Pre-Proceedings of International Workshop on Trustworthiness, Accountability and Forensics in the Cloud (TAFC)

Organised by DIMACS/BIC/A4Cloud/CSA UK Chapter and CSA Irish Chapter

June 6 - 7, 2013
Malaga, Spain
held in conjunction with 7th IFIP WG 11.11 International Conference on Trust Management

ISSN: 2079-2247

Publisher: IFIP WG 11.11 on Trust Management

Printed by University of Malaga, Spain

2013

Table of Contents

Accountability for Privacy in Cloud Computing: Is this a new Problem?

Colin J. Bennett, Department of Political Science, University of Victoria, Victoria, BC. Canada

www.colinbennett.ca

Abstract

The notion of "accountability" is a currently fashionable within the community of scholars, regulators and activists concerned with privacy and data protection. At one level, it has always been a central principle within these laws and policies, and is implicit if not explicit in every attempt to make organizations more responsible for the personal data they collect and process. At one level, there is nothing new. At another level, however, accountability has come to represent a distinct policy approach to the vexing problem of the regulation of international personal data processing, in the past termed "data exports" or "transborder data flows." Over the last few years, the debate on international data protection has become somewhat polarized between those who would continue to support the EU approach, essentially a prohibition on transfers to countries which do not have an "adequate level" of data protection, and the "accountability approach" which focuses more on the protection afforded by individual data controllers.

Scholars of public administration have spilled a lot of ink over the many meanings of the word "accountability." However, there seems to be a consensus that the process must involve being called "to account" by some authority for one's actions. Accountability implies a process of transparent interaction, in which an external body seeks answers and possible rectification. That external agent is presumed to have rights of authority over those who are accountable – including the rights to demand answers and impose sanctions if the organization's "account" is not accurate or complete. If there is no possibility of external compulsion to change practices, there can be no accountability. Thus, there must be a common understanding *of who is accountable, for what and to whom.*

The recent policy discussions about accountability and privacy protection, especially in the context of cloud computing, have not been precise with the result that the word has been expanded and distorted to serve a variety of political and economic interests. Nobody can be against "accountability" in the abstract. But when the concept becomes framed in political discourse, there are a number of questions that need to be raised about its meaning and its relationship to the central goal of protecting privacy. *How policy problems get framed shapes how they will be resolved.*

In this talk, I first review briefly the history of trying to regulate international flows of personal data, with a view to understanding how the "accountability" approach arose. I then review some of the assumptions (implicit and explicit) upon which this current emphasis on accountability seems to be based, and with particular reference to another imprecise phenomenon – "cloud computing".

Speaker biography

Colin Bennett received his Bachelor's and Master's degrees from the University of Wales, and his Ph.D from the University of Illinois at Urbana-Champaign. Since 1986 he has taught in the Department of Political Science at the University of Victoria, where he is now Professor. From 1999-2000, he was a fellow at Harvard's Kennedy School of Government. In 2007 he was a Visiting Fellow at the Center for the Study of Law and Society at University of California, Berkeley. In 2010, he was Visiting Professor at the School of Law, University of New South Wales. He is currently a Visiting Professor with the Law, Science, Technology and Society Centre at the Vrije Universiteit in Brussels.

His research has focused on the comparative analysis of surveillance technologies and privacy protection policies at the domestic and international levels. In addition to numerous scholarly and newspaper articles, he has published six books: Regulating Privacy: Data Protection and Public Policy in Europe and the United States (Cornell University Press, 1992); Visions of Privacy: Policy Choices for the Digital Age (University of Toronto Press, 1999, co-edited with Rebecca Grant); The Governance of Privacy: Policy Instruments in the Digital Age (The MIT Press, 2006 with Charles Raab); The Privacy Advocates: Resisting the Spread of Surveillance (The MIT Press, 2008); Playing the Identity Card: Surveillance, Security and Identification in Global Perspective (Routledge, 2008 co-edited with David Lyon); and Security Games: Surveillance and Control at Mega-Events. He has completed policy reports on privacy protection for the Canadian government, the Canadian Standards Association, the Privacy Commissioner of Canada, the European Commission, the UK Information Commissioner and others. He is currently the co-investigator of a large Major Collaborative Research Initiative grant entitled "The New Transparency: Surveillance and Social Sorting."

Crime and Punishment in the Cloud
Accountability, Transparency, and Privacy

Stefan Berthold, Simone Fischer-Hübner,
Leonardo A. Martucci, and Tobias Pulls*

Karlstad University
651 88 Karlstad, Sweden
[firstname.lastname]@kau.se

Abstract. The goal of this work is to reason on the complexity of the relationship between three non-functional requirements in cloud computing; privacy, accountability, and transparency. We provide insights on the complexity of this relationship from the perspectives of end-users, cloud service providers, and third parties, such as auditors. We shed light on the real and perceived conflicts between privacy, transparency, and accountability, using a formal definition of transparency and an analysis on how well a privacy-preserving transparency-enhancing tool may assist in achieving accountability. Furthermore, we highlight the importance of the privacy impact assessment process for the realisation of both transparency and accountability.

1 Introduction

The complexity of the relationship between the non-functional requirements privacy, accountability, and transparency in cloud computing is high. They are subjective or social constructs, in the case of privacy, and are regulated mostly by legislation and regulation. Social constructs, legislation, and regulation are aspects that are linked to the cultural background of a country or region. Hence, cloud computing services that are delivered online to a global audience need to consider the local flavours and understanding of the privacy, accountability, and transparency.

In this paper, we address the relation between privacy, accountability, and transparency. We provide insights on the complexity of the relationship between the requirements from the perspectives of end-users, cloud service providers (CSPs), and third parties, such as auditors. All requirements are part of a system of checks and balances based on legislation, regulation, economical factors, and competition between CSPs. We do not consider every possible legislation and regulation, but abstract these local parameters as a set of policies that are defined by the CSPs and are communicated to the end-users and auditors. The complexity of the relationship between the requirements is not reduced, but the

* The authors have received funding from the Seventh Framework Programme for Research of the European Community under grant agreement no. 317550.

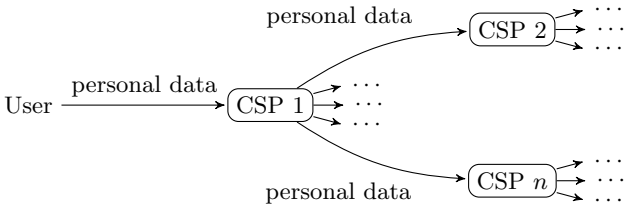

Fig. 1. The flow of personal data into the cloud. The first cloud service provider (CSP 1) offers cloud services to end-users. The personal data of the end-user is forwarded by CSP 1 to other CSPs as parts of the services are outsourced to these CSPs.

representation of local customs and practices is simplified as a set of defined rules. Our conclusions shed light on the real and perceived conflicts between privacy, transparency, and accountability, using a formal definition of transparency and an analysis on how well a privacy-preserving transparency-enhancing tool may assist in achieving accountability. Furthermore, we highlight the importance of privacy impact assessment (PIA) [2] for the realisation of both transparency and accountability.

This paper is organised as follows. Section 2 presents the background. Section 3 provides a formal definition for transparency and opacity. Section 4 presents the relationship between privacy, transparency, and accountability. Section 5 discusses privacy, transparency, and accountability in cloud computing. Section 6 outlines the relationship between all three non-functional requirements from the perspective of a distributed privacy-preserving log trails system for cloud computing. Finally, Section 7 presents the conclusions.

2 Background

A cloud service may be based on other cloud services, platforms or infrastructures. Hence, a user's personal data that is sent to a cloud service provider may be forwarded to other cloud service providers. For instance, a cloud-based application can run on top of a cloud platform that is hosted on top of a cloud-based infrastructure, and the application is a mash-up of other cloud services running on different platforms and infrastructures. We illustrate the complexity of such relationships from the perspective of personal data in Fig. 1.

