Reasoning About Security and Privacy in Cloud Computing under a Unified Meta-Model

A. Pattakou[1], C. Kalloniatis[1] and S. Gritzalis[2]

[1]Cultural Informatics Laboratory, Department of Cultural Technology and Communication, University of the Aegean, University Hill, GR 81100 Mytilene, Greece
[2]Information and Communication Systems Security Laboratory, Department of Information and Communications Systems Engineering, University of the Aegean, GR 83200, Samos Greece
e-mail: {a.pattakou, chkallon}@aegean.gr;sgritz@aegean.gr

Abstract

Over the last decade, cloud computing presents a rapid growth as an increasing number of individuals, private and public organizations tend to adopt cloud technologies for storing their data or providing their services. However, due to the fact that migration into cloud in most cases implies that data subjects lose control of their data, many people and several scientists raise issues about data security and privacy in a cloud infrastructure. However, most of research efforts presented so far deal with either security or privacy protection in the cloud. Raising the trustworthiness of a cloud service provided requires both satisfaction of the security on the cloud assets as well as privacy protection of the end users. This paper presents a conceptual meta-model taking into account the security and privacy concepts that need to be considered when designing cloud services or migrating services to the cloud. This paper is the first step towards the development of a framework that will holistically deal with security and privacy under a unified language thus assisting software engineers on modelling secure and privacy-aware services into the cloud.

Keywords

Cloud, Privacy, Security, Requirements

1. Introduction

Although many people are not aware of cloud computing technology, they use it in their everyday life via social media, email, instant messaging, etc. Cloud computing technology provides an innovated system architecture which tends to transform the traditional IT model into a service model. This new model is changing the way that system resources are allocated, the way that data are stored and also the way that users gain access to their data due to the unique cloud characteristics. These characteristics have been identified by many researchers and referred to virtualization, multi-tenancy, elasticity and scalability, device and location independence (Kalloniatis et al. 2014). Thus, final users of a cloud infrastructure are able to enjoy numerous advantages arising from these characteristics. Typical examples are access to advanced services with low cost, access to data from any location by any device and zero maintenance cost. However, the same features

introduce new security and privacy issues so that new users are discouraged to move into the cloud.

However, when referring to a cloud infrastructure, it is important to take into consideration privacy and security requirements from the perspective of both users and cloud providers (Kalloniatis et al. 2013). Literature provides examples of research efforts in which cloud privacy and security requirements have been analyzed separately [(ENISA 2014), (Kalloniatis, 2015), (Kalloniatis et al. 2005), (Cavoukian and Reed, 2013)]. However, these requirements have to be examined under the same unified framework and not independently, as a failure to fulfill security requirements may affect privacy and vice versa. It is worth noting that the determination of privacy and security requirements should be performed at the designing level in order to support developers to select the appropriate methods and techniques during implementing cloud services (Mouratidis et al. 2013). Otherwise, the adoption of inappropriate implementation techniques may lead to services that do not fulfill users' privacy and security needs. As far as cloud providers are concerned, this determination at the early stage of analysis and design may facilitate the examination of interactions and conflicts between security and privacy requirements as well as the impact of these interactions on user needs.

This paper presents a conceptual meta-model as an initial step for modelling security and privacy under a unified framework. In section 2 respective research efforts from the field of security and privacy requirements engineering methods are presented. In Section 3, we present a set of privacy and security requirements that a cloud infrastructure has to fulfill in order to ensure data security and privacy for users. In section 4 the proposed metamodel is presented while in section 5 conclusions are mentioned.

2. Related Work

Although security and privacy requirements in traditional systems have been identified by several researchers [(Hansen, 2011), (ENISA 2014), (Kavakli et al. 2005), (Kalloniatis et al. 2005), (Kalloniatis et al. 2008)], cloud computing raises many new concerns due to the special cloud architecture and characteristics. On the one side, cloud characteristics and advantages such as elasticity, on-demand services, low cost and easy data sharing make the cloud environment very attractive. On the other side, data security and privacy can be affected by some other characteristics such as resource sharing, virtualization, loss data control and limited data portability. Migrating into the cloud is not an easy task since users or organizations should first evaluate multiple factors. As far as cloud providers are concerned, it is important to demonstrate high reliability, availability and transparency in mechanisms that are used to support privacy and security requirements in order to gain end users' confidence. Data protection should be a cloud provider's main concern during the whole data life cycle, from generation to destruction.

