The «Quality of Information» Challenges in IoT Forensics: an Introduction

Autoren/Autorinnen: Federico Costantini / Marco Alvise De Stefani / Fausto Galvan
Kategorie: Beiträge
Region: Italien
Rechtsgebiete: Sicherheit und Recht, Internet of Things
Sammlung: Tagungsband IRIS 2019
DOI: 10.38023/e55fdaac-80cf-4952-b2ef-7e93397a63be
Zitiervorschlag: Federico Costantini / Marco Alvise De Stefani / Fausto Galvan, The «Quality of Information» Challenges in IoT Forensics: an Introduction, in: Jusletter IT 21. Februar 2019

IoT technologies pose serious challenges to digital forensics. The acquisition of digital evidence is hindered by the number and extreme variety of IoT items, often lacking of physical interfaces, connected in unprotected networks, feeding data to uncontrolled cloud services. In this paper we introduce the main issues of «information quality» in this field. After a short introduction, we provide an overview on digital forensics approach to preserve the «chain of custody», then we detect relevant IoT features in order to analyse main concerns in digital forensics. At the end, we propose a formula for benchmarking forensics trustworthiness (Information Quality Assessment).

Table of contents

1. Introduction

[1] In the last twenty years, we have witnessed the birth and fast rapid development of a forensic science known as Digital Forensics, which aims to develop a rigorous methodology for the retrieval, collection and analysis of digital evidences.[1] One of the greatest difficulties for experts in this field is to keep up with the speed of technical updates that, as we know, in the digital field is faster than in any other sector. In recent years, indeed, the retrieval and collection of digital data as judicial evidence has been the most challenging issue for Digital Forensics experts, especially due to the pervasive use of two technologies, namely Cloud Computing and AI. On the one hand, the virtualization of resources hinders the validation of the source, the accuracy of the analysis and the integrity of the results, since «*evidence can reside everywhere in the world in a virtualization environment*».[2] On the other, the background of a decision taken by Artificial Intelligence systems lack in transparency, being their behaviour as unpredictable as «black box» outcomes.

[2] Until now, such issues have been addressed improving pre-existing methodologies. «Cloud Forensics» can be defined as «*the application of computer forensics principles and procedures in a cloud computing environment*»,[3] whereas «Explainable Artificial Intelligence» (XAI) aims to

develop a suite of techniques that, bringing more transparency in the reasoning process, allow to validate the reconstruction of external events.[4] Notwithstanding the promising results currently achieved in this way, it is a widespread opinion that «enabling technologies» require radically new approaches.

[3] The same methodological discussion is taking place with Internet of Things (IoT)[5]. The term «Internet of Things», which was originally coined in 1999 with specific reference to RFID technologies[6] and soon overcame more general expressions such as «ubiquitous computing»,[7] «pervasive computing»[8] and «ambient intelligence»,[9] now is commonly used to designate «*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*» according to a definition given by ITU in 2012.[10] The marvel that in the past could be just a vision, now has become everyday life. Today millions of different kinds of devices are connected in an extensive infrastructure, exchanging enormous quantities of data, and it is foreseen that in the future such phenomenon will increase exponentially.

[4] Collecting and analysing digital evidences in IoT scenario poses several challenges, data being spread in an undetermined (e.g. in their type, number and location) set of connected devices.[11] Indeed, machines could present security vulnerabilities, so being exposed to hijackers; data transmission could be unencrypted, allowing «third party manipulations», and storage units could not grant suitable access to archives. In an IoT environment any incident could cause exponential damages and traces of criminal activities could be very difficult to detect.

[5] We claim that one of the key problems in IoT forensics is information quality. While, as a matter of fact, in the IoT environment the amount of sources of data and the trustworthiness of information obtained are inversely proportional, each step of all the processes concerning digital evidences has be validated in order to be discussed in courts among parties and judges. The fact is that, when it comes to jurisdiction, quantity cannot be opposed to quality, but they need to be harmonised.

[6] In this paper we focus on three aspects of such issue: firstly, we provide a preliminary explanation on the concept of information quality, since «data» and «information» are quantitative concepts; secondly, we offer a short analysis of the practical concerns that can be considered as expression of the theoretical issues emerged in the previous part; after that, we express some methodological observations that can be useful to build a theoretical model that can be represented in a formula. At the end, we express our final evaluations and draw paths for future research.

