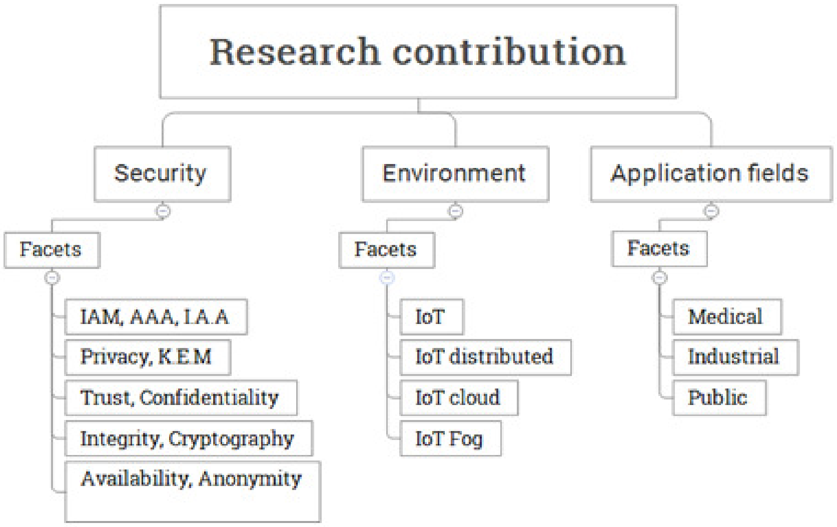


Figure 3: Contributions of relevant studies

5. DISCUSSION

5.1 RQ1: WHAT ARE SECURITY AND PRIVACY ISSUES IN IOT ENVIRONMENT?

Throughout the systematic process, we have identified that all relevant papers discuss about how to secure end-to-end communication. Main issues related to privacy and security are using authentication, data encryption, key exchange mechanisms. Privacy issues are well discussed in general but solutions are not given in details.

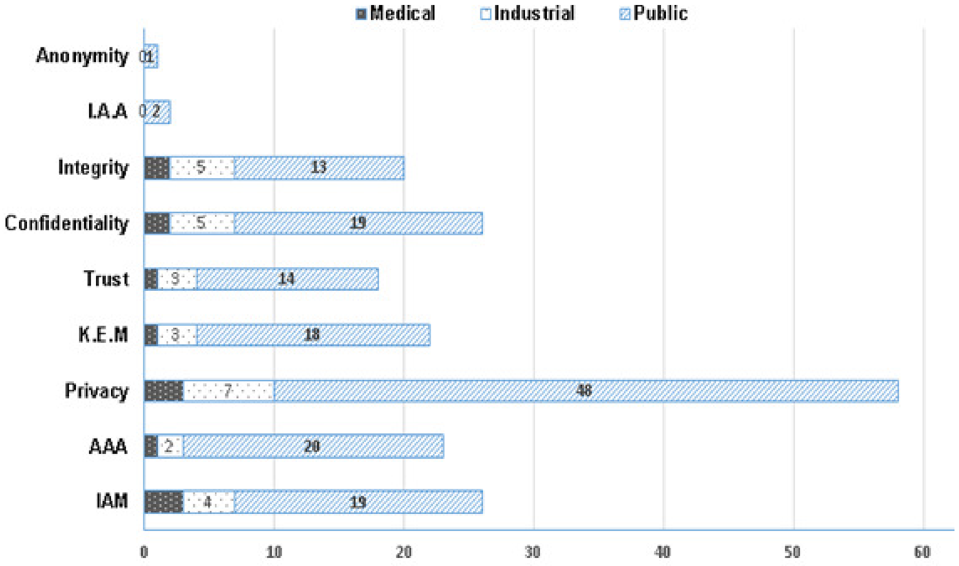


Figure 4: Contributions of relevant studies

5.2 RQ2: WHAT ARE THE FIELD OF THE STUDIES?

Most of the papers (85%) are addressed to public domain. The rest is related to medical (2%) and industrial uses (9%). There are some papers (4%) dealing with all three domains which are public, medical and industrial.