As cloud computing services become commoditised, a cloud service can be easily replaced or offered by multiple providers simultaneously, e. g., a cloud computing service may store user data in different cloud-based infrastructures. The commoditisation of functional requirements does not result in the commoditisation of the non-functional requirements. CSPs that collect data from users are thus required to negotiate and compose policies in the service chains and are thereby contributing to the ex ante transparency [3] of the user. The commoditisation allows CSPs to offer differentiated services regarding the desired

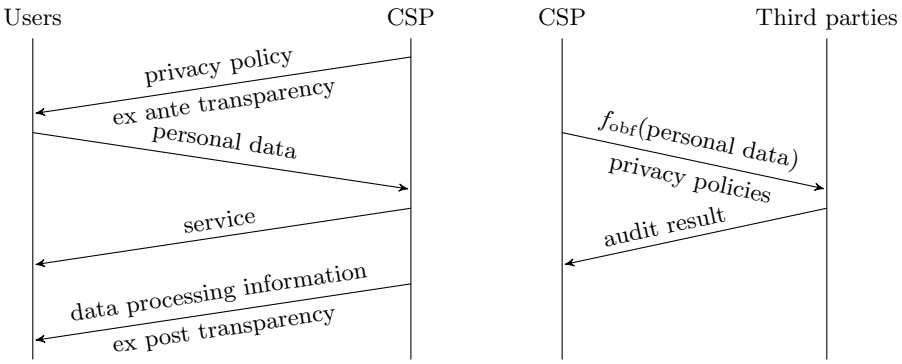

Fig. 2. The relationship between users, cloud service providers (CSP), and third parties, such as auditors or law enforcement. On the diagram to the left, the CSP sends to the users the privacy policy (or agrees upon one) related to the requested cloud service. This step provides users with ex ante transparency. We assume that service provisioning incurs in the transfer of personal identifiable information to the CSP. Ex post transparency [3] is provided by the CSP to the users by offering means for them to verify all the processing information on their personal data. On the diagram to the right, third parties, e. g., auditors or data protection agencies, verify if privacy policies are been executed accordingly by accessing logs that may contain personal data, which is required to be obfuscated to protect the users' privacy.

level of privacy and transparency. However, the flexibility of CSPs to change their subordinate CSPs may diminish, since the privacy policies have to be renegotiated with all actors involved.

The data flows between end-users, CSPs, and third parties are presented as a sequence diagram in Fig. 2. Only data flows that are relevant for accountability, transparency, and privacy are illustrated. Nevertheless, there are additional accountability aspects that are omitted in Fig. 2 for the sake of simplicity. Third parties should be held accountable for their actions regarding the collected data towards the CSP and users, and the CSP is accountable to the third parties, which may represent civil society organisations or governmental agencies. Furthermore, Fig. 2 simplifies some tensions regarding data access by aggregating all users under a single designation. Naturally, users should have access only to the personal data that they own.

3 Transparency and privacy

This section defines the terms transparency and privacy, and discusses their relation. The intuitive meaning of transparency is that nothing is hidden from anyone. In the context of information processing, the scope of the term transparency can be limited to no information is hidden from anyone or, equivalently, all

information is available to everyone. We put this idea in the words of Shannon's information theory [8] and define the term transparency in Definition 1.

Definition 1 (Transparency). *Transparency is the state when every party in the target group possesses perfect knowledge about the observable of interest. In other words, no party in the target group could learn any information (in Shannon's [8] sense) about the observable of interest.*

The observable is an object, a subject, or a process (with inputs and outputs) that can be measured. Its transparency state is determined by the knowledge of all parties in the target group at the same time. Their knowledge has to be perfect. The target group is a group of individuals or information processors that has to be defined for observables of interest before their transparency state can be determined. A party has perfect knowledge, if no fact can be presented to the party that would add to its knowledge. A fact like that would be information in terms of Shannon's information theory.

The observable is opaque, if there is a fact which is information, i. e., a fact that would add to the knowledge of one party. The existence of the fact is sufficient, it does not have to be available for the party. The more information could be learned by one party the greater is the opacity of the observable. We define opacity as a dual to transparency.

Definition 2 (Opacity). *The opacity of the observable of interest is the maximum amount of information one party in the target group could learn about the observable.*

Zero opacity means that every party in the target group possesses perfect knowledge, thus, the observable is transparent. Non-zero opacity implies that at least one party in the target group could learn more about the observable, i. e., add information to its knowledge, and thus the observable is not transparent. Transparency and opacity may vary over time when new information about the observable is created which may not be available to all parties immediately. Thus, transparency and opacity depend on the time of measurement.

In April 2013, the French government made it mandatory for members of the national cabinet to declare their wealth [10]. This can be understood as transparency where the observable is the wealth and the target group is the French society. In this context, transparency for the public and privacy for the state ministers are conflicting objectives.

In data protection (EU Data Protection Directive 95/46/EC), the obligation of the data controller to inform the data subject about the data processing can be understood as transparency where the data processing is the observable and the data subject is the only member of the target group. This does not conflict with the privacy of the data subject as long as the data processing is opaque for everyone except the data subject and the data controller. The term privacy is informally defined in Definition 3.

Definition 3 (Privacy). *Privacy is the right of individuals to control the flow and use of their personal data.*

Privacy as in Definition 3 is also known as the right to informational self-determination. The terms 'control', 'flow', and 'use' mean that individuals are in the position to make informed decisions about data disclosure, storage, and processing, and can impose their decisions on the data controller. This includes the right to minimise the data disclosure (data minimisation), binding the processing of personal data to specific purposes, and deleting the data after specific time periods. Privacy also implies the right of individuals to be informed about the storage and the processing of their personal data. This right is required for making informed decisions.

4 Accountability

This section defines accountability and discusses the relation of it to transparency and privacy. In simple words, accountability is complementing the privacy of individuals with transparency and liability provisions for data controllers. ISO/IEC 29100 puts this in more specific wording.

> Accountability: document policies, procedures and practices, assign the duty to implement privacy policies to specified individuals in the organization, provide suitable training, inform about privacy breaches, give access to effective sanctions and procedures for compensations in case of privacy breaches. [4]

ISO/IEC 29100 provides data controllers with guidelines on how to achieve accountability. We aim to define what accountability is.

Definition 4 (Accountability). *A data controller is accountable, if privacy breaches are transparent to the respective data subjects and the data controller is sanctioned and/or the data subject is compensated in case of privacy breaches.*

Accountability imposes transparency and liability on data controllers. Liability assigs resposibility that may lead to sanctions or compensations. Data controllers that breach privacy store or process personal data of data subjects beyond their the control.

Definition 4 requires the detection of privacy breaches, but does not determine how they are detected. Conceivable are independent third parties, auditors, who check the data processing logs. The auditor would announce the result of the check, i. e., the presence or absence of privacy breaches. However, the public announcement of privacy breaches that are assignable to specific data subjects pose new privacy breaches, since personal data of the first privacy breach is then published in the announcement beyond the control of the data subjects. As a consequence, auditors need to be accountable as well.

An alternative to sending the the full data processing log to the auditor is to send anonymised logs which cannot be used to identify data subjects. An even more fundamental alternative is to send the data processing mechanism as a black box instead of data processing logs. The mechanism can be checked by auditors with random input data. In both cases, the auditors would avoid to commit new privacy breaches.

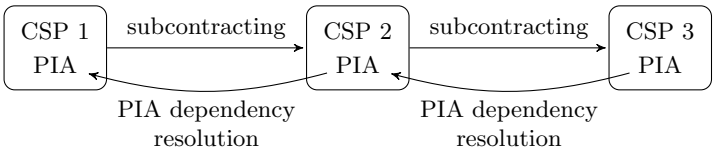

Fig. 3. CSPs are subcontracting the services of other CSPs. Even contracting loops are conceivable. The privacy impact assessment (PIA) of a contractor depends on the outcome of the PIA of the subcontractor.