2. Theoretical background of «information quality» in IoT forensics

[7] The distinction between «data quality» and «information quality» is very debated.[12] The first concept – in accordance with ISO 8000-1 definition[13] – is commonly stated as a measure of the fitness for the intended use of such data,[14] while the second represents a broader range of features, also encompassing the context of the observation.[15] In light of such discussion, we prefer to use the approach concerning «information quality» for three main reasons: (1) the extreme complexity of IoT environments, as described above, in which data are just a part of a complex environment, along with devices and processes; (2) the possibility to take into

consideration both data and metadata; (3) the possibility to include our contribution in a wider theoretical perspective better known as «Philosophy of Information». [16]

[8] According to such approach, «information» has three ontological statuses, identified since the seminal studies of Weaver: [17] «information *as* reality», for example the electrical signal, which is transmitted regardless of the message contained; «information *about* reality», such as the information about natural phenomena, which can be true or false (hence, in philosophical terms, can be said «alethic»); [18] «information *for* reality», which conveys instructions or algorithms to one or many recipients. Each of them has to be considered separately.

[9] Consequently, «information quality» can be studied under three different views.

- Quality in «information as reality» is the most common and emerges, for example, in the traditional problem of reducing noise, distortion or losses in signal transmission theory. In this sense, it measures the affordability of the means implemented to transfer information.
- Quality in «information about reality» is concerned when information is dissimilar to the facts to which it refers. This concept is related to the meaning of information, or «semantics» [19]. Thus, here quality measures the reliability of the information provided in representing the related events.
- Quality in «information for reality» has to be faced when processes present inconsistencies, loopholes or conflicts. This concept involves further processes of information, for example when it is shared with others. Hence, in this respect it measures the trustworthiness of the agent who receives information or, generally, of those involved in further processes.

[10] In digital forensics, the problem of «information quality» has received special consideration under different perspectives. Here we can deploy the same tripartite analytical model to draw a comprehensive framework.

- The first kind of quality is important, in order to preserve authenticity of the collected information, experts developed the concept of «chain of custody» and achieved a broad consensus on «best practices» which have been codified in technological standards. [20]
- The second type of quality is concerned when the trustworthiness in the representation of the events has to be verified with other sources of evidences. [21]
- The third sort of quality is involved in the discussion on the evidences among parties (inquiring authorities, defendants, judges, forensics experts). Here, external variables also can make the difference, such as personal competences of the agents involved, «soft skills» (argumentation skills, trial strategies), cost of analytical tools, available time.

[11] From a theoretical perspective, since in IoT devices are constantly sharing information with each other, «quality of information» is a much complex issue. Indeed, it has to be considered not as a property of a single device, but as a feature of the whole ecosystem in which it is immersed. Specific concerns emerge in each considered aspect.

- «Quality of information *as* reality»: it is difficult to isolate a single device or crystalize a specific piece of information. The boundaries of relevance are blurred. This aspect is, not without a reason, widely discussed by experts. [22]
- «Quality of information *about* reality»: it is problematic to detect a specific source, to trace the chain of interactions, to measure the influence of a single item in shaping the

representation of the event occurred. It is commonly true that «correlation is not causation», however IoT is, above all, a matter of correlation. Here is IoT is where «quality of information» really faces uncertainty.[23]

- «Quality of information *for* reality»: this is the most difficult aspect of IoT forensics. Under this perspective, the «human factor» plays its part besides the technological variables, as shown in digital forensics.

The observation above outlined can be represented in the following table:

Ontological statuses of Information	**«Quality of Information» level of analysis**	**«Quality of Information» in digital forensics**	**«Quality of Information» in IoT forensics**
Information *as* reality	Traditional theory of communication	«chain of custody»	Relevance
Information *about* reality	Consistence with represented facts	External validation with other sources of evidence	Uncertainty
Information *for* reality	Logical coherence	Effectiveness	«Human factor»

Table 1: «Quality of information» tripartite analysis and IoT issues

3. Practical issues in IoT forensics

[12] After having provided a short definition of «quality of information», we intend to underline that the main feature of an IoT network, while performing the given tasks, is the possibility, when necessary, to take advantage exchanging information with other neighbouring elements, regardless the fact that they could belong to different IoT ecosystem, possibly set up for a different purpose. Over the years it became clear that, while it was originally conceived as a sunrise of new opportunities for increasing the efficiency of services – thus to benefit private users and industries - this technology generates a «virtual environment» which contains a huge amount of information which, if needed, can be used as a source of evidence in a forensic scenario. In the following part, we observe that the main task of IoT Forensics, namely the collection of the evidence, is challenging for different causes.

[13] First, the extreme variety of IoT items, with proprietary or undocumented protocols, often without physical interfaces, hinders the direct extraction of evidence from devices.