5.3 RQ3: HOW EVOLVED SECURITY AND PRIVACY IN IOT ENVIRONMENT?

From classification scheme in figure 3, the contribution of relevant studies are about mainly authentication, authorization, data encryptions. In the cloud as well as in the distributed IOT environment, the existing securization methods in the literature are used. Most of the selected papers deal with privacy issues without developing algorithms or giving out a methodology.

5.4 RQ4: WHAT ARE RESEARCH TRENDS IN IOT ENVIRONMENT ABOUT SECURITY AND PRIVACY CONCERNS?

From selected papers after data extraction and contributions mapping (figure. 5), we can assess research trends. IOT uses are widespread in public area while in medical and industrial fields IOT remains less developed. On the other hand, most of relevant papers are dealing with security concerns in distributed environment. Globally, privacy concerns in personal sensitive data collection in IOT cloud or fog environment are not detailed and remain in embryonic stage.

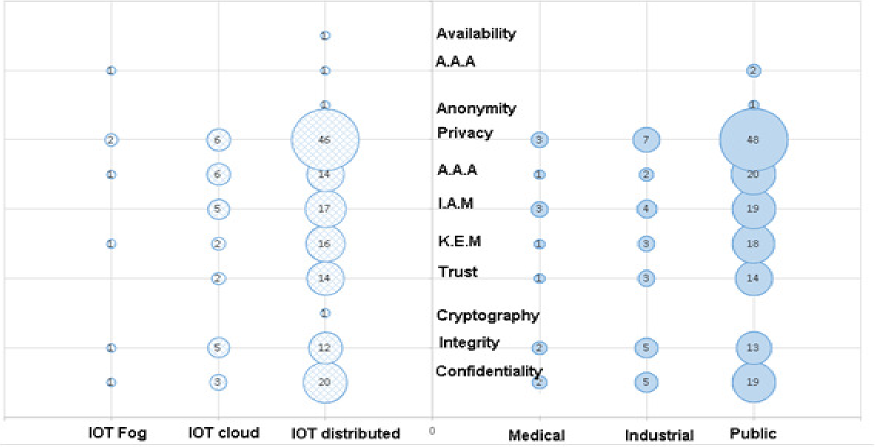


Figure 5: Result mapping of selected studies

6. THREATS TO VALIDITY

In this paper, the method adopted may occur a number of known threats to validity that can bias the result. In our study, we given attention to these threats and more efforts have been done to mitigate these risks. In this section, we list the main threats, which may occur while conducting a Systematic Mapping Study. First, the search criteria of our study were defined on the assumption that our work should only be oriented towards publications related to our research questions (e.g table 1). However, there is a risk that the search engines may have used some relevant publications. To minimize the risk we used unambiguous terms with logical operator to construct a search string. Then, to conduct this study, we selected some academic databases that we considered relevant to our study.

All these digital libraries have been selected on the one hand for their field of application relating to our study and on the other hand for their ranking in scientific research. It is possible that we have not integrated some libraries with relevant publications related to our study. Thus, some relevant articles would be omitted. However, this risk is mitigated by the fact that most of the databases contain a large number of identical items, and we have already experimented with this redundancy in the databases we have selected. Therefore, article redundancy mitigates this risk.

The inclusion and exclusion criteria were defined in a top-down approach from title, abstract, and then full content. First, we have selected publications with title and abstract in English. Then we selected potentially relevant papers that having key terms of our search in the title a nd in the abstract. Finally, we filtered all papers by full content reading according. We probably omit some relevant papers in others languages but our strategy is to execute search string similarly in all selected digital libraries. Finally, the classification scheme of research type or research contribution may be different from one research to another. In our case, we adopted to classify all relevant publications according to the similar terms redundant in their keyword or in their main content.

7. CONCLUSION

By identifying, analysing, classifying publications, we have conducted a systematic mapping study to perform thematic analysis, trends and future works about security and privacy in IOT environment. We have screened 3205 publications, only 54 studies were considered as relevant according to inclusion-exclusion criteria we defined. All papers have been classified according to research type contribution and research type facet. We mapped all papers according to their research contributions and we obtained a graph to assess the current research contributions and their trends in the future.

Our future work will be to complete this work by writing a survey paper to assess all possible solutions to secure and preserve-privacy in IOT environment.