Security and privacy are of paramount importance in cloud computing as users might consider them to be counter-incentives for migration into the cloud. Identification

and analysis of security and privacy requirements during system development are very crucial steps in developing trustworthy systems. For managing security issues in traditional systems, several methodologies have been presented. Mouratidis and Giorgini (2007) proposed Secure Tropos, an approach that analyses security requirements from the early stages of the development process. Additionally, Giorgini et al. (2003) have extended i*/Tropos requirements engineering framework to deal with security requirements. SQUARE (Chen et al. 2004) and SREP (Mead and Steheny, 2005) are asset-based and risk-driven methods that follow a number of steps, for eliciting, categorizing, and prioritizing security requirements. Houmb et al. (2010) introduce the SecReq approach to elicit, analyse and trace security requirements, using Common Criteria Heuristic and UMLsec, from the requirements engineering phase to design. On the other hand, there are several works that focus on the identification and analysis of privacy requirements. PriS is a requirements engineering method that incorporates privacy requirements early in the system development process (Kalloniatis et al., 2008). PriS has been used as a base for the generation of the extended conceptual framework of this paper. Later, Islam et al. (2010) use natural language patterns to extract security requirements from laws and combine them with the ISO/IEC policies. Islam et al. (2012a) proposed a model-based process to support security and privacy requirements engineering using a set of concepts such as goal, actor, constraint and threat. Apart from these methodologies that applied to traditional systems, several works have been presented related to privacy and security issues in a cloud computing environment. Pearson and Benameur (2010) support that privacy threats differ depending on the type of cloud scenario. Additionally, Grobauer et al. (2011) identified these points where possible attacks can occur in a cloud computing. Finally, Islam et al. (2012b) introduced an approach that analyses privacy and security risks as a decision-making criterion for migrating into the cloud. However, most of the works presented above demonstrate a number of constraints. For instance, most methodologies that deal with security issues apply to the requirements stage of traditional systems only and do not consider privacy requirements. Methods that consider both security and privacy treat privacy as a subset of security. On the other side, works that have been developed for cloud-based systems mostly focus on the implementation stage of privacy and security requirements and not in analysis of these requirements.

3. Privacy and Security Related Concepts

A set of privacy and security concepts is presented below, aiming to record these requirements that have to be provided by a trustworthy infrastructure. This set of requirements can provide a strong base during analysis and design of security and privacy policies in the cloud. An accurate determination of security and privacy policies can prove to be crucial for the proper identification and implementation of privacy and security organization goals.

Integrity constitutes one of the most important factors in cloud data security and is aiming to ensure data from intentional modification such insertion or deletion of malicious data and unintentional modification such as random transmission error (Sabitha et al. 2013). Confidentiality is also one of the greatest concerns in cloud

computing security since resources can be shared between many users. Confidentiality is defined as the assurance that sensitive information is not disclosed to unauthorized persons, processes or devices (Goel et al. 2012). It is worth noting that user's data have to remain confidential not only to other cloud customers but also to cloud service provider. Another security property in the context of cloud computing is availability and is based on the idea of "on-demand services". Availability is referred to the ability of a cloud service provider to provide continuous service delivery. Data availability implies software, network and hardware availability (Zissis et al. 2012). In other words, cloud customers should be able to access data at any time from any connected device.

In addition to these properties, non-repudiation constitutes another security requirement and is defined as the ability to ensure that an action has taken place by an authority and this action cannot be repudiated later. Digital signature, one of the most important applications of cryptography, is the most common solution for ensuring non-repudiation in provided cloud services [(Wu et al. 2013), (Whaiduzzaman et al. 2014)].

Nowadays, a vast amount of sensitive data may be stored in a cloud infrastructure. Due to this fact, cloud computing environment needs an authentication mechanism in order to protect access in data from non-legitimate users. Authentication begins when a user tries to access information or a service. Authorization follows authentication aiming to determine what types of activities, resources and services may be accessed by an authenticated user.

Data portability is another great concern and is referred to users' ability to transfer data from one cloud provider to another, according to their needs. On the other hand, interoperability is defined as the ability of different cloud systems to understand each other in order to cooperate and interoperate. Both portability and interoperability presuppose standardization of the type storage.