5 In the cloud

This section discusses transparency, privacy, and accountability in the context of cloud services. In the cloud, cloud service providers (CSPs) may become data controllers and cloud users may become the data subjects. However, cloud services introduce two dimensions that are uncommon in the classic data controller model. On the vertical dimension, each CSP may offer more than one service. On the horizontal dimension, CSPs may be subcontracting services of other CSPs.

The implications of the vertical dimension have been discussed in prior work [5]. Privacy needs to be preserved and transparency to be established for each service independently. The implementation and, if necessary, the trade-off between privacy and transparency must be the result of careful planning, e. g., by applying privacy by design rules [1] or carrying out a PIA. Part of the implementation can be the involvement of third parties who need to be accountable as well, at least if they receive personal data.

On the horizontal dimension, even called the chain of accountability [6], the implementation of privacy and transparency measures are not independent. Again, careful planning has to precede the implementation, in contrast to the vertical dimension, however, the contractor's planning depends on the subcontractors' planning and has to be adjusted whenever the subcontractor is changing its implementation. Fig. 3 illustrates the case for PIAs among subcontracting CSPs.

6 Distributed privacy-preserving log trails

In this section, we look at an example system that was designed with the privacy of end-users in mind. The system is applicable in a cloud setting for making data processing of personal data transparent to end-users.

The goal of the *distributed privacy-preserving log trails* system presented in [7] is to make data processing of users' personal data transparent towards the users whose data is being processed. The system facilitates the transfer of data processing information from CSPs to users while protecting the privacy of the users. Only the information logged for a user is transparent to that user, to all other parties the information is opaque. This is accomplished by cryptographic means, in terms of encryption but also by ensuring that users are only identified

by transaction pseudonyms where both log entries and identifiers are unlinkable. When a user's personal data is spread within the CSP's service chain, as illustrated in Fig. 1, a new transaction pseudonym for the user is generated for each system that performs data processing. The service chain can be both distributed and dynamic, i. e., there is no need to know before data disclosure which or how many data processing systems the CSPs use. Users can anonymously reconstruct and verify the integrity of all descriptions of data processing logged for them across all of the systems that performed data processing as a consequence of the user's disclosure of personal data. These privacy protections minimise the amount of personal data generated by the transparency-enhancing tool, which in turn ensures that using the tool preserves the users' privacy.

Returning to Fig. 2, the system in [7] is suited for providing ex post transparency of data processing towards users. Ultimately, this plays a role in making the CSP accountable towards their users. In [7], the CSP shares the complete set of data with the users, however, the system does not facilitate support for sharing to third parties anything but the complete set of data provided by the CSP to users. The lack of obfuscation makes the system far from ideal, since ideally the personal data shared with third parties should be fully obfuscated, i. e., opaque. There has been some work on obfuscating audit logs, such as [9] in the context of intrusion detection. However, there is a need for future work on minimising the amount of personal data disclosed while still retaining the ability for an auditor to keep a CSP accountable. Furthermore, we note that while the logging system in [7] facilitates ex post transparency of data processing by CSPs towards users, there is still a need for further work on supporting redress once a user learns of data processing which violates the previously agreed to privacy policy. Without redress, e. g., in the form of financial compensation to the user or sanctions towards the misbehaving CSP, the CSP may not be considered accountable.

7 Conclusions

Cloud computing is becoming increasingly complex as services are turning into commodities, easily swapped out and replaced, into dynamic service chains. Making CSPs accountable while respecting the privacy of users is a truly daunting task. This is because in general, accountability, transparency, and privacy are perceived as conflicting goals. In this paper, we have shown that when it comes to *end-user* privacy there is conceptually no conflict with providing transparency and accountability while at the same time respecting the privacy of end users. The CSP should be accountable for privacy breaches.

Towards end users, the CSP can make all processing on a user's personal data transparent. The CSP needs to make sure that the processing is only transparent to the user to whom the personal data belongs while the processing remains opaque to everyone else. This does not constitute a privacy breach, because each user only learns of the processing on their own data. We discussed an example system for realising this kind of transparency in Section 6.

Towards third parties, the CSP only needs to make the privacy breaches transparent, not the personal data of users. This requires that the third parties are able to inspect, at the very least, each processing mechanism the CSP uses to be able to detect breaches. Again, this does not breach the privacy of end-users.

The privacy impact assessment (PIA) as a transparency tool plays a central role, especially in complex and dynamic settings such as cloud computing. PIA is used to uncover privacy issues and possible privacy breaches for the CSP and to convey these issues to other CSPs and end-users. This makes accountability as defined in Definition 4 possible.

If we expand the concept of privacy to include the "privacy" of CSPs, there is a real conflict between privacy, transparency, and accountability. Detecting privacy breaches, in the sense of illegitimate data processing, requires CSPs to make their data processing transparent. Such transparency may reveal intellectual property or trade secrets of the CSPs. This is recognised, e. g., in recital 41 of the EU Data Protection Directive 95/46/EC.

Unlike the moral dilemma presented in Dostoyevsky's *Crime and Punishment*, our work offers a happier ending. Accountability, transparency, and privacy are conceptually realisable without negatively effecting the privacy of end-users. This however comes at the cost of the "privacy" of CSPs, whose data processing needs to become more transparent towards both end-users and auditing third-parties. The question is: Is this morally justifiable?

References

1. Cavoukian, A.: Privacy by design. White paper, Information and Privacy Commissioner of Ontario (2009)
2. Clarke, R.: Privacy impact assessment: Its origins and development. Computer Law & Security Review 25(2), 123–135 (2009)
3. Hildebrandt, M.: Behavioural biometric profiling and transparency enhancing tools. Project Deliverable 7.12, Future of Identity in the Information Science (FIDIS, Network of Excellence within the European Community's 6th Framework Program, No. 507512) (2009)
4. ISO/IEC: Privacy framework. ISO/IEC 29100, ISO/IEC (2011)
5. Pearson, S.: Taking account of privacy when designing cloud computing services. In: Software Engineering Challenges of Cloud Computing, 2009. CLOUD '09. ICSE Workshop on. pp. 44–52 (2009)
6. Pearson, S., Tountopoulos, V., Catteddu, D., Südholt, M., Molva, R., Reich, C., Fischer-Hübner, S., Millard, C., Lotz, V., Jaatun, M., Leenes, R., Rong, C., Lopez, J.: Accountability for cloud and other future internet services. In: 4^{th} IEEE Int. Conf. on Cloud Computing Technology and Science (CloudCom). pp. 629–632 (2012)
7. Pulls, T.: Privacy-preserving transparency-enhancing tools. Licentiate thesis 2012:57, Karlstad University, Department of Computer Science (2012)
8. Shannon, C.E.: A mathematical theory of communications. Bell System Technical Journal 27, 379–423, 623–656 (1948)
9. Sobirey, M., Fischer-Hübner, S., Rannenberg, K.: Pseudonymous audit for privacy enhanced intrusion detection. In: SEC. pp. 151–163 (1997)
10. The Economist: Transparency days. Printed Edition **407** (8832) (20 Apr 2013)

Trusted Clouds

Mike Burmester

Florida State University, Department of Computer Science
Tallahassee, FL 32306, USA
{burmester}@cs.fsu.edu

'*When you have completed 95% of a journey then you are halfway there*' Japanese proverb

Abstract. A new paradigm for network applications emerged in the 1990s as the centralized mainframe computer model evolved into a PC client/server based model. This captured a broader scope including business, commerce and finance. Recent Cloud computing and Big Data deployments suggest that we have now come full circle with centrally managed trust infrastructures supporting an even broader application base for any-time, any-where, synchronized access to data and services. This extends the flexibility/manageability of the client/server paradigm and allows for ubiquitous lightweight service endpoints such as notebooks, tablets or smart phones that do not need to store sensitive data (other than cryptographic keys in "sealed storage").
Even though it may take some time before we understand the full extent of the Cloud paradigm, some features have already emerged and can be analyzed and studied. For example for backward compatibility, legacy practices will be maintained. In particular, cloud deployment models will comprise several technologies including public, private and hybrid. Also, past practices strongly support open virtualization, so clouds can be customized and tailored to specific security settings. Finally, the emerging paradigm will clearly be impacted by social media technologies and the Internet of Things, suggesting that social behavior, profiling and causal reasoning will play a major role.
In this report we analyze the cloud paradigm from a security point of view. Our goal is to show that for critical applications, not only is the new paradigm more flexible, but it is also technically easier to secure. Finally, the Cloud has a dark side, at least from a security point of view. We shall discuss some of its more obnoxious features.

