The Data of Things: Strategies, Patterns and Practice of Cloud-based Participatory Sensing

Michalas, A. and Giannetsos, T.

This is an electronic version of a paper presented the *International Conference on Innovations in InfoBusiness and Technology (ICIIT)* Colombo, Sri Lanka. 04 Mar 2016.

The Data of Things: Strategies, Patterns and Practice of Cloud-based Participatory Sensing

Antonis Michalas
Cyber Security Group,
Department of Computer Science
University of Westminster, UK
michalas@*w*estminster.ac.uk

Thanassis Giannetsos
Surrey Centre for Cyber Security
Department of Computer Science
University of Surrey, UK
a.giannetsos@surrey.ac.uk

***Abstract*—The broad capabilities of current mobile devices have paved the way for Mobile Crowd Sensing (MCS) applications. The success of this emerging paradigm strongly depends on the quality of received data which, in turn, is contingent to mass user participation; the broader the participation, the more useful these systems become. However, there is an ongoing trend that tries to integrate MCS applications with emerging computing paradigms such as cloud computing. The intuition is that such a transition can significantly improve the overall efficiency while at the same time it offers stronger security and privacy-preserving mechanisms for the end-user. In this position paper, we dwell on the underpinnings of incorporating cloud computing techniques to facilitate the vast amount of data collected in MCS applications. That is, we present a list of core system, security and privacy requirements that must be met if such a transition is to be successful. To this end, we first address several competing challenges not previously considered in the literature such as the scarce energy resources of battery-powered mobile devices as well as their limited computational resources that they often prevent the use of computationally heavy cryptographic operations and thus offering limited security services to the end-user. Finally, we present a use case scenario as a comprehensive example. Based on our findings, we posit open issues and challenges, and discuss possible ways to address them, so that security and privacy do not hinder the migration of MCS systems to the cloud.**

I. Introduction

During the last few years the area of mobile sensing has met a great development and has the potential to offer a new understanding of our environment that will lead to innovative applications with tangible positive impact on the day-to-day users' experience. The widespread capabilities of commodity mobile devices have paved the way for the emerging of Participatory Sensing (PS). This new sensing paradigm changes the traditional view of the location-based services where people are passive data consumers, with one where people are directly involved in the information collection and sharing process.

The openness of such systems and the richness of user data they entail (one can collect valuable data, practically from everywhere) raise significant concerns for their storage and processing. Despite the benefits of using mobile sensing applications, users' have been slow to adopt such applications especially when compared to other sectors like banking where customer information is also sacrosanct. Among the most important reasons for the slow adoption of such services is the fear of storing sensitive data online. Without proper security mechanisms to protect users data from unauthorized access, it is much easier for sensitive information to be leaked to interested third parties.

The more the users engage and are called upon by the PS system, the richer the data they contribute (or consume) and, thus, the more susceptible they are to privacy threats. Sensitive information, including daily routines, location and social relations, is given away [1]. The fine-grained nature of such personal data can lead to extensive user-profiling, unsolicited targeted advertisement or, even, personal attacks and stalking [2]. This is intensified when users belong to small groups that share similar characteristics (e.g., work/residence area, entertainment preferences [3]). However, as recent experience shows, assuming that users can simply trust the PS system they contribute sensitive data to, is no longer a viable option. Therefore, it is imperative to address privacy concerns because users perceive them to be significant; as a result, they may refuse to use or even oppose a service.

Privacy protection is necessary to motivate user participation, but it is not (by itself) a sufficient condition. What is needed, is to provide *incentives* to engage as many people as possible, notably with diverse backgrounds, interests and availability. Indeed, relying only on the altruistic behavior of contributing participants [4] may not be adequate. This is why the research community has identified various types of incentives and ways to materialize them, such as reputation systems [5, 6], service quotas [7] and monetary rewards [8]. However, it is necessary to provide such incentives in a privacy-preserving manner. For example, users should be rewarded with credits for their contributions without revealing what kind of data they shared or the task they participated in.