In order to ensure privacy in a cloud environment, anonymity is a key. In the context of cloud computing, anonymity is defined as the ability of a customer to use cloud resources and services without being obliged to reveal his/her identity and without being tracked (Kalloniatis et al. 2014). The main objective of anonymity is to conceal personal identifiable information when there is no need to disclose such information (Kalloniatis, 2015). The concept of pseudonymity is close to the meaning of anonymity. In a cloud computing environment, pseudonymity is referred to the user's ability to use cloud resources and services by acting under one or many pseudonyms, without revealing his/her identity (Kalloniatis et al. 2005, December). Pseudonymity allows users to be tracked and be accountable for their actions in the cloud infrastructure.

Unlinkability is also one of the vital requirements that should be considered by a cloud vendor in order to provide privacy to customers. In a cloud environment, unlinkability has a twofold role; firstly, to prevent linkage between data and the user that processes the specific data and secondly when a sender and a recipient

communicate, they should not be identified as communicating each other (Kavakli et al. 2005 September).

In cloud computing, undetectability has to do with the ability of users to interact with cloud services and to use cloud resources without being detectable by potential attackers. Unobservability in the cloud is supposed to be stronger as well as is aiming to keep cloud users undetectable and anonymous too when interacting with cloud services or other users in a cloud infrastructure.

Apart from the above concepts, there is a set of requirements that aims at data protection against privacy violations. This set includes the concepts of provenanceability, transparency, isolation, accountability, intervenability and traceability.

Provenanceability is referred to the mechanism that collects data in a structured way in order to describe the history of a particular piece of data inside a cloud infrastructure. This description may include people, entities and activities that were involved in producing a data object (Katilu et al. 2015). But, since provenance data may reveal sensitive data, it is important cloud provider to be able to secure them.

Transparency is also one of the vital requirements in cloud computing area and is referred to the ability of a cloud customer to be aware of the policies, procedures and functions that a cloud provider follows. According to Gartner (Brodkin, 2008), cloud providers have the obligation to provide customers with clear details about architectures, risk controls policies, data location, recovery mechanisms etc.

Multi-tenancy, one of the most common attributes of cloud environment, allows the parallel use of resources by many users. Due to the sharing of resources between multi tenants, cloud provider should guarantee a certain level of isolation in order to achieve the complete seal of user's data (Kalloniatis et al. 2014).

Accountability is referred to the ability of a provider to give to his customers the appropriate control and transparency as to how their data are used, through auditing user's data and maintaining log records (Hande and Mane, 2015). As Jaatun et al. (2014) support an accountable cloud provider should be responsible and answerable for its data practices, clearly define his policies regarding their data, monitor its data practices, correct violations and demonstrate policy compliance.

Intervenability is one of the most important privacy protection goals (Hansen, 2011) and is referred to the ability of a user to interfere in the processing of his data. The meaning of intervenability includes the rights to data access without limitations, rectification and erasure of data, objection to data processing when processing does not comply with rules as well as the right to withdraw consent [(Kalloniatis et al. 2014), (European Commission, 2014), (Directive 95/46/EC)].

Traceability is referred to the mechanism that allows the registration of every human operation [i.e. the lifecycle of a user file (create, edit, transfer, delete)] in a chain of

events (log files) (Nakahara et al. 2011).

4. Conceptual Model

This section aims to present a conceptual framework that considers cloud privacy and security concepts within the system design process. This conceptual model is based on PriS method which was first introduced [(Kalloniatis et al. 2005 (August)), (Kalloniatis et al. 2008)] as a privacy requirements engineering method in traditional systems only. The main goal of the conceptual model is to represent a modelling language that will provide a strong base for those people that are involved in system analysis and design of security and privacy policies in the cloud, as it can assist in the identification of privacy and security organization goals. However, from the user's side, an analysis of these requirements can be proved extremely useful for the evaluation of cloud providers.

As shown in Fig 1, the central concept of the extended conceptual model is "goal". Goals refer to any intentional objectives that an organization needs to achieve. Goals in a cloud environment can be derived not only by a Cloud Service Provider (CSP) but by anyone involved in the cloud infrastructure such as cloud users, system designers and any external provider or entity. More specifically, goals are generated due to the issues raised by stakeholders. For instance, a CSP must operate and provide services within a specific legal framework, must protect user's privacy as legislation stipulates and secure user's data from any malicious attack. All these restrictions generate issues that in turn can generate new goals. Also, many issues might be derived by a SWOT (strength, weakness, opportunity, threats) analysis of the cloud-based system. Thus, before proceeding in system design, all these issues must be identified and analyzed in order to determine accurately the objectives of the system.