1 Introduction

Cloud computing is an evolving paradigm. It is a technology that supplies on demand computing services as a utility, with price elasticity, continuity of service, quick scaling and reliability. NIST defines it as [1]: "A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.*, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

Below we briefly overview the cloud models, the provided services and the service agreements (for more details see [2]).

Models. There are four general types of cloud deployment models: public clouds, that supply infrastructure and computational resources to the general public over the Internet, and are owned and operated by cloud providers; community clouds that are owned and operated by several organization, but have common regulatory and security policies; and hybrid clouds.

Services. There are three basic cloud computing services on demand: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). The cloud client typically chooses the operating system and development environment to host the services. Service agreements specify the terms and conditions for access to cloud services For most cloud technologies security provisions that go beyond the basic infrastructure services are carried out by the cloud client.

Service agreements. These specify the terms and conditions for using cloud services, which includes the expected level of service—the Service Level Agreement (SLA), and the compensation if that level is not reached, licensing details as well as security and privacy.

Related Work. Most of the cloud computing publications in the literature focus on the "computing as a utility" business service (*e.g.,* [3–7]). There are only a few publications that address security issues in the Cloud (*e.g.,* [2, 8, 9]), and these use a fragmented approach.

2 Cloud architectures for secure applications

The Cloud is a client-driven access control infrastructure that manages computing services. A cloud Monitor mediates between clients and service providers with access granted based on service agreements that establish a trust-bond between clients and providers.

2.1 Cloud Monitors

A cloud Monitor can be modelled by a trust-graph $G = (V, E)$. G is a directed labeled graph with nodes $X, Y, Z, \ldots$, the clients, the cloud providers and the cloud services. There are two types of edges: (a) edges $X \xrightarrow{\tau_{xy}} Y$ that link clients X to providers Y with labels τ_{xy} that contain: an SLA, terms of use, privacy/security policies and the compensation in the event the provider fails to deliver at the specified level or violates agreed policies; (b) edges $Y \xrightarrow{\tau_{yz}} Z$ that link providers Y to services Z with labels τ_{yz} that contain: the agreement regarding the particular service Z, privacy/security policies and the compensation if Z is not delivered at the specified level or agreed policies are violated.

Labels of the type τ_{xy} capture the confidence the client has in the provider regarding specific services as well as the risks involved (a function of the criticality of the service and the agreed compensation). Labels of the type τ_{yz} capture the confidence that the client has in the specific service Z.

Trust is not transitive: $X \xrightarrow{\tau_{xy}} Y$ and $Y \xrightarrow{\tau_{yz}} Z$ implies $X \xrightarrow{\tau_{xz}} Z$ only when the service agreement of τ_{yz} is specified in the description of τ_{xy} as a required service. In this case we say that τ_{xy} dominates τ_{yz} and write $\tau_{xy} \succeq \tau_{yz}$. Access to a service Z provided by Y is granted to client X if $\tau_{xy} \succeq \tau_{yz}$. For private clouds, trust labels can be much simpler reducing to, for example, public key certificates, or symmetric keys.

The trust-graph G is dynamic with edges added (deleted) in real-time corresponding to new service requests (completions) or new services becoming available (withdrawn).

2.2 Access control models

Access control models are trust infrastructures that manage the resources of computer or network systems. Bell-LaPadula [10] was the first proposed access control model. It enforces need-to-know (confidentiality) policies. Other models followed. Biba [11] enforces integrity policies; Clark-Wilson [13] enforces separation of duties (integrity) policies; and Role Based Access Control (RBAC) [12] enforces authorization policies. In these models, clients and resources are assigned labels selected from a linearly ordered set (or lattice) and access is based on domination. For example, in Bell-LaPadula a client with "secret" label (clearance) can access all resources with label (classification) "secret" or less.

These models all focus on managing data resources, *not* computing services that are functions of data. For cloud deployments we have to design new access control models and specify new policies for the secure management of computing services. In this report we propose to use the trust levels τ in Section 2.1 as labels, appropriately modified to capture dynamic management and policies that enforce need-to-know and separation-of-duties.

For cloud deployments need-to-know refers to the trust τ_{xz} required for accessing a particular computing resource Z: it should be no more than strictly necessary. For example, a client and provider need not share any secret encryption keys if private channels are not necessary for the service. If secret keys are needed (*e.g.,* for integrity) then these must be session keys. If long term keys have to be shared then these must be public keys.

Separation of duties refers to the trust τ_{yz} between a provider Y and the computing service Z: it should be no more than strictly necessary. In particular the provider should not be able to access data or secret keys of the client. For example, for an Infrastructure-as-a-Service application, the cloud provider should not get access to any data or secret keys that the IaaS shares with the cloud client.

2.3 Trusted Computing

The Trusted Computing Group [14] has published specifications for architectures and interfaces for several computing implementations. Platforms based on these are expected to meet the functional and reliability requirements of computer systems and provide increased assurance of trust. The Trusted Platform Module (TPM) [15] and the Trusted Network Connect (TNC) [16] are two such architectures.

The TPM is a Trusted Computing (TC) architecture that binds data to platform configurations of hardware systems to enhance software security. It has two basic capabilities: remote attestation and sealed storage, and is supported by a range of cryptographic primitives. TPMs employ trusted engines, called *roots of trust*, to establish trust in the expected behavior of the system. Trust is based on an integrity protected boot process in which executable code and associated configuration data are measured before execution—this requires that a hash of the BIOS code is stored in a Platform Configuration Register (PCR).

For remote attestation the TPM uses an attestation identity key to assert the state of the current software environment to a third party—by signing PCR values. Sealed storage is used to protect cryptographic keys. To encrypt/decrypt/authenticate, keys are released conditional on the current software state (using current PCR values). The TPMs must be physically protected from tampering. This includes binding the TPM to physical parts of the platform (*e.g.* the motherboard).

The TNC is a TC architecture for trusted network applications. What distinguishes TNC from other interoperability architectures is the requirement that the OS configuration of the client and server is checked prior to a communication channel being established. A trusted link between a client and server is established only if: (*i*) the identity of the client and server is trusted. A Public Key Infrastructure is used to establish trust-links between a Root Authority and the TPMs of the client/server; (*ii*) the client has real-time access to the server; (*iii*) the client and server are authenticated. A root of trust on the TPM of both parties is invoked to release the required keys to execute a handshake protocol [16]; (*iv*) the integrity of communicated data, and if necessary the confidentiality, is enforced by the TPM.

The TC paradigm has been studied extensively, with TPM- and TNC-compliant systems implemented in several configurations. There are some concerns regarding implementations, which mainly involve poor design: the TC paradigm relies heavily on strict compliance to policies, procedure and hardware design, and unless these are being adhered to, there is no protection. Other concerns involve "Big Brother" privacy issues. However for critical applications or DoD type networks, implementation issues and privacy leakage can be addressed.

2.4 A threat model and security framework for TC-compliant systems

The TPM prevents compromised components of a TC-compliant system from executing. As a result, if we exclude run-time (execution) threats, malicious

(Byzantine) threats are reduced to DoS threats that can be addressed with redundancy.