Cloud computing has all the necessary features in order to offer strong security and privacy preserving mechanisms to the users of such applications. Just as the Internet has become a global phenomenon, so too has cloud computing, which is poised to become *the* catalyst for change in the near future.

Until recently, large-scale computing was available exclusively to large organizations with an abundance of in-house expertise. Cloud computing has changed that to the point where any user with even basic technical skills can obtain access to vast computing resources at low cost. In the

technology adoption lifecycle, cloud computing has now moved from an early adopters stage to an early majority, where we typically see exponential number of deployments. Throughout the past few years, many users have started relying on cloud services without realizing it. Major web mail providers utilize cloud technology; tablets and smartphones often default to automatically uploading user photos to cloud storage and social networks; finally, several prominent CRM vendors offer their services using the cloud. In other words, the adoption of cloud computing has moved from focused interest to widely spread intensive experimentation and is now rapidly approaching a phase of near ubiquitous use.

Enterprises increasingly recognize the compelling economic and operational benefits of cloud computing. Virtualizing and pooling IT resources in the cloud enables organizations to realize significant cost savings and accelerates deployment of new applications, simultaneously transforming business and government at an unprecedented pace. As a result, participatory sensing applications can benefit by moving to the cloud. Users' will be able to execute computationally heavy operations by using cloud resources instead of relying to the constraint power of their devices.

A. Contribution

In this position paper, we dwell on the underpinnings of incorporating cloud computing techniques to facilitate the vast amount of data collected in PS. More precisely, we present a list of core system, security and privacy requirements and challenges that must be considered when migrating participatory sensing applications to a cloud environment. To this end, we first address several competing challenges not previously considered in the literature such as the scarce energy resources of battery-powered mobile devices as well as their limited computational resources that they often prevent the use of computationally heavy cryptographic operations and thus offering limited security services to the end-user.

These security requirements were derived based on our experience with migrating existing applications to a private Infrastructure-as-a-Service (IaaS) cloud [9]. We extend this guide by discussing important characteristics for cloud environments that will pave the way for providing tighter security when building participatory sensing application for the cloud.

B. Organization

The remainder of this paper is organized as follows: In Section II we present the main entities that will participate in our system model and we proceed by defining our problem statement. In Section III we analyze the core set of requirements that are needed for a successful swift of a PS application to the cloud while in Section IV. Finally, in Section V we conclude the paper and we also present some future steps regarding the implementation and evaluation of the proposed architecture.

II. Problem Statement and Preliminaries

In this section, we describe the main entities that participate in the proposed architecture and we explicitly define the problem that we try to tackle.

Cloud Service Provider (CSP): One of the common models of a cloud computing platform is Infrastructure-as-a-Service (IaaS). In its simplest form, such a platform consists of cloud hosts which operate virtual machine guests and communicate through a network. Often a cloud middleware manages the cloud hosts, virtual machine guests, network communication, storage resources, a public key infrastructure and other resources. Cloud middleware creates the *cloud infrastructure* abstraction by weaving the available resources into a single platform. In our system model we consider a cloud computing environment based on a trusted IaaS provider like the one described in [10]. The IaaS platform consists of cloud hosts which operate virtual machine guests and communicate through a network. In addition to that, we assume a PaaS provider, like the one described in [11], that is built on top of the IaaS platform and can host multiple outsourced databases. Furthermore, the PaaS provider offers an API through which a developer can deploy a PS application.

Registration Authority (RA): RA is responsible for the registration of users. Additionally, RA has a public/private key pair denoted as $\mathsf{pk}_{\mathsf{RA}}/\mathsf{sk}_{\mathsf{RA}}$. Apart from that, RA is responsible for generating parameters that will be used for the proper function of the PS application (submit a new report, reveal the identity of a misbehaving user etc.). RA can run as a separate third party but can be also implemented as part of the cloud platform we described earlier.

