ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 11, May 2016

International Conference on Innovations in Engineering and Technology (ICIET'16)

6th & 7th April 2016

Organized by

K.L.N. College of Engineering and Technology, Madurai, Tamil Nadu, India

# An Inclusive Methodology to Privacy in the Cloud-based Internet of Things: A Study

Padmaja. Pulicherla

Associate Professor, Dept. of CSE, Malineni Lakshmaiah Engineering College, Ongole, A.P, India

**ABSTRACT**: Internet of Things devices are intended to infiltrate fundamentally all aspects of life, including homes and urban spaces, in use cases such as health care, assisted living, and smart cities. One often suggested solution for dealing with the huge amount of data collected by these devices and contribution services on top of them is the federation of the Internet of Things and cloud computing.To address this vital issue and for this reason, recognise the cloud-primarily based Internet ofThings for aimplication of different utility areas, we present comprehensive approach to privacy in this anticipated setting. We permit an individual user to enforce all her privacy requirements earlier than any sensitive data is uploaded to the cloud, permit designers of cloud services to combine privacy capability already into the improved method of cloud services, and offer users an obvious and adaptable interface for configuring their privacy requirements.

**KEYWORDS:** Privacy, Cloud Computing, Internet of Things, Model-drivenDevelopment, User Acceptance

## I.INTRODUCTION

The Internet of Things (IoT) is the imaginative and prescient of interconnecting a very large amount of smart things (IoTgadgets), making its way into nearly all factors of everydayexistence. Typical examples for the estimated deployment ofIoT structures for end-customers consist of, however, aren't restricted to,pervasive fitness care assisted residing, and smart cities [1],[2]. IoT devices are frequently restrained in their computationaland storage resources and are probably powered by using a battery.Additionally, they may be mobile or lose connectivityand therefore cannot be assumed to be continually available. Toovercome these constraints, it seems herbal to leverage theelastic and constantly available resources of the cloud [3]–[7].Cloud solutions simplify storage and processing of accrueddata, usage of equal information inside several offerings, in addition tocombining information from several customers and assisting consumer mobilitywithout data fragmentation over several databases.While important sensors and cloud solutions already existnowadays, consumer popularity of the sort of comprehensive solutionstays an important thing [2], [8]–[10]. Especially, a consumer'sprivateness can be the situation to a wide range of threats, notablyfor an extensively deployed gadget. Hence, it's miles vital to make certainusers' datacontrol – optionally being able to feed, e.g., inside thecontext of pervasive healthcare, health higher than privatenessin an emergency. This is simplest viable through anchoring privatenesscomponents in the system itself, orientated at customers' demands.

However, cloud services are typically not developed solely for one specificuser but instead target a large group of heterogeneous customers [13]. Hence,it is infeasible to decide on all privacy aspects already during the developmentof a cloud service as privacy by design might suggest. Instead, in order for usersto accept such a service, privacy choices must be left to the user. This, however,significantly increases the complexity of designing and developing cloud servicesand at the same time puts a tremendous burden on the user who often hasno awareness of the (technical) consequences of her privacy choices. Therefore,we strive to encompass domains, end-users as well as service provider'sperspective with our comprehensive understanding of cloud-based IoT services.In this paper, we present UPECSI, our solution for User-driven PrivacyEnforcement for Cloud-based Services in the IoT. UPECSI takes a comprehensive approach to privacy for the cloud-based IoT by providing an integratedsolution for privacy enforcement that focuses on individual end-users and developers of cloud services at the same time. UPECSI consists of several technicalcomponents and organizational processes. More specifically, with UPECSI, wepresent the following core contributions: i) individual, user-driven enforcement of privacy requirements already before any potentially sensitive data ishanded over to the cloud, ii) a novel technique for designing and implementingcloud-based services that

integrate privacy functionality into the developmentprocess, and iii) an easy to understand, flexible, and transparent approach forusers of different privacy expertise to configure their individual privacy settings. These contributions of our comprehensive approach to privacy in thecloud-based IoT allow us to lay the foundation for bringing the IoT and cloudcomputing together in a user-accepted fashion.