REFERENCES

[1] Aaditya Jain, B. S. (2016, April). Internet of Things: Architecture, security goals, and challenges. International Journal Innovative Research in Science & Engineering (IJIRSE), Vol.No2:Issue4.

[2] Alfaqih, T. M., & Al-Muhtadi, J. (2016). Internet of Things Security based on Devices Architecture.International Journal of Computer Applications.

[3] Athreya, A. P., DeBruhl, B., & Tague, P. (2013). Designing for self-configuration and self-adaptation in the “internet of things" in Collaborative Computing: Networking Applications and Worksharing. 9th International Conference Collaboratecom, (pp. 585-592).

[4] Bagozzi, R. Y. (1991). Assessing Construct Validity in Organizational Research . Administrative Science Quarterly (36:3), pp 421-458.

[5] Bouij-Pasquier Imane, A. A. (2015). A Security Framework for Internet of Things. 14 th International conference, CANS 2015, , (pp. 19-31 Volume 9476 of the series Lecture Notes in Computer Science). Marrakesh.

[6] Burnett L., K. B.-S. (Volume 10, Issue 4, May 2003). The GeneTrustee: a universal identification system that ensures privacy and confidentiality for human genetic databases. Journal of law and medicine, 506-513.

[7] Cavalcante E. et al. (2016). On the interplay of Internet of Things and Cloud Computing: A systematic mapping study. Computer Communications Volumes 89-90, Pages 17-33.

[8] Charu C. Aggarwal; Philip S. Yu, eds. (2008). "A General Survey of Privacy". Privacy-Preserving Data Mining – Models and Algorithms

[9] Ding Chao, L. Y. (2011). Security Architecture and Key Technologies for IoT/CPS . ZTE Communication, 17(1):11-16.

[10] Erez Shmueli, T. Z. (2014). Constrained obfuscation of relational databases. Information Sciences, Volume 286, 35.

[11] Gang G., L. Z. (2011). "Internet of things security analysis," in Internet Technology and Applications (iTAP), 2011 International Conference on, 1-4.

[12] Gregor, S. (2006). The Nature of Theory in Information Systems. MIS Quarterly (30:3), 611-642.

[13] Hernandez-Ramos JosAľ L., J. B. (2015). Preserving Smart Objects Privacy through Anonymous. Sensors - Open Access Journal.

[14] Hevner, A. M. (2004). Design Science in Information Systems Research. MIS Quarterly (28:1), 75- 105.

[15] JianQiang Li, J.-J. Y. (2013). A top-down approach for approximate data anonymisation . Enterprise Information Systems, 272.

[16] Junqing Le, X. L. (2016). Full Autonomy: A Novel Individualized Anonymity Model for Privacy Preserving. Computers & Security.

[17] Kocher, P. L. (2004). Security as a new dimension in embedded. In: Proceedings of the 41st Annual Design Automation Conference, DAC 2004, San Diego, CA, USA, June 7-11 (pp. 753-760). New York: ACM.

[18] Liu C., Y. Z. (2012). Research on Dynamical Security Risk Assessment for the Internet of Things inspired by immunology, in Eighth International Conference on Natural Computation (ICNC).

[19] Leusse P, P. P. (2009). Security Cell, a security model for the Internet of Things and Services.International Conference on in Advances in Future Internet, (pp. 47-52).

[20] Loukil F., Ghedira C., Aïcha-Nabila B., Boukadi K., Maamar Z. Privacy-Aware in the IoT Applications: A Systematic Literature Review. International Conference on Cooperative Information Systems (CoopIS) 2017. Proceedings, Part I. Lecture Notes in Computer Science 10573, Springer 2017, ISBN 978-3-319-69461-0, Oct 2017, Rhodes, Greece.

[21] Mingqiang Xue, P. P. (2011). Distributed privacy preserving data collection. In Proceedings of the 16th international conference on Database systems for advanced applications.

[22] Ninghui Li, Tiancheng Li, and Suresh Venkatasubramanian "t-Closeness: Privacy Beyond k-Anonymity and l-Diversity," 2007 IEEE 23rd International Conference on Data Engineering, Istanbul, 2007, pp. 106-115.

[23] Pan Yang, X. G. (2013). A Privacy-Preserving Data Obfuscation Scheme Used in Data Statistics and Data Mining. IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing, (p. 881).