User (u): In our scenario a user that uses the PS application is considered as a typical user. The operations that a user can perform are the following: *a)* register to the service, *b)* generate encryption keys to safely protect her data, *c)* store data in the cloud as well as retrieve and search over her private data that has been sent to the cloud. In addition to that, each u_i should be able to share her private data with other legitimate users. By u_i we denote a user with a unique identification i.

Furthermore, we assume that the reader is familiar with the concept of public key cryptography. Moreover, we assume that each authority has generated a public/private key pair. The private key is kept secret, while the public key is shared with the rest of the community. These keys will be used to secure message exchanges in the community, hence the communication lines between parties are assumed to be secure. It is also assumed that users knows the public keys of RA and the hosts operated by the CSP.

Problem Statement: *Let $U = \{u_1, \ldots, u_n\}$ be the set of all users that are registered through a registration authority (RA) and CSP the cloud service provider that stores users' data. Lets assume that a user u_i collects data d_j^i from her environment and wishes to store them to the CSP. The problem here is to find a way to achieve the following:*

1) *Keep the identity of u_i private, even if CSP colludes with RA (provide unlinkability);*
2) *Store d_j^i in an encrypted form in order to protect private information from unauthorized access;*

3) *User u_i should be able to securely share d_j^i with another user;*
4) *Trace back a user who is acting maliciously (provide accountability);*

III. Requirements

Seeking to successfully transit from a traditional architecture to a cloud-based environment, one has to cater to the system, security and privacy requirements of all involved actors and stake-holders. In an nutshell, the general design goal should entail moving from *centralization* to *ubiquitous* so that much of the processing will take place as close as possible to where the data is captured [12]. Achieving this objective is not straightforward. Thus, a necessary first step is a clear definition of the key requirements that such systems must meet. Such an analysis can be used as a stepping stone and provide essential information of the required steps for a successful migration to a cloud infrastructure (by minimizing the risks and avoiding common pitfalls).

Requirements identification is an necessary step in the process of transferring an information system (deployed on physical hardware) to a fully virtualized environment. At the same time, it is important to ensure that neither functionality nor performance will be degraded and that such requirements should include adequate mechanisms for mitigating security risks introduced by virtualization.

• **R1: Security & Privacy Concerns for End-users:** When building cloud services, two of the biggest challenges revolve around the security and privacy of end-users. The externalized aspect of outsourcing can make it harder to maintain data integrity and privacy and organizations should include mechanisms to mitigate security risks introduced by virtualization. Especially when they deal with sensitive data the protection of stored information comes as a top priority. Therefore, data security can be seen as the foundation upon which the whole PS initiative should be based on.

Even more privacy concerns and issues arise when outsourcing this data to the cloud. For end-users, the major concern is the perceived loss of control over data if it is outsourced to the cloud. This mainly results from the fact that 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 unintended purposes. Due to these concerns, end-users tend to refrain from using cloud-based services for (highly) sensitive data.

Since most cloud architectures deal with shared resource pools across multiple groups (both internal and external), security and multi-tenancy must be integrated into every aspect of an operational architecture and process. Services need to be able to provide access to only authorized users and in this shared resource pool model the users' need to be able to trust that their data and applications are secure.

Furthermore, by moving PS systems to the cloud, users can store, organize, share, and access private information for practically, *anything*, from *anywhere* and at *anytime*. Thus, all entities should be authenticated and their communications should be protected from any alteration and disclosure to unauthorized parties. In addition, users can decide to release part or their whole data collection history to other users. Even though the shared information should be provided in an efficient and timely manner, the existence of mechanisms that will ensure that shared data will be kept private and secure is mandatory. Additionally, users' must have full control of what information they share and with whom while at the same time they must be able to know not only who has access to their data but also who looked at them.