## II.LITERATURE SURVEY

Securely outsourcing data, which is collected by smalldevices, to the cloud has already been proposed by relatedwork. For example, Lounis et al. [17] provide a secure cloudbased solution for health care data, while the SensorCloudproject [3]–[5], [7], [18], [19] aims at providing a secureinfrastructure for realizing services which operate on allkinds of sensor data. Although these approaches focuson security aspects, they do not address privacy concernsbeyond providing confidentiality and access control.In domains, IoT and cloud computing, solutions forpreserving privacy have been proposed. Examples for theIoT domain include the privacy-preserving computation ofstatistical values on health care data [20] and a context-awaresystem for assisted living and residential monitoring [21]. Toensure privacy in cloud computing, solutions ranging fromannotating data with fine-grained privacy obligations [10]to using tamper-proof hardware components for realizingprivacy-aware data storage and processing [22] have beenproposed. Although these approaches present techniques forpreserving privacy in the IoT and the cloud, we are notaware of a comprehensive approach for providing privacy inthe combination of the two to support users and developersin using or, resp., designing services in a privacy-aware way.

A large number of approaches aim at securing health data when it is outsourced to the cloud. One of the first approaches in this direction was proposedby Lounis et al. [36]. In their work, they particularly focus on guaranteeing confidentiality and integrity of outsourced medical data with minimum managementand processing overheads. Thilakanathan et al. [37] proposed a platform thatrealizes mobile telecare by allowing doctors to remotely monitor patients. Forthis, they rely on the cloud as a central data storage which requires them totake special care of security, confidentiality, and access revocation. In a similar context, Li et al. [38] and Liu et al. [21] proposed approaches for realizingthe scalable and secure sharing of personal health records (PHRs) using thecloud. In order to secure the health records in this setting, they make use ofattribute-based encryption respectively signcryption.

## III.APPROACHES

**Network Scenario**: Based on our application areas, we derived the following network scenario forrealizing cloud-based services for the IoT which is depicted in Figure 1. As wefocus on the privacy aspects of the integration of the IoT with cloud computing,our network scenario follows a user-centric view. Each user (U) of our systemowns and thus operates one or more IoT devices (D), often also referred toas smart objects. Following the definition of Gubbi et al. [17], we considerIoT devices that sense information from the environment, interact with thephysical world, and most importantly allow communication using traditionalInternet standards. Typical examples for IoT devices in our application areasrange from sensitive floors for movement monitor and fall detection in homeenvironments and smart textiles (e.g., shirts, wristbands, or shoes) monitoringvarious vital parameters and connected to emergency notification systems toadvanced devices capable of monitoring specialized implants, such as artificialcardiac pacemakers (ACP).

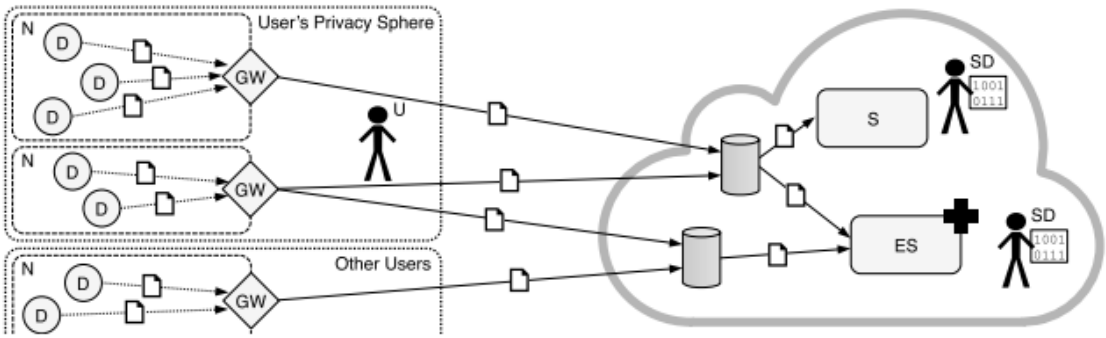


Figure 1: An individual user (U) operates one or more IoT networks (N). The IoT devices(D) in these networks send data to the cloud via a gateway (GW). The cloud stores data indifferent databases and provides it to services (S), as well as emergency services (ES), whichare provided by service developers (SD) and were authorized to access data by the user.

**Privacy Concerns of End-users:** The data collected by IoT devices often consists of sensitive informationthat unauthorized third parties might be interested in [2]. For example, as oneof our application areas is (public) mobility

assistance, information collectedby a car-based telematics system might be extremely valuable for insurancecompanies, as this knowledge could be used to increase a person's fee or even deny a new contract. Additionally, not only the sensed data itself but alsocorresponding meta information might be considered sensitive, especiallywhen thinking of location privacy, where location fixes and/or time stampscollected by GPS, wireless networks, or NFC tags are considered importantmeta information. Hence, users often do not want to reveal the data collectedby their IoT devices to any third parties.