Processes can realise goals. However, processes cannot be applied directly to the main goal, as the achievement of that goal might presuppose the achievement of one or more sub-goals. Thus, the origin goal has to be broken down to simpler goals by system designers. A sub-goal might be related to the achievement of more than one goal, thus forming a structure of goals/sub-goals and their relationships. It is worth mentioning that during this process, it is possible that new goals are identified and others are rejected or replaced in the hierarchy of goals. In Figure 1, the satisfaction relationships between goals and sub-goals is illustrated with the AND/OR decomposition entity.

Additionally, conceptual model introduce another type of relationship between two or more different goals. This type is referred to as an influencing relation type as it examines whether two different goals are conflicting or not. In other words, system analysts have to analyze the relation between goals. In this direction, two relation types can be identified. The first one is referred as a Support relationship where the achievement of one goal assists in the achievement of another. The second one is illustrated as a Conflict relationship where the achievement of one goal prevents the achievement of another. In case of a conflict relationship, the stakeholders involved

have to negotiate in order to resolve these conflicts.

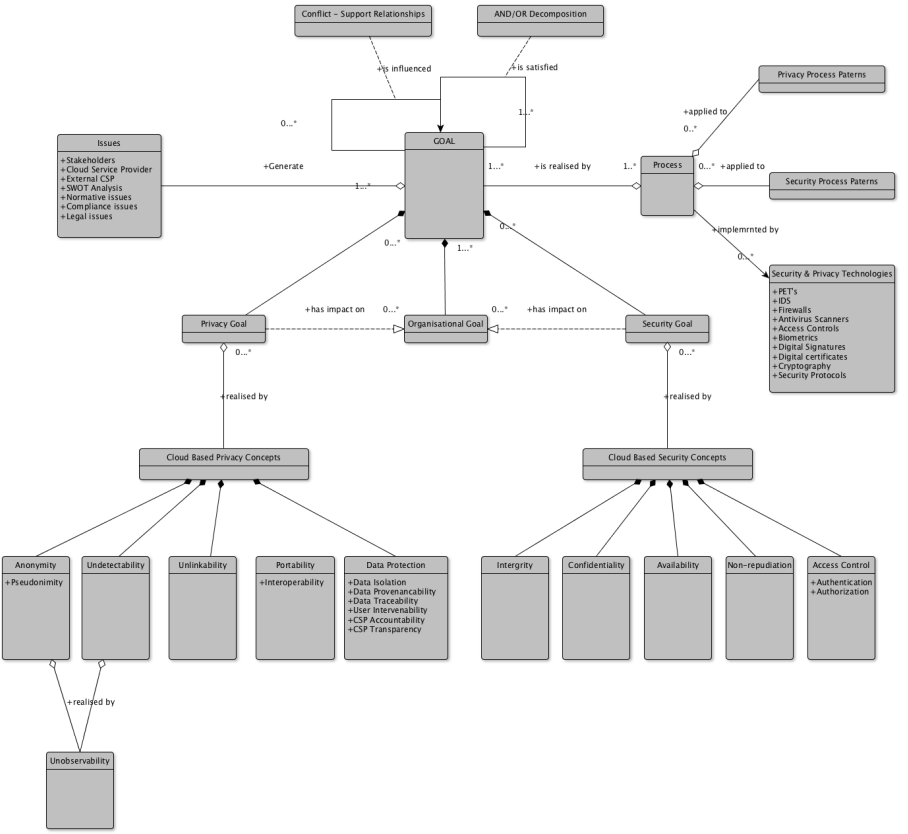

Figure 1: Conceptual Model

In the conceptual model, goals are classified into three types namely organizational goals, privacy goals and security goals. Organizational goals are referred in the main objectives that an organization needs to achieve through the system into consideration. On the other side, privacy and security goals are introduced due to the special privacy and security concepts of a cloud based system. Anonymity, pseudonimity, undetectability, unlinkability, portability, interoperability and data protection have been identified as privacy-related concepts. Data protection includes the concepts of isolation, provenancability, traceability, intervenability, accountability and transparency as these concepts aim at protecting system or user's data in a cloud infrastructure. Unobservability has been illustrated as a concept deriving from the coexistence of undetectability of assets and anonymity of users. On the other side, integrity, confidentiality, availability, non-repudiation and access control have been indicated as security concepts. As shown in Fig 1, authentication and authorization have been included in access controls concept as both aim at defining user's access level to the cloud infrastructure. However, privacy and

security goals may have an impact on organizational goals as the identification of privacy and security requirements during system design might trigger new organization goals or reject others. A detailed description of all the aforementioned security and privacy concepts can be found in (Kalloniatis et al. 2014).