Integrity is another aspect of data security relevant in this context. Considering that information captured from user's mobile device has an important impact on their experience, it is essential that stored data are not altered or deleted without proper authorization.

• **R2: Energy Consumption:** A second key argument is that of the energy consumption. Providing strong security and privacy-preserving mechanisms consumes extra energy and users' are not willing to use PS applications if they drain their batteries considerably faster.

Even though there are many PS applications that try to provide strong security and privacy-preserving mechanisms [13, 14, 5] none of them is using the power of cloud computing to increase the security of the overall application without increasing the energy consumption [15] in a significant manner. Cloud computing, can offer a significant change to PS landscape since protocol designers can built applications that will provide strong security guarantees and will efficiently isolate their data using established cryptographic tools that will mostly run on the cloud. As a result, most of the computational burden can take place on the hosts of the CSP, thus, minimizing the overall energy consumption of user's device while at the same time providing stronger security. Incorporating cloud computing in PS applications can be proved as an efficient tool that will pave the way for the wider adoption of PS applications from the users'.

• **R3: Availability:** Another important problem when migrating a PS system to a cloud platform is availability. Organizations need to thoroughly analyze and understand the impacts on performance and availability and must take actions in order to be able to provide resources for the highest possible load situation. The risk of systems unavailability is a major issue since there are many cases where providers are unable to operate if their applications and/or users' data are not accessible. Even though cloud services could experience failures due to software and hardware faults, network faults or even natural disasters [16] cloud providers must ensure that their services will be properly delivered to the end users'. To do this, organizations must plan on disaster scenarios in order to improve the redundancy and reliability of their systems. Thus, it is necessary to apply multiple redundant energy sources for the data center and even have replication between multiple geographical locations in case of disasters.

The cloud's availability was called into question most sharply in April 2011, when large portions of Amazons Web Services infrastructure went down for as much as three days. This was a

major blow to a plethora of companies that used it. The popular video service Netflix, for example, relied heavily on Amazon, yet remained unaffected by the outage. How did Netflix escape a crisis? By working hard to build in redundancy so that it could stay running even in the event of a huge disruption or a DDoS attack [17, 18].

The on-demand, elastic, scalable, and customizable nature of the cloud must be considered when deploying cloud architectures. Many different customers might be accessing the same back-end application(s), but each customer has the expectation that only their application will be properly delivered to users. Making sure that multiple instances of the same application are delivered in a scalable manner requires both load balancing and some form of server virtualization.

• **R4: Scalability:** Furthermore, cloud based PS systems needs to be designed in such a way that will take advantage of the rapid scalability and deployment capabilities that cloud computing offers. In such environments scalability can be defined as "*the ability of a computing system to grow relatively easily in response to increased demand*" [19]. In other words, cloud-based PS applications should provide an inherently flexible and scalable infrastructure from the edge to the datacenter. With flexible architecture to ingest various types of data, and performance to meet varying workload requirements, our architecture enables scaling to meet evolving needs. With the power of cloud computing PS applications will be able to immediately augment existing resources in order to accommodate sudden increased requests, or scale down when the load is low without incurring additional capital expenses.

• **R5: Regulatory Compliance:** By storing data in the cloud, users hand it over to a provider that may have data centres in different geographical locations, countries or even continents. However, organizations that work with sensitive data, such as user's location records or personal health records, require complete control over the physical storage location and data access. As a result, storing sensitive data in the cloud complicates adherence to regulatory compliance laws, since such data may fall under different regulations depending on where it is physically stored. If for example data is moved to a different country, a set of different regulatory requirements may apply. Thus, prior to storing and processing data through the cloud, organizations must take into consideration the legal issues in order to ensure that users are in legal compliance [20]. Physical location of data in cloud storage is an increasingly urgent problem. In a short time, it has evolved from the concern of a few regulated businesses to an important consideration for many cloud storage users. A concrete analysis of the existing solutions can be found in [21].