[24] Pierangela Samarati and L. Sweeney. k-anonymity: a model for protecting privacy. Proceedings of the IEEE Symposium on Research in Security and Privacy (S&P). May 1998, Oakland, CA.

[25] Kai Petersen, Robert Feldt, Shahid Mujtaba, and Michael Mattsson. 2008. Systematic mapping studies in software engineering. In Proceedings of the 12th international conference on Evaluation and Assessment in Software Engineering (EASE'08), Giuseppe Visaggio, Maria Teresa Baldassarre, Steve Linkman, and Mark Turner (Eds.). BCS Learning & Development Ltd., Swindon, UK, 68-77.

[26] Philipp Offermann, O. L. (2009). Outline of a design science research process. In Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology (DESRIST '09).

[27] Ricardo Neisse, G. S. (2015). A Model-based Security Toolkit for the Internet of Things.ScienceDirect.

[28] Robert Bredereck, A. N. (2014). The effect of homogeneity on the computational complexity of combinatorial data anonymization. Data Mining and Knowledge Discovery, Volume 28, Number 1, 65.

[29] Samani A., H. H. (2015). Privacy in Internet of Things: A Model and Protection Framework. The 6th International Conference on Ambient Systems, Networks and Technologies (ANT-2015), the 5th International Conference on Sustainable Energy Information Technology (SEIT-2015) (pp. Volume 52, 2015, Pages 606-613). Procedia Computer Science.

[30] Shmatikov, J. B. (2006). Efficient anonymity-preserving data collection. In Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining (KDD '06). ACM, New York, NY, USA, (pp. 76-85).

[31] Syazarin, N., Aziz, N. A., Daud, S. M., & Syarif, S. A. (2017). An Overview on Security Features or Internet of Things (IoT) in Perception Layer. Journal of Engineering and Applied Sciences.

[32] Usha P., R. S. (2014). Sensitive attribute based non-homogeneous anonymization for privacy preserving data mining. International Conference on Information Communication and Embedded Systems (ICICES2014), 1.

[33] Venable, J. (2006). The Role of Theory and Theorising in Design Science Research . First International Conference on Design Science Research in Information Systems and Technology, (pp. 1-18). Claremont, CA: Claremont Graduate University.

[34] Xiao L, H. B. (2010). A knowledgeable security model for distributed health information systems.Computers & Security., (pp. 331-349).

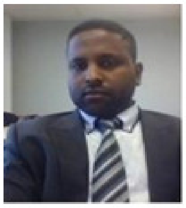
[35] Xin Ma, Q. H. (2010). Study on the Applications of Internet of Things in the Field of Public Safety.China Safety Science Journal, 20(007):170-176.

[36] Yunjung Lee, Y. P. (2015). "Security Threats Analysis and Considerations for Internet of Things". 2015 8th International Conference on Security Technology (SecTech), (pp. vol. 00, no. , pp. 28- 30).

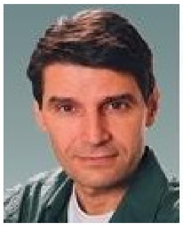
[37] ZhangW., B. Q. (2013). Security Architecture of the Internet of Things Oriented to Perceptual Layer.in International Journal on Computer, Consumer and Control (IJ3C), Volume 2, No.2.

[38] Zhiqiang Yang, S. Z. (2005). Anonymity-preserving data collection. In Proceedings of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining (KDD ’05). ACM, New York, NY, USA, (pp. 334-343).

AUTHORS



Moussa WITTI is a consulting engineer and IT architect in the R&D. He is advising bank and insurance firms in content and data management. He has more than 13 years of IT application development and deployment experience. He has obtained an MBA from Toulouse Business School and master Research in Computer Science from university of Franche-Comté in Besançon (FRANCE).



Dimitri KONSTANTAS is Professor at the University of Geneva (CH) and director of the . He has been active since 1987 in research in the areas of Object Oriented systems, agent technologies, and mobile health systems, with numerous publications in international conferences and journals. His current interests are Mobile Services and Applications with special focus in the well-being services for elderly and information security. Professor D. Konstantas has a long participation in European research and industrial projects and is consultant and expert to several European companies and governments.