As previously stated goals are realised by processes. For the generation of these processes, it is proposed that system designers and developers use patterns in order to build processes with specific properties. Process patterns are generalised process models that deal with a specific issue through a number of specific steps. In this direction, a system designer/developer should be able to select from a repository of patterns those that best fit in the process into consideration. Depending on the goal that a process is aiming to implement, the related pattern has to be selected. For instance, a privacy process pattern can be selected in case the relevant process aims at realizing a privacy goal. Respectively, a security process pattern can be used to achieve a security goal. It is worth mentioning that the use of the related process patterns may assist developers in selecting the most appropriate technology (PET's, IDS, Digital Signature, firewalls etc.) based on the process patterns that best satisfies privacy and security requirements. In general, the use of process patterns aims at describing the effect of privacy/security requirements on system processes and at facilitating the identification of the technology that best supports security and privacy goals.

5. Conclusions

Cloud computing is a modern technology with very attractive features such as low cost, on-demand services, device and location independence. However, a cloud-computing environment, as it concentrates a vast amount of data, consists a tempting target for possible attackers. Under these circumstances, users raise privacy and security concerns, a fact that creates restrictions in migration into the cloud. Several researchers focus on the identification of security or privacy requirements separately while others consider privacy as a subset of security. In this paper, security and privacy have been considered as two different concepts but they have been examined under the same conceptual model due to the fact that a security breach may affect users' privacy and vice versa. Thus, an extended conceptual model has been presented where both security and privacy requirements have been considered as organizational goals that need to be attained. This conceptual model will provide the basis for our future work in the area of cloud computing security and privacy analysis and modelling.

6. References

Brodkin, J. (2008). Gartner: Seven cloud-computing security risks. Infoworld, 2008, 1-3

Cavoukian, A., & Reed, D. (2013). Big Privacy: Bridging Big Data and the Personal Data Ecosystem through Privacy by Design. Information Privacy Commissioner, Toronto, December, available from www. ipc. on. ca/images/Resources/pbdbig_privacy. pdf

Chen, P., Dean, M., Ojoko-Adams, D., Osman, H., & Lopez, L. (2004). Systems quality requirements engineering (square) methodology: Case study on asset management system (No. CMU/SEI-2004-SR-015). CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

ENISA (2014): "Privacy and Data Protection by Design – from policy to engineering", www.enisa.europa.eu

European Commission,A Digital Agenda for Europe (2014): "Cloud Service Level Agreement Standardisation Guidelines", https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines

Giorgini, P., Massacci, F., Mylopoulos, J., 2003. Requirement engineering meets security: a case study on modelling secure electronic transactions by VISA and Mastercard. In: 22nd International Conference On Conceptual Modeling (ER2003), vol. 2813 of Lecture Notes in Computer Science, Springer, pp. 263–276

GOEL, Abhishek; GOEL, Shikha. Security Issues in cloud computing. International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2012, 1.4., http://www.ijaiem.org/volume1Issue4/IJAIEM-2012-12-26-033.pdf

Grobauer, B., Walloschek, T., Stocker, E., 2011. Understanding cloud computing vulnerabilities. IEEE Security & Privacy Magazine 9 (2), 50–57

Hande, S. A., & Mane, S. B. (2015, May). An analysis on data Accountability and Security in cloud. In Industrial Instrumentation and Control (ICIC), 2015 International Conference on (pp. 713-717). IEEE

Hansen, M. (2011). Top 10 mistakes in system design from a privacy perspective and privacy protection goals. In Privacy and Identity Management for Life (pp. 14-31). Springer Berlin Heidelberg

Houmb, S.H., Islam, S., Knauss, E., Jürjens, J., Schneider, K., 2010. Eliciting security requirements and tracing them to design: an integration of common criteria, heuristics, and UMLsec. Requirements Engineering Journal 15 (1 (Mar)), 63–93