From a service providers point of view, ignoring the previously depicted concerns can lead to undesired consequences, ranging from the non-acceptance of a service to costly lawsuits. Furthermore, especially when providing cloud services, legal restrictions, e.g., regarding the storage location and duration of data, have to be addressed [10], [15]. Particularly for legal requirements, service providers often need support from cloud providers.

• **R6: Cost:** The number one benefit of cloud migration is the potential for cost savings. By migrating a PS platform to the cloud, organizations can get powerful functionality in the most cost effective manner.

Ensuring the aforementioned properties separately is relatively straight-forward. Nevertheless, ensuring all of them at the same time is a challenge due to their (some) inherent contradictions. Overall, cloud migration can help organizations reduce the need for IT teams to operate and maintain expensive internal infrastructure, reduce software costs and shed at least some of their expensive IT infrastructure and shift computing costs to more manageable operational expenses.

Nonetheless, if the transition is not planned carefully, it can lead to unpredictable results. The main reason for that is the fact that there is a plethora of available solutions and many of them are not able to meet the specific needs of a PS system. Thus, a cloud solution that will not attain the above mentioned criteria can have catastrophic results for the adoption of PS by the end-users.

IV. Use-Case Scenario

In this section we briefly present a typical use-case scenario in which we incorporate a cloud infrastructure with an agnostic participatory sensing application. Figure 1 illustrates an overview of the system model as well as the typical functionality that is provided to the users'.

In the first step, user u_i registers her smart-phone by installing the participatory sensing software from an application distributed market such as the Android Market or thew App Store. The authorization at this step could happen during the installation process as employed by the Android phones or at the start of an application as on iPhones. During installation, a credential $cred_{u_i}$ is issued and stored to user's device. The stored credential should contain a set of attributes that can be used later on by the user to prove that she is legitimate.

The second step requires u_i to contact the registration authority in order to register to the actual PS application. To do so, u_i proves the she is a legitimate user by revealing some attributes from $cred_{u_i}$ to RA. The set of attributes that u_i sends to RA are encrypted with $\mathsf{pk}_{\mathsf{RA}}$. Thus, only the registration authority is able to decrypt them and check their validity. At this step, we need to mention that proper mechanisms to prevent replay attacks should be implemented. Upon reception, RA checks if the user is legitimate. If so, generates a unique credential that can be used by u_i to start storing data to the CSP.

Now that u_i has registered she can start storing data to the CSP. We assume, that a PaaS provider is running over a trusted IaaS cloud server. In addition to that, we assume that the PaaS can verify that the hosts in the IaaS provider are trusted by running an attestation scheme that will verify the integrity of the launched virtual machines. Furthermore, each time that u_i wishes to store fresh data to the CSP can receive a verification that the underlying host is running under a certain/trusted security profile and thus it is considered as trusted. We assume that u_i uses her mobile device to collect