There are two kinds of faults that may affect a TC-compliant computer system: natural (this includes accidents) and adversarial (intentional/malicious/insider). Natural faults can be predicted, in the sense that an upper bound on the probability of such faults can be estimated. Redundancy can then be used to reduce this probability to below an acceptable threshold. Malicious DoS faults cannot be predicted. However they are overt and, because of the TPM and TNC integrity verification, must be physical (*e.g.*, involve tampering the TPM chip). So there is a cost involved. One way to thwart them is to make the cost high enough to prevent them.

There are several security models that use economics and risk analysis based on redundancy [17] that are appropriate for threat models with overt faults. These assume a bound on adversarial resources and an architecture with sufficient redundancy to make such DoS attacks prohibitively expensive.

2.5 The good, the bad and the ugly

The good. The TPM protects system components from behaving in an unexpected way. In particular, prior to the execution of any trusted program an integrity check of its state (against a stored PCR configuration) is required. Consequently if the program is compromised it will not be executed by the OS.

The bad. The TPM allows only trusted code to execute. Therefore the integrity of trusted code (which includes the OS) is a fundamental requirement in order to ensure trust in the computing infrastructure. The system software must be well designed, with no security holes backdoors or vulnerabilities that could be exploited by an adversary. An exploit in the OS may allow the adversary to bypass the protection offered by the TPM. There are several reasons why the design of software programs may be faulty. A major reason is the complexity of the execution environment (the OS and CPU hardware). Another is poor software development practices.

The ugly. "*Security is not necessarily composable*". Proof-carrying code is not closed with respect to composability unless the proofs are composable (Universal Composability [18]). An interesting example involving routing protocols is discussed in [19], where it is shown that a routing protocol that is secure in isolation is not secure when executed concurrently with itself. Consequently the TPM provides integrity guarantees only at load-time, not run-time.

An exploit of the OS may make it possible for the adversary to change the execution flow of a trusted program. There are several run-time attacks [20] that use metamorphic malware such as the self-camouflaging Frankenstein [21] or more generally, return oriented programming (ROP) [22]. For these the adversary must be able to control the execution flow on the stack, and there are ways to prevent this [23].

However as pointed out earlier, even if there are no exploits, concurrent execution of trusted code (that is not Universally Composable) may lead to untrusted behavior.

2.6 An Architecture for Trusted Clouds

The basic components of a Cloud are: the clients, the providers, the computing services and the cloud Monitor. For a Trusted Cloud we propose an architecture with:

- A private cloud deployment and trusted service providers.
- A trusted cloud Monitor (Section 2.1).
- An access control model for computing services that supports need to know and separation of duties policies (Section 2.2).
- TC-compliant computing services (Section 2.3).
- Lightweight TC-compliant client service endpoints.

The private cloud deployment is intended to secure computing services for critical infrastructures and DoD type networks. This deployment should not be used in hybrid mode, or concurrently with other clouds. All service providers should be trusted to adhere to service agreements as well as the security policies. The cloud Monitor should enforce need-to-know and separation of duties policies. All computing services should be TC-compliant. This prevents execution of untrusted code, while guaranteeing adherence to the service agreements. The requirement for lightweight TC-compliant service endpoints is based on the fact that the Trusted Cloud is the most appropriate place to store sensitive data (from physical and cyber threats). Ideally a lightweight (such as TinyOS [27]) operating system should be used—all the code that is needed can be run on a PaaS.

Assuming that all the components of the Cloud are trusted, and that all execution code is trusted, the only remaining (load-time) threats are DoS attacks, which because of the redundancy in the Cloud are not a concern. For applications in which real-time access is critical, services may have to be prioritized. The system must have enough redundancy to guarantee that all critical computing services are executed in real-time.

3 The Dark Side of the Cloud

Well defined architectures that are based on trusted system behavior in the presence of an adversary will be secure unless the trust is breached. By assuming that all service providers are trusted, and that any computing service will not deviate from its expected behavior (because of the TC controls), we make certain that the only remaining threats are those that bypass the trust mechanisms. From our discussion in Section 2.5 (the ugly case) it is clear that concurrent execution of trusted codes may lead to untrusted (run-time) system behavior. To mitigate such threats, any successful approach will have to: (a) limit the

openings for exploitation on platform software and, (b) employ methods to detect run-time compromise.

(a) To achieve a smaller attack surface, client endpoint devices must abide by constraints on functionality and resource usage, operating with a structured, well-defined, enumerated set of duties. Clearly the presence of software flaws is related to the complexity and size of software.
(b) There is substantial existing work on techniques for dynamically detecting code faults (dynamic integrity monitoring and taint analysis) [24–26]. Although most solutions carry a significant computational overhead, critical applications can justifiably be expected to bear the computational resources. However, the time required to address such threats may be an issue.

Acknowledgments. This material is based upon work supported by the National Science Foundation Grant No. 1027217.

References

1. P. Mell and T. Grance, "The NIST Definition of Cloud Computing", Publication 800-145, 2011. `http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf`
2. W. Janson and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing", NIST Publication 800-144, 2011. `http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf`
3. S. K. Garg, S. Versteeg, and R. Buyya, "A framework for ranking of cloud computing services," *Future Generation Comp. Syst.*, vol. 29, no. 4, pp. 1012–1023, 2013.
4. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, Apr. 2010.
5. T. Velte, A. Velte, and R. Elsenpeter, *Cloud Computing, A Practical Approach*, New York, NY, USA: McGraw-Hill, Inc., 2010.
6. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Comp. Syst.*, vol. 25, no. 6, pp. 599–616, 2009.
7. A.-M. K. Pathan, J. Broberg, and R. Buyya, "Maximizing utility for content delivery clouds," in *WISE*, ser. Lecture Notes in Computer Science, G. Vossen, D. D. E. Long, and J. X. Yu, Eds., vol. 5802. Springer, 2009, pp. 13–28.
8. R. H. K. Yanpei Chen, Vern Paxson, "Whats New About Cloud Computing Security? CS Division, EECS Dept. UC Berkeley, TR UCB/EECS-2010-5."
9. B. R. Kandukuri, R. P. V., and A. Rakshit, "Cloud security issues", in *IEEE SCC*. IEEE Computer Society, 2009, pp. 517–520.
10. E. D. Bell and J. L. La Padula. Secure computer system: Unified exposition and Multics interpretation. Bedford, MA, 1976.
11. K. J. Biba. Integrity considerations for secure computer systems. MITRE Corp., Tech. Rep., 1977.
12. R. S. Sandhu, E. J. Coyne, and C. E. Feinstein, H. L.and Youman Role-Based Access Control Models. *IEEE Computer*, vol. 29, no. 2, pp. 38–47, 1996.