[14] Second, IoT devices ceaselessly send information to «their own» cloud service providers. So, obtaining evidences from cloud service implicates other challenges: technical ones (cloud forensics) and legal ones (interact with foreign companies in different legal frameworks).

[15] Third, evidences could be manipulated by cloud service providers. Indeed, raw data fed by IoT devices are analysed, parsed and stored in databases and server, yet adding more layers of interpretations and classifications. Those processes can aggregate data, but also deteriorate

them, thus weaken the quality of the acquired information.

[16] In order to explain such issues, we provide an example: let us assume that we need to acquire the complete geolocalization history of a specific account from a cloud service provider (i.e. Google Timeline History[24]).

[17] Let's suppose that we have the account's credentials (i.e. username and password): we could use a forensic software (i.e. Oxygen Forensic® Cloud Extractor) to acquire the geolocalization history[25]. After the acquisition we could explore and analyse the collected data: we would likely find a very clear and detailed set of information, spanning years and neatly organized. The typical forensic software user interface for this type of data consist of a world map we can freely zoom and search, a time filter and coloured pins and lines that represents geolocalization info and probable movements.

[18] This great source of info can lead us to assume that the quality of those data is very high, but after an additional analysis we should find out that actually we don't know where information come from. We know that these cloud service provider acquire geolocalization data from a great range of source related to that specific account: smartphone's GPS; EXIF data of images; cellular network radio tower; WiFi known geolocalization; NFC; fitness apps; Uber rides; IP geolocalization; fitbands; smartwatches; navigation apps; reviews of shops or restaurants; public transportation tickets; and many other IoT sources. The timeline can even be manipulated by the user through the cloud service web interface (i.e. in Google Timeline we can easily add a new geolocalization or change or deleted an old record).

[19] If we focus to a specific day we only have the alleged geolocalization history: some points (consisting in longitude, latitude and timestamp) and lines that connect those points to speculate movements, but we are not able to discover where each point comes from. Even if in some metatag there is an information about the source of the info, we can access only the parsed data: we don't know if the source is reliable or if the data has been manipulated, compromised or not properly interpreted. The original data can't even be accessible (i.e. If the geolocalization comes from a fitband's GPS, probably we can't physically connect to the device; we can acquire the paired smartphone and analyse the Fitband's app's databases, but even that isn't the original data…).

4. Theoretical model

[20] The evaluation of the «Information Quality» in a set of data is not generally a trivial task, as emerged in the previous sections. The various steps of the assessment always hang on different factors, many of whom sometimes cannot be precisely verified, but only estimated, without forgetting the «noise» coming with the data flow, which must be carefully identified and removed. In addition to these basic difficulties, in common for every environment, the quality of information needed in a forensics scenario must undergone to a further filter, represented by the «check for the admissibility», which allows the acquired data to be a part of a trial procedure.

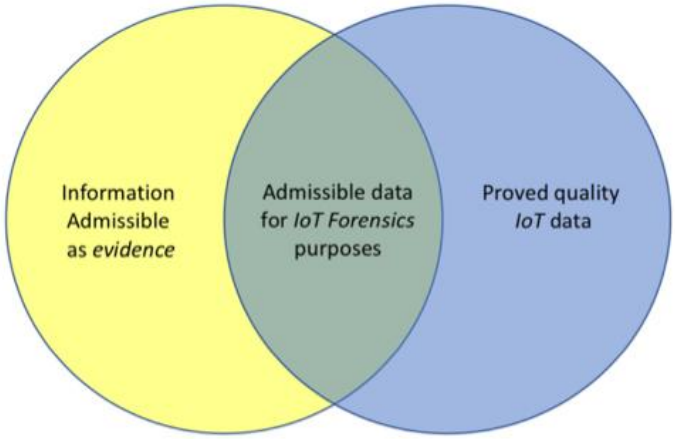

Fig.1 The first approach in the Information Quality assessment for Forensics IoT purposes. [26]

[21] A first approach for this issue could be based upon the verification of «quality of information» in two different fields, as exposed in Figure 1. Information which will be proved to be, at the same time, admissible as an evidence in a trial (as it has been properly acquired and stored) and reliable as a collection of data, will serve as an input for the forensics analysis. In our opinion, this method is affected by two main risks: wasting time with one of the two controls when the outcome of the other is negative, and rejecting key evidences which, for some reason, are not proven to be reliable as high quality IoT data (e.g. a noisy image which, considered together with other evidences, could have an important meaning). For the above explained reasons, we prefer to adopt another approach, where the two aspects of the extracted information (as rough data, and as forensic evidence) are spread all over the addends of a «sum of proper features».