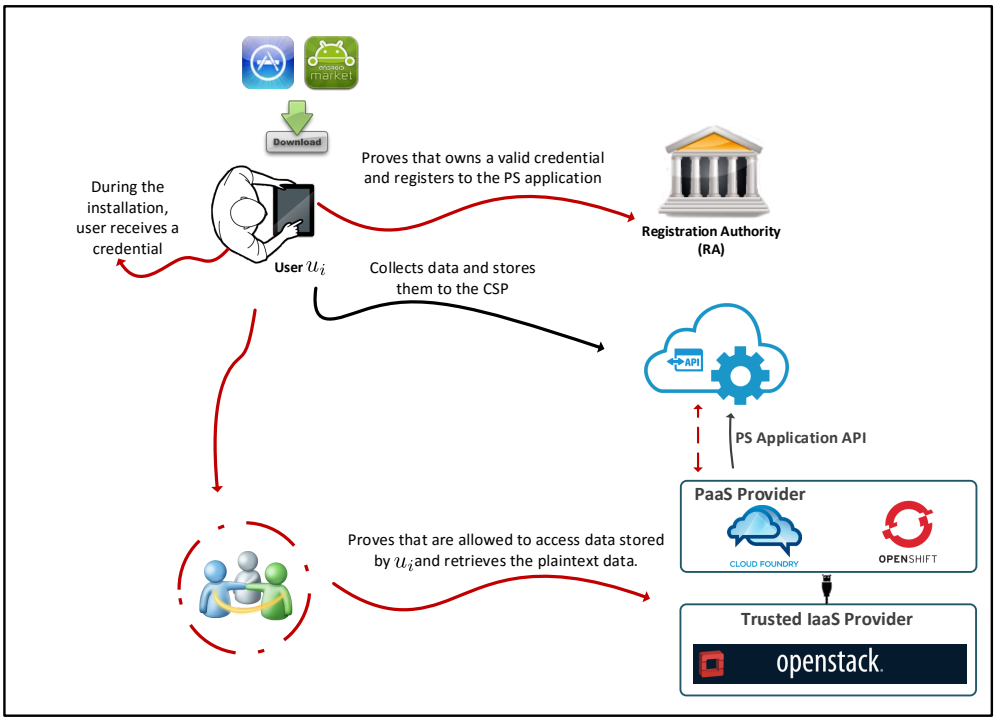

Fig. 1. Cloud-Based PS Scenario Overview

data d_j^i. Then, she contacts the CSP by using the API that is provided by the PaaS provider in order to store the data in the cloud. Every time that u_i contacts the CSP, she first needs to prove that is a legitimate user without proving her real identity. Then, she can send d_j^i to the CSP. To do so, u_i first encrypts d_j^i with a symmetric key $\mathsf{K_i}$ that is known only to her and sends the encrypted data to the CSP. Upon reception, the CSP stores the received ciphertext and also sends back to the user a token that can be used later on from u_i in order to retrieve the stored data. This step is crucial since we want to store the data in an anonymous way. Then, each time that u_i wishes to retrieve d_j^i sends the token to the CSP. The CSP finds the corresponding ciphertext and sends it bacj to u_i. Upon reception, u_i uses the symmetric key $\mathsf{K_i}$ to decrypt the data.

The last step in our scenario is when u_i wishes to share d_j^i with another user u_k. To do so, u_i should contact u_k in order to establish a new symmetric key $\mathsf{K_{i,k}}$. Then, u_i retrieves d_j^i as we described earlier and creates a new encryption by using $\mathsf{K_{i,k}}$. Then, contacts the CSP and stores the encrypted information. Then, the CSP returns a fresh unique token to u_i. Upon reception, u_i encrypts this token with $\mathsf{K_{i,k}}$ and shares it with u_k. At that point, u_k can retrieve the encrypted information by contacting the CSP and using the token and key $\mathsf{K_{i,k}}$ thas was established with u_i.

The aforemenioned protocol that allows two or more users to share a file is not efficient if u_i wishes to share d_j^i with many users. As a result, a different approach would be to implement a forward-looking design for a cryptographic cloud storage that will be using the very promising approach of searchable encryption [22]. In such a scenario a user can search over encrypted data without having to decrypt them first. Such an approach will also lead us to outline the principles for building a secure cloud storage on top of a cloud storage provided by a possible untrusted infrastructure.

V. Conclusion

In this paper, we provided a guide for incorporating cloud computing with PS applications. To this end, we presented key aspects for securely migrating existing PS applications to a fully virtualized cloud. We presented a list of security requirements relevant for the deployment of an agnostic PS application in an IaaS cloud. Next, we described a prototype cloud-based PS application that improves the confidentiality and privacy protection of users' records without affecting data access functionality from a user perspective.

The security risks and requirements relevant to a PS system deployment in an IaaS cloud presented in this paper cover only a fraction of the technical and security challenges facing a large-scale migration of PS systems to the cloud. We hope this contribution will encourage an exchange of best practices and lessons learned in migrating PS systems to fully virtualized cloud environments.