13. D.D. Clark and D.R. Wilson. A Comparison of Commercial and Military Computer Security Policies. newblock *Proc. IEEE Symp. on Research in Security and Privacy* (SP'87), May 1987, Oakland, CA. IEEE Press, pp. 184–193.
14. Trusted Computing Group (TCG), "http://www.trustedcomputinggroup.org/."
15. TCG, "TPM Structures, Level 2, Version 1.2, Revision 116, Communication networks and systems for power utility automation", *http://www. trustedcomputinggroup. org/resources/tpm_main_specification*, March 2011.
16. ——, "Trusted Network Connect Architecture for Interoperability; Specification 1.3; Revision 6," April 2008.
17. M. Lelarge and J. Bolot, "Economic incentives to increase security in the internet: The case for insurance," *INFOCOM 2009*, pp. 1494–1502, 2009.
18. R. Canetti, "Universally composable security: A new paradigm for cryptographic protocols," in *FOCS*. IEEE Computer Society, 2001, pp. 136–145.
19. M. Burmester and B. de Medeiros, "On the security of route discovery in manets", *IEEE Trans. Mob. Comput.*, vol. 8, no. 9, pp. 1180–1188, 2009.
20. A. Baratloo, N. Singh, and T. Tsai, "Transparent run-time defense against stack smashing attacks," in *Proceedings of the annual conference on USENIX Annual Technical Conference*, ser. ATEC '00, Berkeley, CA, USA: USENIX Association, 2000, pp. 21–21.
21. V. Mohan and K. W. Hamlen, "Frankenstein: Stitching malware from benign binaries," in *WOOT*, E. Bursztein and T. Dullien, Eds. USENIX Association, 2012, pp. 77–84.
22. R. Roemer, E. Buchanan, H. Shacham, and S. Savage, "Return-Oriented Programming: Systems, Languages, and Applications," *ACM Trans. Inf. Syst. Secur.*, vol. 15, no. 1, pp. 2:1–2:34, 2012.
23. Davi, Lucas and Sadeghi, Ahmad-Reza and Winandy, Marcel, "Ropdefender: a detection tool to defend against return-oriented programming attacks," in *Proc. 6th ACM Symposium on Information, Computer and Communications Security* (ASIACCS '11), New York, NY, USA: ACM, 2011, pp. 40–51.
24. Walter Chang, Brandon Streiff, and Calvin Lin. Efficient and extensible security enforcement using dynamic data flow analysis. In *ACM Conference on Computer and Communications Security*, pages 39–50, 2008.
25. W. Cheng, Qin Zhao, Bei Yu, and S. Hiroshige. Tainttrace: Efficient flow tracing with dynamic binary rewriting. In *11th IEEE Symposium on Computers and Communications, 2006. ISCC '06*, pp. 749–754, 2006.
26. Feng Qin, Cheng Wang, Zhenmin Li, Ho seop Kim, Yuanyuan Zhou, and Youfeng Wu. Lift: A low-overhead practical information flow tracking system for detecting security attacks. In *Microarchitecture, 2006. MICRO-39. 39th Annual IEEE/ACM International Symposium on*, pages 135 –148, dec. 2006.
27. TinyOS, http://www.tinyos.net/

Towards a Model of Accountability for Cloud Computing Services

Daniele Catteddu[1], Massimo Felici[2], Giles Hogben[1], Amy Holcroft[2], Eleni Kosta[3], Ronald Leenes[3], Christopher Millard[4], Maartje Niezen[3], David Nuñez[5], Nick Papanikolaou[2], Siani Pearson[2*], Daniel Pradelles[2], Chris Reed[4], Chunming Rong[8], Jean-Claude Royer[6], Dimitra Stefanatou[3], Tomasz Wiktor Wlodarczyk[7]

[1]Cloud Security Alliance, [2]Hewlett-Packard, [3]Tilburg University, [4]Queen Mary - University of London, [5]Universidad de Malaga, [6]Ecole des Mines – Nantes, [7]University of Stavanger

Abstract. This paper presents a model of accountability for cloud computing services, based on ongoing work as part of the A4Cloud project[1]. We define a three-layer model of accountability as a general concept for data governance, distinguishing between accountability attributes, accountability practices, and accountability mechanisms and tools.

1 Introduction

Accountability is an important but complex notion that encompasses the obligation to act as a responsible steward of the personal information of others, to take responsibility for the protection and appropriate use of that information, to be transparent (give account) about how this has been done and to provide remediation and redress. This notion is increasingly seen as a key market enabler in global environments and in helping overcome barriers to cloud service adoption. However, the relative complexity of the service provision chain makes it very challenging both legally and technically to provide accountability for and in the cloud. We propose a co-designed approach that encompasses legal and regulatory mechanisms and a range of technological enhancements that can provide the necessary basis for initiating and sustaining trustworthy data processing and a trusted relationship between data subjects, regulators and cloud service providers.

We define a three-layer model of accountability as a general concept for data governance, distinguishing between accountability attributes, accountability practices, and accountability mechanisms. Accountability attributes are the concepts from which accountability is built, and these are drawn from an extensive survey of the literature;

[1] The A4Cloud project is targeted at EU Framework 7 Call 8 Objective ICT-2011.1.4 Trustworthy ICT, and particularly on objective (c) (i.e. data policy, governance and socio-economic ecosystems). See http://www.a4cloud.eu/.

* Corresponding author

they include responsibility, liability, transparency, observability, verifiability, sanctions, provision of assurance and satisfaction of obligations.

Accountability practices are sets of behaviours that an organisation should have in order to be accountable, and are distinguished into four broad categories:

1. defining governance to comply in a responsible manner with internal and external criteria,
2. ensuring the implementation of appropriate actions to actualise such governance,
3. explaining and justifying those actions, namely, demonstrating regulatory compliance,
4. remedying any failure to act properly.

These are closely aligned to the definition of accountability used by the project.

Accountability mechanisms are procedures and tools – often technical tools, including software, but also organisational and/or legal procedures and other mechanisms – by which accountability practices are supported and implemented.

There are numerous references to accountability in regulatory frameworks, and these are surveyed in this document. The most relevant opinions expressed by the EU's Article 29 Working Party (an independent advisory body on the interpretation of the data protection framework set up under article 29 of Directive 95/46/EC) as well as the European Data Protection Supervisor (EDPS), among others, are described. In addition, data governance best practices, as well as risk assessment guidance for the handling of personal data by organisations, are surveyed. Definitions and models of accountability used in computer science are also reviewed, from high-level presentations to low-level cryptographic models used for proving properties about systems.

The problems presented by cloud service provision ecosystems, and how they may be addressed by an accountability approach, are considered; these include multi-tenancy, the dynamic, ever changing environment, data duplication, and easy access to data from multiple locations. This paper is structured as follows. Section 2 proposes our definitions of accountability in the cloud. Section 3 describes an accountability model based on the given definitions. Section 4 draws some concluding remarks.

2 Proposed Definitions of Accountability in the Cloud

The following definition captures a shared understanding of accountability based on reviewing previous related work and discussion within the project:

> **Conceptual Definition of Accountability:** *Accountability consists of defining governance to comply in a responsible manner with internal and external criteria, ensuring implementation of appropriate actions, explaining and justifying those actions and remedying any failure to act properly.*

Governance here is the processes which devise ways of achieving accountability. The conceptual definition of accountability encompasses different understandings drawn from different disciplines. It is intentionally generally applicable across differ-

ent domains. Further to this generic definition, we tailor the conceptual definition of accountability to the domain of focus of the A4Cloud Project, namely to data protection in the cloud [1]. Thus, the following A4Cloud definition contextualises the notion of accountability (that is, the Conceptual Definition of Accountability) and makes it relevant to the scope of the project:

> **A4Cloud Definition of Accountability:** *Accountability for an organisation consists of accepting responsibility for the stewardship of personal and/or confidential data with which it is entrusted in a cloud environment, for processing, storing, sharing, deleting and otherwise using the data according to contractual and legal requirements from the time it is collected until when the data are destroyed (including onward transfer to and from third parties). It involves committing to legal and ethical obligations, policies, procedures and mechanisms, explaining and demonstrating ethical implementation to internal and external stakeholders and remedying any failure to act properly.*

The definitions highlight the main conceptual aspects of accountability. They characterise the necessary practices emerging in organisations that take an accountability-based approach, with respect to specific attributes supporting accountability.

3 A Model of Accountability in the Cloud

An analysis that deconstructs the accountability definitions introduced in the previous section highlights a model consisting of *accountability practices*, *attributes*, *mechanisms and tools*, as discussed further below. Figure 1 shows the relationships between these aspects of accountability, and how together they form a model.

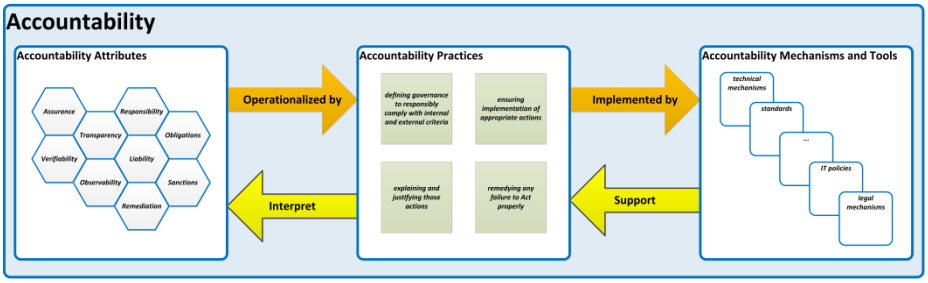

Figure 1 Accountability Attributes, Practices, Mechanisms and Tools

The central elements of this model are:

- **Accountability attributes** – conceptual elements of accountability as used across different domains (i.e. the conceptual basis for our definition, and related taxonomic analysis)
- **Accountability practices** – emergent behaviour characterising accountable organisations (that is, how organisations operationalize accountability or put accountability into practices)
- **Accountability mechanisms and tools** – diverse mechanisms and tools that support accountability practices (that is, accountability practices use them).