In order to support such method, and to express the result of trustworthiness of a set of *n* IoT devices that have to be acquired as digital evidences, we formalize how the above mentioned factors must be taken into consideration, introducing a percentage coefficient that we named IQA (Information Quality Assessment) as follows:

$$IQA = \frac{\sum_{i=1}^{n}(DCT_i + DST_i + CS_i + PC_i + OT_i + OS_i)}{6n} \times 100. \qquad (1)$$

Where:
i = i-th device
DTC = device technical status
DST = device security status (Confidentiality, Integrity, Availability, …)
CS = cloud service security status
PC = privacy (GDPR) compliance
OT = observer technological advancement
OS = observer skills
(allowed values: all decimal between 0 = bad and 1 = good)

[22] Giving an interpretation of (1) it's straightforward, if we observe that a device scoring «1» to every component of the sum implies a 100% of Information Quality. This percentage must be averaged with the one scored by other components of the set, if any.

[23] We underline that, also because IoT Forensics is one of the newer subareas of Digital Forensics,[27] very few studies have been carried out with the specific aim of modelling a theoretical approach[28] and, of course, a lot of work has still to be done to refine and improve the above formula. Possible criticisms of this approach may be:

[24] 1) It may not be possible to define each item for all types of IoT devices. E.g. the term C.S implies that the device is always connected to its environment, but it can be used also «offline»;

[25] 2) The information needed to define these terms may not be accessible. This would be possible not only technically, but because of restrictions imposed by the companies that own them. For example, let's think about an investigation in Italy that requires data related to a journey of a Chinese car, stored in a server in that country.

5. Conclusions

[26] As «information» has many meanings, «quality of information» has many facets. Furthermore, in the process of building knowledge, complexity and uncertainty must always be taken into account. Technological innovation, such as human nature, are inevitable factors with unpredictable effects.

[27] It has to be remarked that «quality of information» is crucial in Digital Forensics. Civil and criminal proceedings can be diverted from their fair conclusions by mistakes or misinterpretations of several actors: judges, defendants, prosecutors, police officers, consultants, witnesses. In this, digital evidence becomes more and more important not only because it is increasingly widespread, but also because of the ever-increasing skills required to face it.

[28] Of the many challenges currently faced by Digital Forensics, IoT technologies bring the more concerning not only for practical causes, but also for theoretical reasons.

[29] From a theoretical perspective, many questions need to be deepened. Aside the discussion between «data quality» and «information quality» approaches, it should be considered how «quality of information» evolves in different levels of «complexity» (human to human, human to machine, machine to machine). From this perspective, «information quality» could be considered an ethical value to pursue in the design of IoT devices and ecosystems.

[30] From a practical perspective, we need to understand which type of data we can collect and how it's been manipulated. From this perspective, «information quality» could be considered a kind of metadata: information about information. In a nutshell, in order to analyse IoT evidences, it is required not only information itself, but also the «information history», from the original source to the repository that we are collecting.

[31] Based upon the above considerations, we analysed two model to address the issue of Information Quality Assessment in IoT Forensics. The first takes separately into account the two faces of the extracted information, namely as a rough set of data that has to be proved as thrustable, and as a possible evidence which has to be admitted in a court. We then exposed some reasons why this model had to be discarded, and proposed a second one, this time with a proper formula, where every component represent a different aspect of the IoT data which could have to be analysed. Its novelty certainly will lead to the possibility of suggestions for (even radical) corrections and improvements.

[32] In the future we intend to deepen the implementation of such model of assessment, possibly with on-the-field testing. As an example, for every IoT must be possible defining the first four terms of the formula, since the last two only depends upon the observer.

6. References

AARTS, EMILE H. L./ ENCARNAÇÃO, JOSÉ LUIS (Eds.), True visions: the emergence of ambient intelligence, Springer, Berlin, 2006.

ADADI, AMINA/ BERRADA, MOHAMMED, Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI), IEEE Access, volume 6, 2018, p. 52138-52160.

ASHTON, KEVIN, That «Internet of Things» Thing, RFID Journal, 2009. https://www.rfidjournal.com/articles/view?4986 (accessed 7 January 2019).

BABAR, SACHIN/MAHALLE, PARIKSHIT/STANGO, ANTONIETTA/PRASAD, NEELI/PRASAD, RAMJEE, Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT). In: Meghanathan Natarajan, Boumerdassi Selma, Chaki Nabendu, Nagamalai Dhinaharan (Eds.), Recent Trends in Network Security and Applications Springer, Berlin, Heidelberg, 2010, p. 420-429.