Future work involves the implementation of a fully functional cloud-based PS solution that will provide strong security and privacy-preserving mechanisms for the end-user. In addition to that, we plan to enhance our design by incorporating intrustion detection techniques such as the one we developed in [23, 24].

Moreover, applications in the area of vehicular communication [25, 12] can benefit from such a framework since it can offer strong security mechanisms and privacy-preserving mechanisms with limited resources.

Finally, we plan to implement a privacy preserving reputation system for cloud-based participatory sensing applications. The envisioned system will be based on [26, 27]and will effectively maintain the privacy and anonymity of users'.

REFERENCES

[1] S. Cleveland. "In search of user privacy protection in ubiquitous computing." In: *IEEE 13th Conference on Information Reuse and Integration (IRI)*. 2012, pp. 694–699.

[2] I. Boutsis and V. Kalogeraki. "Privacy Preservation for Participatory Sensing Data". In: *IEEE Conference on Pervasive Computing and Communications (PerCom)*. 2013.

[3] A. Singla and A. Krause. "Incentives for Privacy Tradeoff in Community Sensing". In: *Proceedings of the 1st AAAI Conference on Human Computation and Crowdsourcing (HCOMP)*. Palm Springs, 2013.

[4] Peter Kollock. "The economies of online cooperation: gifts and public goods in cyberspace". In: *Communities in the cyberspace*. 1st ed. Routledge, Feb. 1999, pp. 259–262.

[5] Antonis Michalas and Nikos Komninos. "The lord of the sense: A privacy preserving reputation system for participatory sensing applications". In: *Computers and Communication (ISCC), 2014 IEEE Symposium*. IEEE. 2014, pp. 1–6.

[6] Antonis Michalas et al. "Vulnerabilities of Decentralized Additive Reputation Systems Regarding the Privacy of Individual Votes". English. In: *Wireless Personal Communications* 66.3 (2012), pp. 559–575. ISSN: 0929-6212.

[7] T. Luo and C. K. Tham. "Fairness and social welfare in incentivizing participatory sensing." In: *IEEE 9th Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*. Seoul, 2012.

[8] I. Krontiris and A. Albers. "Monetary incentives in participatory sensing using multi-attributive auctions". In: *International Journal on Parallel Emerging Distributed Systems* 27.4 (2012), pp. 317–336.

[9] Antonis Michalas, Nicolae Paladi, and Christian Gehrmann. "Security aspects of e-Health systems migration to the cloud". In: *e-Health Networking, Applications and Services (Healthcom), 2014 IEEE 16th International Conference on*. IEEE. 2014, pp. 212–218.

[10] Nicolae Paladi, Antonis Michalas, and Christian Gehrmann. "Domain Based Storage Protection with Secure Access Control for the Cloud". In: *Proceedings of the 2014 International Workshop on Security in Cloud Computing*. ASIACCS '14. Kyoto, Japan: ACM, 2014. ISBN: 978-1-4503-2805-0.

[11] Yiannis Verginadis et al. "PaaSword: A Holistic Data Privacy and Security by Design Framework for Cloud Services". In: *Proceedings of the 5th International Conference on Cloud Computing and Services Science*. 2015, pp. 206–213. ISBN: 978-989-758-104-5. DOI: 10.5220/0005489302060213.

[12] T. Giannetsos, S. Gisdakis, and P. Papadimitratos. "Trustworthy People-Centric Sensing: Privacy, security and user incentives road-map". In: *Ad Hoc Networking Workshop (MED-HOC-NET), 2014 13th Annual Mediterranean*. 2014, pp. 39–46.

[13] Stylianos Gisdakis, Thanassis Giannetsos, and Panos Papadimitratos. "SPPEAR: security & privacy-preserving architecture for participatory-sensing applications". In: *Proceedings of the 2014 ACM conference on Security and privacy in wireless & mobile networks*. ACM. 2014, pp. 39–50.