Next we shall consider these elements further in turn.

3.1 Defining Accountability Attributes

In order to interpret accountability clearly, we need to distinguish between *accountability practices* and *accountability attributes* (as shown in Figure 1). Accountability attributes encompass concepts that are considered part of and supporting accountability. Typical attributes, among others, include assurance, liability, remediation, responsibility and transparency. The identified attributes stem directly from the definitions of accountability. There exist emerging relationships (e.g. implication and inclusion) among attributes dependent on different viewpoints of analysis (which are related to different accountability perspectives, for instance, like societal, legal and ethical perspectives).

For instance, from a legal perspective, responsibilities imply obligations, which consequently may involve sanctions. From a social perspective, transparency implies both observability and verifiability (and vice versa, transparency is obtained by combining observability and verifiability). Accountability attributes are concepts that relate strongly to accountability. These include: key properties of accountability (e.g. transparency); conceptual elements (e.g. remediation); consequences (e.g. sanctions); related objects (e.g., obligations, insurance).

Obligations prove to be very important in terms of discussion of accountability within service provision networks.

> **Obligation:** An obligation is a requirement, agreement or promise for which there are certain consequences if it is breached. It can be one of three main types: contractual, regulatory, and normative (i.e. derived from social norms).

Other types of obligations, such as user preferences, could fit under these different categories in different contexts; for example, in some contexts user preferences might create a legal obligation but in others they do not.

Other relationships may exist depending on the operationalization of accountability by organisational practices in different domains. It would be also of interest to extend the analysis of accountability to other related concepts and their relationship to accountability: *Access control, Attribution, Audit, Contract, Control, Data protection, Data stewardship, Demonstration, Evidence, Immutability, Non-repudiation, Penalty, Privacy, Privacy by design, Privacy impact assessment, Redress, Risk and Trust.*

> **Responsibility:** Responsibility may be defined as the state of being assigned to take action to ensure conformity to a particular set of policies or rules.

Attribution of responsibility is a key element of accountability, as is apparent from definitions given in dictionaries, which tend to centre on accountability as the quality or state of being held to account for one's actions and an obligation or willingness to accept responsibility for one's actions – for example: *"Accountability is the obligation and / or willingness to demonstrate and take responsibility for performance in light of agreed upon expectations. Accountability goes beyond responsibility by obli-*

gating an organisation to be answerable for its actions" [2]. Specifically, an accountable organisation is responsible for the stewardship of personal and/or confidential data with which it is entrusted.

Attributability: Attributability describes a property of an observation that discloses or can be assigned to actions of a particular actor (or system element).

Accountability can be regarded as an extension of attributability when the action is governed by regulations [3]. This is related to liability since in order for liability to function, it must be attributable to a legal or natural person. In case of a deviation from the expected behaviour (fault), accountability should provide attribution in that it reveals which component is responsible [4].

Evidence is also important in the context of attributability (and hence liability), and thereby in proving non-compliance to governing rules, as well as compliance to governing rules. These governing rules could include obligations in the sense that we use them below, i.e. including legal requirements, contractual requirements and stakeholder requirements (including normative expectations about behaviour).

Liability: Liability is the state of being liable (legally responsible).

Correspondingly, a liable entity is an entity which is legally responsible for the (legal) consequences of a certain action. Often losses (including intangible losses) will trigger liability. The entity that is held liable is then responsible for financial redress, legally termed damages. Hence liability may trigger an obligation to pay damages. Other forms of liability include criminal liability and other statutory liability (e.g. on the basis of data protection regulation). For example, if failure to report incidents results in a fine of 2% of total wealth and Bob is liable for reporting incidents, then if an incident is not reported, Bob is liable to a value of 2% of his total wealth for failure to report incidents. Liability is an element of almost every definition of accountability. For example, Koppell's five elements of accountability include [5]: *"Liability: Did the organisation face consequences for its performance?"* An accountable organisation may be held responsible in respect to violation of the obligations (cf. policies) that they have defined, and as a result have liability imposed on it. According to the A4Cloud definition, accountability extends liability in the sense that ethical elements are introduced when determining obligations.

Sanctions: Sanctions are the (legal) consequences of failing to comply with some requirement.

In the context of data protection, the legal consequences deriving from the lack of respect towards certain obligations lead to different forms of sanctions that are imposed by the member states to the accountable entities, ranging from court decisions to administrative measures.

Sanctions have a *post hoc* effect, they place a (financial) burden on the punished entity, and an *ex ante* effect, fear of being punished promotes compliant behaviour. Strong sanctions encourage adequate investment in an accountability-based approach;

not only do there need to be strong penalties in case of failure to act properly, but they strengthen the motivation for an organisation to take an accountability-based approach if the organisation is treated more leniently if it can be demonstrated that it has tried to ensure implementation of appropriate actions. The importance of holding to account is shown in this quotation from [6]: *"A vital theme is Accountability. Primary responsibility must be placed on organisations to get it right and they must be held to account if they get it wrong. Organisations must deploy the right technology and have a privacy-by-design approach at the heart of their plans."* Similarly, the working definition of an accountable entity given in [7] stresses this element as it is given in terms of *punishment*: *"An entity is accountable with respect to some policy (or accountable for obeying the policy) if, whenever the entity violates the policy, then with some non-zero probability it is, or could be, punished."*

Assurance: Assurance is a positive declaration intending to give confidence.

Assurance can take the form of evidence. An accountability system can produce evidence that can be used to convince a third party that a fault has or has not occurred [4]. In the context of accountability, assurance could refer to provision of *ex ante* evidence for compliance to governing rules, and possibly also to evidence that the governing rules and other factors provide appropriate grounds for trustworthiness. The Galway project includes in its definition of essential elements of accountability [2]: *"systems for internal, on-going oversight and assurance, reviews and external verification"*. An accountable organisation should provide assurance in order to demonstrate to relevant stakeholders (both internal and external to that organisation) that it has defined governance appropriately, implemented actions appropriately, and to explain and justify those actions.

Transparency: Transparency is the property of an accountable system that it is capable of "giving account" of, or providing visibility of, how it conforms to its governing rules and commitments.

A very broad definition of transparency is that it involves operating in such a way as to maximise the amount of and ease-of-access to information which may be obtained about the structure and behaviour of a system or process. For example, a cloud provider offers transparency of its security processes if it provides a web page with current and historical availability. It provides further transparency if it offers explanations for outages. However, this definition is too broad in the sense that it is used as a component of accountability, as there might be a conflict between such maximal openness and the obligation to have appropriate technical and organisational security measures in place to protect personal data. More specifically, the focus of transparency as an attribute of accountability is on *'ex ante transparency'* that should enable the anticipation of consequences before data are actually disclosed (usually with the help of privacy policy statements), and on *'ex post transparency'* that informs about consequences if data already has been revealed (i.e. what data are processed by whom and whether the data processing is in conformance with negotiated or stated policies) [8].