BAR-HILLEL, YEHOSHUA/ CARNAP, RUDOLF, Semantic Information, The British Journal for the Philosophy of Science, volume 4, issue 14, 1953, p. 147-157.

BATINI, CARLO/CAPPIELLO, CINZIA/FRANCALANCI, CHIARA/MAURINO, ANDREA, Methodologies for data quality assessment and improvement, ACM Computing Surveys, volume 41, issue 3, 2009, p. 1-52.

BENI, MAJID DAVOODY, Syntactical Informational Structural Realism, Minds and Machines, volume 28, issue 4, 2018, p. 623-643.

BORGMANN, ALBERT, Holding on to reality. The nature of information at the turn of the millennium, University of Chicago Press, Chicago, 1999.

CHEN, DONG/CHANG, GUIRAN/SUN, DAWEI/LI, JIAJIA/JIA, JIE/WANG, XINGWEI, TRM-IoT: A trust management model based on fuzzy reputation for internet of things, Computer Science and Information Systems, volume 8, issue 4, 2011, p. 1207-1228.

CONTI, MAURO/DEHGHANTANHA, ALI/FRANKE, KATRIN/WATSON, STEVE, Internet of Things security and forensics: Challenges and opportunities, Future Generation Computer Systems, volume 78, 2018, p. 544-546.

DELONE, WILLIAM H./ MCLEAN, EPHRAIM R., Information Systems Success: The Quest for the Dependent Variable, Information Systems Research, volume 3, issue 1, 1992, p. 60-95.

DELONE, WILLIAM H./ MCLEAN, EPHRAIM R., The DeLone and McLean Model of Information Systems Success: A Ten-Year Update, Journal of Management Information Systems, volume 19, issue 4, 2003, p. 9-30.

DRETSKE, FRED I., Knowledge & the flow of information, MIT Press, Cambridge (Mass.), 1981.

FLORIDI, LUCIANO (Ed.), The Onlife Manifesto. Being Human in a Hyperconnected Era, Open Access Springer International Publishing, Cham 2015.

FLORIDI, LUCIANO, The Philosophy of Information, Oxford University Press, Oxford, 2013.

FLORIDI, LUCIANO/ ILLARI, PHYLLIS, The philosophy of Information quality, Synthese library, 358, Springer, Berlin, 2014.

FRIEDEWALD, MICHAEL/ RAABE, OLIVER, Ubiquitous computing: An overview of technology impacts, Telematics and Informatics, volume 28, issue 2, 2011, p. 55-65.

GIACOBBE, MAURIZIO/DI PIETRO, RICCARDO/LONGO MINNOLO, ANTONINO/PULIAFITO, ANTONIO, Evaluating Information Quality in Delivering IoT-as-a-Service, 2018 IEEE International Conference on Smart Computing (SMARTCOMP), 2018, p. 405-410.

HANSMANN, UWE, Pervasive computing handbook, Springer, Berlin-New York, 2001.

HEGARTY, ROBERT/LAMB, DAVID J./ATTWOOD, ANDREW, Digital Evidence Challenges in the Internet of Things, Proceedings of the Tenth International Network Conference (INC) 2014 School of Computing & Mathematics Plymouth University, Plymouth, 2014, p. 163-172.

HÖLLER, JAN/TSIATSIS, VLASIOS/MULLIGAN, CATHERINE/KARNOUSKOS, STAMATIS/AVESAND, STEFAN/BOYLE, DAVID, From machine-to-machine to the internet of things: introduction to a new age of intelligence, Academic Press, Amsterdam, 2014.

HOSSAIN, M./KARIM, Y./HASAN, R., FIF-IoT: A Forensic Investigation Framework for IoT Using a Public Digital Ledger, 2018 IEEE International Congress on Internet of Things (ICIOT) IEEE, 2018, p. 33-40.

ITU, Recommendation ITU-T Y.2060 Overview of the Internet of things, 2012.

LUNDGREN, BJÖRN, Does semantic information need to be truthful?, Synthese, 2017.

MAGRUK, ANDRZEJ, The Most Important Aspects of Uncertainty in the Internet of Things Field – Context of Smart Buildings, Procedia Engineering, volume 122, 2015, p. 220-227.