Even more privacy concerns and issues arise when outsourcing this data tothe cloud. The major concern of end-users in this setting is the perceived loss ofcontrol over data when it is outsourced to the cloud [11, 12]. Hence, providersof cloud-based services must explicitly commit themselves to guarantee confidentiality and protection of the stored and processed data, because otherwise,an adoption barrier consequently is likely to appear for the data owner due toher individual concerns. Such individual concerns mainly result from the factthat there is no control or at least transparency over the access to this data and,hence, data might be handed over to third parties or misused for unintendedpurposes [12]. Due to these concerns, end-users ultimately tend to refrain fromusing cloud-based services for (highly) sensitive data such as health-related information, for instance stored and shared by cloud-based personal health records(PHRs) systems.

**Privacy Considerations of Service Providers:** Notably, considering end-user's privacy concerns is not only important for researchers, but at least equally relevant for service providers. If service providers do not address the above depicted concerns adequately, they have to expect severe undesired consequences, ranging from the complete nonacceptance of their service to extremely costly lawsuits. Additional to these lawsuits, which mainly target private law issues between individual end-users and service providers, service providers also have to follow several legal restrictions. This becomes especially important when the realization of service functionality is outsourced to the cloud. One legal restriction that is considered extremely challenging with respect to the cloud and that also raises severe concerns ofend-users, is the transfer, storage, and processing of customer data across legislative boundaries.

## VI.CONCLUSION

The Federation of the Internet of Things and cloud computing with all itsadvantages is overly involved by intense privateness worries of end-users and privacy concerns of service providers. In order to overcome these excessive issues, mainly for privateness-crucial application regions including assisted dwelling and public mobility assistance, we offered our comprehensive approach to privacy inthe cloud-based IoT that addresses stop-customers and service developers at the identicaltime. As result of effort, we provided the UPECSI approach containing a complete set of technologies together with organizational measures tocomprehend user-driven privacy enforcement for cloud-based services in the IoT.

## REFERENCES

[1] L. Atzori, A. Iera, and G. Morabit, "The Internet of Things: A survey," Computer Networks, vol. 54, no. 15, 2010.
[2] J. H. Ziegeldorf, O. Garcia Morchon, and K. Wehrle, "Privacy in the Internet of Things: Threats and Challenges," Security and Communication Networks, 2013.
[3] R. Hummen et al., "A Cloud Design for User-controlled Storage and Processing of Sensor Data," in IEEE CloudCom, 2012.
[4] M. Henze et al., "Maintaining User Control While Storing and Processing Sensor Data in the Cloud," IJGHPC, vol. 5, no. 4, 2013.
[5] M. Eggert et al., "Sensor Cloud: Towards the Interdisciplinary Development of a Trustworthy Platform for Globally InterconnectedSensors and Actuators," RWTH Aachen University, Tech. Rep., 2013.
[6] F. Li et al., "Efficient and Scalable IoT Service Delivery on Cloud,"in IEEE CLOUD, 2013.
[7] M. Henze et al., "A Trust Point-based Security Architecture for SensorData in the Cloud," in Wissenschaftliche Ergebnisse des Trusted Cloud Technologieprogrammes, 2014.
[8] I. Ion et al., "Home is Safer than the Cloud! Privacy Concerns forConsumer Cloud Storage," in SOUPS, 2011.
[9] H. Takabi, J. Joshi, and G. Ahn, "Security and Privacy Challengesin Cloud Computing Environments," IEEE Security Privacy, vol. 8,no. 6, 2010.
[10] M. Henze, R. Hummen, and K. Wehrle, "The Cloud Needs Cross Layer Data Handling Annotations," in IEEE SPW, 2013.
[11] S. Koch, "Healthy Ageing Supported by Technology: A Cross Disciplinary Research Challenge," Inform. Health Soc. Care, vol. 35, no. 3-4, 2010.
[12] D. Christin et al., "A survey on privacy in mobile participatory sensing applications," J. Syst. Software, vol. 84, no. 11, 2011.
[13] I. G. Smith, Ed., The Internet of Things 2012 – New Horizons. IERC, 2012.
[14] R. Beckwith, "Designing for Ubiquity: The Perception of Privacy," IEEE Pervasive Computing, vol. 2, no. 2, 2003.
[15] S. Pearson, "Taking Account of Privacy when Designing Cloud Computing Services," in ICSE Workshop on Software Engineering Challenges of Cloud Computing, 2009.
[16] C. Powers, P. Ashley, and M. Schunter, "Privacy Promises, Access Control, and Privacy Management – Enforcing Privacy Throughout an Enterprise By Extending Access Control," in ISEC, 2002.
[17] A. Lounis et al., "Secure and Scalable Cloud-Based Architecture for e-Health Wireless Sensor Networks," in ICCCN, 2012.
[18] A. Navarro Perez and B. Rumpe, "Modeling Cloud Architectures as ´Interactive Systems," in MDHPCL, 2013.
[19] L. Hermerschmidt, A. Navarro Perez, and B. Rumpe, "A Model-based ´Software Development Kit for the SensorCloud Platform," in Wissenschaftliche Ergebnisse des TrustedCloud Technologieprogrammes, 2014.
[20] A. D. Molina, M. Salajegheh, and K. Fu, "HICCUPS: Health Information Collaborative Collection Using Privacy and Security," in ACM SPIMACS, 2009.
[21] A. Wood et al., "Context-Aware Wireless Sensor Networks for Assisted Living and Residential Monitoring," IEEE Network, vol. 22, no. 4, 2008.