[14] Stylianos Gisdakis, Thanassis Giannetsos, and Panos Papadimitratos. "SHIELD: A Data Verification Framework for Participatory Sensing Systems". In: *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. WiSec '15. New York, New York: ACM, 2015, 16:1–16:12. ISBN: 978-1-4503-3623-9.

[15] Lin Ye et al. "Path Metric Authentication for Low-Power and Lossy Networks". In: *Proceedings of the 1st ACM International Workshop on Cyber-Physical Systems for Smart Water Networks*. CySWater'15. Seattle, WA, USA: ACM, 2015, 5:1–5:6. ISBN: 978-1-4503-3485-3.

[16] Eman AbuKhousa, Nader Mohamed, and Jameela Al-Jaroodi. "e-Health Cloud: Opportunities and Challenges." In: *Future Internet* 4.3 (2012), pp. 621–645. URL: http://dblp.uni-trier.de/db/journals/fi/fi4.html#AbuKhousaMA12.

[17] Antonis Michalas et al. "New client puzzle approach for dos resistance in ad hoc networks". In: *Information Theory and Information Security (ICITIS), 2010 IEEE International Conference*. IEEE. 2010, pp. 568–573.

[18] A. Michalas, N. Komninos, and N.R. Prasad. "Multiplayer game for DDoS attacks resilience in ad hoc networks". In: *Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on*. 2011, pp. 1–5. DOI: 10.1109/WIRELESSVITAE.2011.5940931.

[19] Elizabeth Frander et al. "Getting your Head in the Clouds: The Use of Cloud Technology to Enhance Student Success". In: *Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications 2013*. Ed. by Jan Herrington, Alec Couros, and Valerie Irvine. Victoria, Canada: AACE, 2013, pp. 1415–1417.

[20] J. Domzal. "Securing the cloud: Cloud computer security techniques and tactics (Winkler, V.; 2011) [Book reviews]". In: *Communications Magazine, IEEE* 49.9 (2011), pp. 20–20.

[21] N. Paladi and A. Michalas. ""One of our hosts in another country": Challenges of data geolocation in cloud storage". In: *Wireless Communications, Vehicular Technology, Information Theory and Aerospace Electronic Systems (VITAE), 2014 4th International Conference on*. 2014, pp. 1–6.

[22] Antonis Michalas and Rafael Dowsley. "Towards Trusted eHealth Services in the Cloud". In: *1st International Workshop on Cloud Security and Data Privacy by Design (CloudSPD'15), co-located with the 8th IEEE/ACM International Conference on Utility and Cloud Computing (UCC)*. IEEE/ACM. Limassol, Cyprus, 2015.

[23] Ioannis Krontiris et al. "Cooperative Intrusion Detection in Wireless Sensor Networks". In: *Proceedings of the 6th European Conference on Wireless Sensor Networks*. EWSN '09. Cork, Ireland: Springer-Verlag, 2009, pp. 263–278. ISBN: 978-3-642-00223-6.

[24] Thanassis Giannetsos and Tassos Dimitriou. "LDAC: A localized and decentralized algorithm for efficiently countering wormholes in mobile wireless networks". In: *Journal of Computer and System Sciences* 80.3 (2014), pp. 618–643.

[25] S. Gisdakis et al. "SEROSA: SERvice oriented security architecture for Vehicular Communications". In: *Vehicular Networking Conference (VNC), 2013 IEEE*. 2013, pp. 111–118.

[26] T. Dimitriou and A. Michalas. "Multi-Party Trust Computation in Decentralized Environments". In: *New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on*. 2012, pp. 1–5.

[27] "Multi-party trust computation in decentralized environments in the presence of malicious adversaries". In: *Ad Hoc Networks* 15 (2014), pp. 53 –66.