MEFFERT, CHRISTOPHER/CLARK, DEVON/BAGGILI, IBRAHIM/BREITINGER, FRANK, Forensic State Acquisition from Internet of Things (FSAIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition, Proceedings of the 12th International Conference on Availability, Reliability and Security ACM, Reggio Calabria, Italy, 2017, p. 1-11.

MICIC, NATASHA/NEAGU, DANIEL/CAMPEAN, FELICIAN/ZADEH, ESMAEIL HABIB, Towards a Data Quality Framework for Heterogeneous Data, 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017, p. 155-162.

PALMER, GARY, A Road Map for Digital Forensic Research. Report From the First Digital Forensic Research Workshop (DFRWS), New York, 2001.

POVAR, DIGAMBAR/ GEETHAKUMARI, G., A Heuristic Model for Performing Digital Forensics in Cloud Computing Environment. In: Mauri JaimeLloret, Thampi SabuM, Rawat DandaB, Jin Di (Eds.), Security in Computing and Communications, Communications in Computer and Information Science Springer Berlin Heidelberg, 2014, p. 341-352.

SHAMALA, PALANIAPPAN/AHMAD, RABIAH/ZOLAIT, ALI/SEDEK, MULIATI, Integrating information quality dimensions into information security risk management (ISRM), Journal of Information Security and Applications, volume 36, 2017, p. 1-10.

SIMOU, STAVROS/KALLONIATIS, CHRISTOS/KAVAKLI, EVANGELIA/GRITZALIS, STEFANOS, Cloud Forensics: Identifying the Major Issues and Challenges. In: Jarke Matthias, Mylopoulos John, Quix Christoph, Rolland Colette, Manolopoulos Yannis, Mouratidis Haralambos, Horkoff Jennifer (Eds.), Advanced Information Systems Engineering, Lecture Notes in Computer Science Springer International Publishing, 2014, p. 271-284.

WEAVER, WARREN, The Matemathics of Communication, Scientific American, volume 181, issue 1, 1949, p. 11-15.

WEISER, MARK, The computer for the 21st century, SIGMOBILE Mob. Comput. Commun. Rev., volume 3, issue 3, 1999, p. 3-11.

WILLS, GARY B./ALENEZI, AHMED/ZULKIPLI, NIK/HUDA, NURUL, IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things, Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security Scitepress, 2017, p. 315-324.

WOODALL, PHILIP/BOREK, ALEXANDER/PARLIKAD, AJITH KUMAR, Data quality assessment: The

Hybrid Approach, Information & Management, volume 50, issue 7, 2013, p. 369-382.

YAQOOB, IBRAR/HASHEM, IBRAHIM ABAKER TARGIO/AHMED, ARIF/KAZMI, S. M. AHSAN/HONG, CHOONG SEON, Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges, Future Generation Computer Systems, volume 92, 2019, p. 265-275.

ZAREEN, MUHAMMAD SHARJEEL/WAQAR, ADEELA/ASLAM, BABER, Digital Forensics: Latest Challenges and Response, 2013 2nd National Conference on Information Assurance (NCIA) IEEE, Piscataway, NJ, 2013, p. 21-29.

ZAWOAD, S./ HASAN, R., FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things, 2015 IEEE International Conference on Services Computing IEEE, 2015, p. 279-284.

---

1 Digital Forensics has been defined «*the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations*» PALMER, A Road Map for Digital Forensic Research. Report From the First Digital Forensic Research Workshop (DFRWS), New York, 2001, (p. 23).

2 SIMOU/KALLONIATIS/KAVAKLI/GRITZALIS, Cloud Forensics: Identifying the Major Issues and Challenges. In: Jarke, M./Mylopoulos, J./Quix, C./Rolland, C./Manolopoulos, Y./Mouratidis, H. and Horkoff, J. (Eds.), Advanced Information Systems Engineering, Lecture Notes in Computer Science Springer International Publishing, 2014, p. 271-284 (p. 273).

3 POVAR/GEETHAKUMARI, A Heuristic Model for Performing Digital Forensics in Cloud Computing Environment. In: Mauri, J./Thampi, S./Rawat, D. and Jin, D. (Eds.), Security in Computing and Communications, Communications in Computer and Information Science Springer Berlin Heidelberg, 2014, p. 341-352 (p. 344).