[22] W. Itani, A. Kayssi, and A. Chehab, "Privacy as a Service: PrivacyAware Data Storage and Processing in Cloud Computing Architectures," in IEEE DASC, 2009.
[23] M. Eggert, R. H¨außling, D. Kerpen, K. R¨ussmann, SensorCloud: Sociological Contextualization of an Innovative Cloud Platform, in: H. Krcmar, R. Reussner, B. Rumpe (Eds.), Trusted Cloud Computing, Springer, 2014, pp. 295{313. doi:10.1007/978-3-319-12718-7_18.
[24] M. Lesk, The Price of Privacy, IEEE Security Privacy 10 (5) (2012) 79{81. doi:10.1109/MSP.2012.133.
[25] R. Beckwith, Designing for Ubiquity: The Perception of Privacy, IEEE Pervasive Computing 2 (2) (2003) 40{46. doi:10.1109/MPRV.2003.1203752.
[26] S. Pearson, Taking Account of Privacy when Designing Cloud Computing Services, in: 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, IEEE, 2009, pp. 44{52. doi:10.1109/CLOUD.2009. 5071532.
[27] S. Pearson, A. Benameur, Privacy, Security and Trust Issues Arising from Cloud Computing, in: 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), IEEE, 2010, pp. 693{702. doi:10.1109/CloudCom.2010.66.
[28] M. Zhou, R. Zhang, W. Xie, W. Qian, A. Zhou, Security and Privacy in Cloud Computing: A Survey, in: 2010 Sixth International Conference on Semantics Knowledge and Grid (SKG), IEEE, 2010, pp. 105{112. doi: 10.1109/SKG.2010.19.
[29] J. Heiser, M. Nicolett, Assessing the Security Risks of Cloud Computing, Tech. Rep. G00157782, Gartner (2008).
[30] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Generation Computer Systems 28 (3) (2012) 583{592. doi:10.1016/j. future.2010.12.006.
[31] De Brauw Blackstone Westbroek N.V., EU Country Guide Data Location & Access Restriction (2013).
[32] J. Rosen, The Right to Be Forgotten, Stanford Law Review Online 64 (2012) 88{92.
[33] M. Henze, L. Hermerschmidt, D. Kerpen, R. H¨außling, B. Rumpe, K. Wehrle, User-driven Privacy Enforcement for Cloud-based Services in the Internet of Things, in: 2014 International Conference on Future Internet of Things and Cloud, IEEE, 2014, pp. 191{196. doi:10.1109/FiCloud. 2014.38.
[34] M. Glinz, S. Fricker, on shared understanding in software engineering: an essay, Computer Science - Research and Development (2014). doi: 10.1007/s00450-014-0256-x.
[35] C. Powers, P. Ashley, M. Schunter, Privacy Promises, Access Control, and Privacy Management Enforcing Privacy Throughout an Enterprise By Extending Access Control, in: Third International Symposium on Electronic Commerce, IEEE, 2002, pp. 13{21. doi:10.1109/ISEC.2002. 1166906.
[36] A. Lounis, A. Hadjidj, A. Bouabdallah, Y. Challal, Secure and Scalable Cloud-Based Architecture for e-Health Wireless Sensor Networks, in: 2012 21st International Conference on Computer Communications and Networks (ICCCN), IEEE, 2012, pp. 1{7. doi:10.1109/ICCCN.2012.6289252.
[37] D. Thilakanathan, S. Chen, S. Nepal, R. Calvo, L. Alem, A platform for secure monitoring and sharing of generic health data in the Cloud, Future Generation Computer Systems 35 (2014) 102{113. doi:10.1016/j. future.2013.09.011.
[38] M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou, Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption, IEEE Transactions on Parallel and Distributed Systems 24 (1) (2013) 131{143. doi:10.1109/TPDS.2012.97.