Islam, S., Mouratidis, H., Kalloniatis, C., Hudic, A., Zechner, L., 2012a. Model based process to support security and privacy requirements engineering. International Journal of Secure Software Engineering (IJSSE)

Islam, S., Mouratidis, H., Weippl, E., 2012b. A goal-driven risk management approach to support security and privacy analysis of cloud-based system. In: Security Engineering for Cloud Computing: Approaches and Tools. IGI Global Publica- tion, United States of America by (an imprint of IGI Global) 701 E. Chocolate Avenue, Hershey, PA 17033

Islam, S., Mouratidis, H., Wagner, S., 2010. Toward a framework to elicit and manage security and privacy requirements from laws and regulation. In: Proceeding of Requirements Engineering: Foundation for Software Quality (REFSQ), Lecture Notes in Computer Science, vol. 6182/2010, pp. 255–261

Jaatun, M. G., Pearson, S., Gittler, F., & Leenes, R. (2014, December). Towards Strong Accountability for Cloud Service Providers. In CloudCom (pp. 1001-1006)

Kalloniatis, C. (2015). Designing Privacy-Aware Systems in the Cloud. In Trust, Privacy and Security in Digital Business (pp. 113-123). Springer International Publishing

Kalloniatis, C., Mouratidis, H., Vassilis, M., Islam, S., Gritzalis, S., & Kavakli, E. (2014). Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts. Computer Standards & Interfaces, 36(4), 759-775

Kalloniatis, C., Mouratidis, H., & Islam, S. (2013). Evaluating cloud deployment scenarios based on security and privacy requirements. Requirements Engineering, 18(4), 299-319

Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2008). Addressing privacy requirements in system design: the PriS method. Requirements Engineering, 13(3), 241-255

Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2005, August). PriS methodology: incorporating privacy requirements into the system design process. In Proceedings of the SREIS 2005 13th IEEE International Requirements Engineering Conference–Symposium on Requirements Engineering for Information Security, J. Mylopoulos, G. Spafford (Eds.)

Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2005, December). Dealing with privacy issues during the system design process. In Signal Processing and Information Technology, 2005. Proceedings of the Fifth IEEE International Symposium on (pp. 546-551). IEEE

Katilu, V. M., Franqueira, V. N., & Angelopoulou, O. (2015, August). Challenges of Data Provenance for Cloud Forensic Investigations. In Availability, Reliability and Security (ARES), 2015 10th International Conference on (pp. 312-317). IEEE

Kavakli, E., Kalloniatis, C., & Gritzalis, S. (2005, September). Addressing Privacy: Matching User Requirements with Implementation Techniques. In 7th Hellenic European Conference on Computer Mathematics and its Applications (HERCMA 2005), Athens, Greece

Mead, N.R., Steheny, T., 2005. Security quality requirements engineering (SQUARE) methodology. SIGSOFT Software Engineering Notes 30 (4), 1–7

Mouratidis, H., Islam, S., Kalloniatis, C., & Gritzalis, S. (2013). A framework to support selection of cloud providers based on security and privacy requirements. Journal of Systems and Software, 86(9), 2276-2293

Mouratidis, H., Giorgini, P., 2007. Secure tropos: a security-oriented extension of the tropos methodology. International Journal of Software Engineering and Knowl- edge Engineering 17 (2), 285–309

Nakahara, S., et al.: Cloud traceability (CBoC TRX). NTT Technical Journal, 31–35 (October 2011)

Pearson, S., Benameur, A., 2010. Privacy, Security and Trust Issues Arising from Cloud Computing. In: 2nd IEEE International Conference on Cloud Computing Technology and Science, IEEE Computer Society. PRISM, UK, pp. 693–702

Sabitha, S. & George, R. S. (2013). Survey on Data Integrity in Cloud Computing. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Vol, 2

Whaiduzzaman, M., Sookhak, M., Gani, A., & Buyya, R. (2014). A survey on vehicular cloud computing. Journal of Network and Computer Applications, 40, 325-344

Wu, W., Zhou, J., Xiang, Y., & Xu, L. (2013). How to achieve non-repudiation of origin with privacy protection in cloud computing. Journal of Computer and System Sciences, 79(8), 1200-1213

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation computer systems, 28(3), 583-592