4 ADADI/BERRADA, Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI), IEEE Access, volume 6, 2018, p. 52138-52160.

5 HEGARTY/LAMB/ATTWOOD, Digital Evidence Challenges in the Internet of Things. Proceedings of the Tenth International Network Conference (INC) 2014 School of Computing & Mathematics Plymouth University, Plymouth, 2014, p. 163-172, HOSSAIN/KARIM/HASAN, FIF-IoT: A Forensic Investigation Framework for IoT Using a Public Digital Ledger. 2018 IEEE International Congress on Internet of Things (ICIOT) IEEE, 2018, p. 33-40, ZAWOAD/HASAN, FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things. 2015 IEEE International Conference on Services Computing IEEE, 2015, p. 279-284, MEFFERT/CLARK/BAGGILI/BREITINGER, Forensic State Acquisition from Internet of Things (FSAIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition. Proceedings of the 12th International Conference on Availability, Reliability and Security ACM, Reggio Calabria, Italy, 2017, p. 1-11.

6 ASHTON, That «Internet of Things» Thing, RFID Journal, 2009.

7 WEISER, The computer for the 21st century, SIGMOBILE Mob. Comput. Commun. Rev., volume 3, issue 3, 1999, p. 3-11.

8 HANSMANN, Pervasive computing handbook, Springer, Berlin; New York, 2001.

9 AARTS/ENCARNAÇÃO (Eds.), True visions: the emergence of ambient intelligence Springer, Berlin, 2006.

10 ITU, Recommendation ITU-T Y.2060 Overview of the Internet of things, 2012, FRIEDEWALD/RAABE, Ubiquitous computing: An overview of technology impacts, Telematics and Informatics, volume 28, issue 2, 2011, p. 55-65.

11 ZAREEN/WAQAR/ASLAM, Digital Forensics: Latest Challenges and Response. 2013 2nd National Conference on Information Assurance (NCIA) IEEE, Piscataway, NJ, 2013, p. 21-29.

12 For the sake of brevity, here we cannot deepen the concept of «quality». However, it can be said that such term is used in different disciplines (from business to philosophy) to compare a given object, often

an empirical one, with a set of requirements. The term of comparison can be a technical standard, such as an ISO certification, or theoretical model, such as a set of abstract or «ethical» values.

13 https://www.iso.org/standard/50798.html.

14 DELONE/MCLEAN, Information Systems Success: The Quest for the Dependent Variable, Information Systems Research, volume 3, issue 1, 1992, p. 60-95, DELONE/MCLEAN, The DeLone and McLean Model of Information Systems Success: A Ten-Year Update, Journal of Management Information Systems, volume 19, issue 4, 2003, p. 9-30, BATINI/CAPPIELLO/FRANCALANCI/MAURINO, Methodologies for data quality assessment and improvement, ACM Computing Surveys, volume 41, issue 3, 2009, p. 1-52, WOODALL/BOREK/PARLIKAD, Data quality assessment: The Hybrid Approach, Information & Management, volume 50, issue 7, 2013, p. 369-382.

15 SHAMALA/AHMAD/ZOLAIT/SEDEK, Integrating information quality dimensions into information security risk management (ISRM), Journal of Information Security and Applications, volume 36, 2017, p. 1-10, GIACOBBE/DI PIETRO/LONGO MINNOLO/PULIAFITO, Evaluating Information Quality in Delivering IoT-as-a-Service. 2018 IEEE International Conference on Smart Computing (SMARTCOMP), 2018, p. 405-410.

16 FLORIDI (Ed.), The Onlife Manifesto. Being Human in a Hyperconnected Era, Open Access Springer International Publishing, Cham, 2015, FLORIDI, The Philosophy of Information, Oxford University Press, Oxford, 2013.

17 In the original exposition of Theory of Communication such concepts were expressed as different «levels», respectively as «technical», «semantic» and «influential» WEAVER, The Matemathics of Communication, Scientific American, volume 181, issue 1, 1949, p. 11-15, (p. 11). Instead, cybernetics defined «technological», «natural» and «cultural» information. BORGMANN, Holding on to reality. The nature of information at the turn of the millennium, University of Chicago Press, Chicago, 1999.

18 LUNDGREN, Does semantic information need to be truthful?, Synthese, 2017, DRETSKE, Knowledge & the flow of information, MIT Press, Cambridge, Mass., 1981.

19 BENI, Syntactical Informational Structural Realism, Minds and Machines, volume 28, issue 4, 2018, p. 623-643, BAR-HILLEL/CARNAP, Semantic Information, The British Journal for the Philosophy of Science, volume 4, issue 14, 1953, p. 147-157.

20 International Standards published by the International Organization for Standardization (ISO), i.e. ISO/IEC 27037:2012 — Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence; ISO/IEC 27041:2015 — Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative methods; ISO/IEC 27042:2015 — Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence; ISO/IEC 27050 — Information technology — Security techniques — Electronic discovery — Part 1 (2016): Overview and concepts and Part 3 (2017): Code of practice for electronic discovery.

21 FLORIDI/ILLARI, The philosophy of Information quality, Synthese library, 358, Springer, Berlin-Heidelberg, 2014.

22 WILLS/ALENEZI/ZULKIPLI/HUDA, IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things. Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security Scitepress, 2017, p. 315-324, CONTI/DEHGHANTANHA/FRANKE/WATSON, Internet of Things security and forensics: Challenges and opportunities, Future Generation Computer Systems, volume 78, 2018, p. 544-546.

23 Few authors have talked suck issue, see MAGRUK, The Most Important Aspects of Uncertainty in the Internet of Things Field – Context of Smart Buildings, Procedia Engineering, volume 122, 2015, p. 220-227.

24 https://www.google.com/maps/timeline.

25 We presume that the forensic software is compliant with all Digital Forensics procedures and standard.

26 It has to be taken into account, in two separate evaluation pipelines, both the quality of the data (i.e. low noise, reliable source, etc) and its admissibility as evidence in court (i.e. acquired according to the Best Practices). Data which pass through this double filter are suitable to be used in the forensics analysis. Although feasible in theory, its practical application can leads to some undesirable drawbacks: unnecessary loss of time and discarding important evidences.

27 YAQOOB/HASHEM/AHMED/KAZMI/HONG, Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges, Future Generation Computer Systems, volume 92, 2019, p.

265-275, HÖLLER/TSIATSIS/MULLIGAN/KARNOUSKOS/AVESAND/BOYLE, From machine-to-machine to the internet of things: introduction to a new age of intelligence, Academic Press, Amsterdam, 2014.

28 MICIC/NEAGU/CAMPEAN/ZADEH, Towards a Data Quality Framework for Heterogeneous Data. 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017, p. 155-162, CHEN/CHANG/SUN/LI/JIA/WANG, TRM-IoT: A trust management model based on fuzzy reputation for internet of things, Computer Science and Information Systems, volume 8, issue 4, 2011, p. 1207-1228, BABAR/MAHALLE/STANGO/PRASAD/PRASAD, Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT). In: Meghanathan, N./Boumerdassi, S./Chaki, N. and Nagamalai, D. (Eds.), Recent Trends in Network Security and Applications Springer, Berlin, Heidelberg, 2010, p. 420-429.

0 Kommentare

Es gibt noch keine Kommentare

** Pflichtfelder*

Was ist Ihr Kommentar?

Titel:

Ihr Kommentar: *

Name: *

Federico Costantini

Senden

Ihr Kommentar wird durch eine Moderatorin bzw. einen Moderator geprüft und in Kürze freigeschaltet.

Source details

usletter IT

copus coverage years: from 2017 to 2019

ublisher: Weblaw AG

E-ISSN: 1664-848X

ubject area: Social Sciences: Law | Computer Science: Computer Science (miscellaneous)

View all documents > | Save to source list | Journal Homepage

CiteScore 2019
0.1

SJR 2019
0.121

SNIP 2019
0.071

iteScore | CiteScore rank & trend | Scopus content coverage

¡ Improved CiteScore methodology

CiteScore 2019 counts the citations received in 2016-2019 to articles, reviews, conference papers, book chapters and data papers published in 2016-2019, and divides this by the number of publications published in 2016-2019. Learn more >

CiteScore 2019

$$0.1 = \frac{18 \text{ Citations 2016 - 2019}}{356 \text{ Documents 2016 - 2019}}$$

Calculated on 06 May, 2020

CiteScoreTracker 2020

$$0.1 = \frac{19 \text{ Citations to date}}{356 \text{ Documents to date}}$$

Last updated on 10 June, 2020 • Updated monthly

iteScore rank 2019

ategory	Rank	Percentile
ocial Sciences – Law	#632/685	7th
omputer Science – Computer Science (miscellaneous)	#63/64	2nd

iew CiteScore methodology > | CiteScore FAQ > | Add CiteScore to your site

About Scopus

What is Scopus
Content coverage
Scopus blog
Scopus API
Privacy matters

Language

日本語に切り替える
切换到简体中文
切換到繁體中文
Русский язык

Customer Service

Help
Contact us

ELSEVIER

Terms and conditions ↗ Privacy policy ↗

Copyright © Elsevier B.V ↗. All rights reserved. Scopus® is a registered trademark of Elsevier B.V.

We use cookies to help provide and enhance our service and tailor content. By continuing, you agree to the use of cookies.

RELX