Transparency encompasses the property of an accountable system that it is capable of "giving account" of, or providing visibility of how it conforms to its governing rules and commitments: "*Information Accountability means that Information usage should be transparent so it is possible to determine whether a use is appropriate under a given set of rules"* [9]. More broadly, an accountable organisation is transparent in the sense that it makes known to relevant stakeholders the policies defined about treatment of personal and/or confidential data, can demonstrate how these are implemented and provides appropriate notifications in case of policy violation, as well as responding adequately to data subject access requests. Note that transparency does not involve revealing the personal and/or confidential data itself, as that should be kept confidential, with the exception that data subjects have the right to access their own data (cf. data subject access). This is analogous to the privacy principle of transparency, which is about the need for transparency of privacy policies and not of the personal data (e.g. as elucidated in the OECD privacy guidelines [10].

Remediation: Remediation is the act or process of correcting a fault or deficiency.

In IT literature, remediation generally refers to being able to restore systems to earlier states in case of system failures, which may require going back many months for a known-good configuration. In relation to data and security breaches, remediation is part of the *incident response*, *notification*, and *remediation*. When harm occurs due to a failure of an organisation's privacy practices or to a lapse in its compliance with its internal policies, individuals should have access to a recourse mechanism [2], which can be triggered by an incident report. The organisation acts upon the incident report by notifying the relevant stakeholders (e.g. affected data subjects, regulators, services elsewhere in the service chain) and by repairing the damages. This may involve restoring data to the state prior to the incident, but also support forensic recording of incident data. In a broader context remediation also relates to legal remedies. When data are lost or misused, users may suffer financial damage. Remediation in this sense may refer to claiming compensatory damages or even punitive damages.

In the context of accountability, the accountable organisation is required to take corrective action in case of failure to apply governing rules and honour commitments. This is one of the five elements of accountability mentioned by the Galway project [2]. Remediation is also explicitly specified in our definition of accountability.

Verifiability: Verifiability is a property of an object, process or system that its behaviour can be verified against a requirement or set of requirements.

Quality or level of verifiability depends directly on the available evidence [11]. It is important to notice that some argue that verifiability can be purposefully limited in the contract specification [12]. A closely related notion is *validation*, which relates to the property of accountability whereby it allows users, operators and third parties to verify a posteriori if the system has performed a data processing task as expected [4]. Similarly, *verification* is a process that evaluates whether a system complies with related governing regulations [13], and in the context of accountability is the ability to

provide *ex post* evidence for compliance to governing rules (again mentioned by the Galway project [2]).

> **Observability:** Observability is a property of an object, process or system which describes how well the internal actions of the system can be described by observing the external outputs of the system.

The term observability originates from control theory and was introduced by Kalman in [14]. While the formal matrix-based definitions of system observability might be difficult to directly apply to service accountability, they do offer a strong and useful basis for guiding metric definition and construction of framework of evidence. Particularly of interest is a related weaker term *detectability*. Detectability is a property that assumes that all unobservable elements are stable, that is, they do not change the outputs of the system [15]. Observability may have additional effects. Experiments in the psychology of economics have shown that a considerable improvement in contribution towards a public good (which could also include responsible data stewardship) can be achieved by increasing the degree to which a human process is observable – see, for example, [16]. The strong link between accountability and deterrence is also brought out within [7].

> **Responsiveness:** being responsive to your public's viewpoint and debates, being familiar with its key influences and styles, and aware of its ideas and frames of reference is an essential part of being accountable.

When developing tools or mechanisms to demonstrate accountability, being responsive entails that these mechanisms and tools take into account the specific circumstances and practices within which these mechanisms and tools are implemented. The mechanisms and tools that entail such responsiveness are more likely to have a greater trickle-down effect and therefore more efficient.

3.2 Accountability Practices

In accordance with the conceptual definition of accountability, accountable organisations need to define and implement appropriate governance mechanisms relating to treatment of personal data and/or confidential data. They need to explain what actions are taken, particularly in the sense of demonstrating regulatory compliance. In particular, they need to provide transparency of those actions in order to show that stakeholders' expectations have been met and that organisational policies have been followed. Moreover, they need to remedy any failure to act properly, for example, notifications (to the affected data subjects and/or regulators), redress to affected data subjects or organisations (e.g. sanctions intend to discourage inappropriate behaviour), even in global situations where multiple cloud service providers are involved.

Accountability practices, derived directly from the definitions given, characterise emerging behaviour (highlighting operational and organisational goals to be met) manifested in accountable organisations:

- **defining governance to responsibly comply with internal and external criteria**, particularly relating to treatment of personal data and/or confidential data
- **ensuring implementation of appropriate actions**
- **explaining and justifying those actions**, namely, demonstrating regulatory compliance, that stakeholders' expectations have been met and that organisational policies have been followed
- **remedying any failure to act properly**, for example: notifying the affected data subjects or organisations, and/,or providing redress to affected data subjects or organisations, even in global situations where multiple cloud service providers are involved.

In the context of A4Cloud, the actions in question pertain to the collection, storage, processing and dissemination of personal and/or confidential data by cloud service providers and associated actors. More specifically, the A4Cloud definition of accountability enhances these aspects to include a focus on the treatment of personal and/or confidential data in cloud environments. It highlights the need for management of data across the whole data lifecycle (from the time it is collected until and including the destruction of the data). The ethical nature of an accountability-based approach and the organisational obligations that result from taking this approach represent a shift from reactive to proactive governance of personal and/or confidential data. Organisations commit to the stewardship of personal and/or confidential data by addressing legal and ethical obligations. In order to do so, they deploy and use different mechanisms and tools (e.g. policies, procedures, standards), take account of social norms, provide evidence to internal and external stakeholders, and remedy any failure to act properly.

3.3 Accountability Mechanisms and Tools

The **accountability mechanisms and tools** referred to above are to be understood as concrete tools and techniques supporting accountability practices; in a broader social science sense, these may be thought of as accountability objects. These include, for example, IT security controls and policies as well as technical mechanisms, standards, legal mechanisms, financial penalties and insurance.

Some of these mechanisms and tools will be developed by A4Cloud; others are available from other parties. Depending upon the context, they may be used individually, or in combination. Organisations may select from different alternatives: for example, they may choose to use the Privacy Level Agreement format specified within CSA [17] to express privacy-related obligations, or the Cloud Trust protocol [18] to ask for and receive information from cloud service providers about the elements of transparency, or they may take another approach to do so.

4 Concluding Remarks

This paper describes a model of accountability in the context of data governance for cloud computing services. It is the first to present the A4Cloud project's definitions of accountability, which will form the basis of further discussion and analysis.

5 References

1. Mell, P., Grance, T. (2011). The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September.
2. Center for Information Policy Leadership (CIPL) (2009) 'Data protection accountability: the essential elements. A document for discussion', available at http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf (accessed on 1 March 2010).
3. Watson, Gary (1996), "Two Faces of Responsibility." Philosophical Topics 24: 227–248
4. Castelluccia, C., Druschel, P., Hübner, S., et al. (2011). Privacy, Accountability and Trust - Challenges and Opportunities, ENISA.
5. Koppell, J. (2005) "Public administration review," *Public Administration Review*, vol. 65, pp. 94–108.
6. Thomas, R. (2009). Foreword of RAND study "Review of Data Protection Directive Summary", Available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive_summary.pdf
7. Feigenbaum, J., Jaggard, A.D. and Wright, R.N. (2011) 'Towards a Formal Model of Accountability', In Sean Peisert, Richard Ford, Carrie Gates, and Cormac Herley, editors, NSPW , page 45-56. ACM, 2011, http://dl.acm.org/citation.cfm?id=2073276.
8. Hildebrandt, M. (2009). *Biometric Behavioural Profiling and Transparency Enhancing Tools*. FIDIS Project Deliverable 7.12. Available at: http://www.scribd.com/doc/72120638/Fidis-wp7-Del7-12-Behavioural-biometric-Profiling-and-Transparency-Enhancing-Tools
9. Weitzner, D.J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., Sussman, G.J. (2008). Information accountability. Communications of ACM 51(6), p. 87, June.
10. OECD (1980) 'Guidelines for the protection of personal data and transborder data flows', available at http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html (accessed on 2 July 2012).
11. Bull J., Watson J., "Evidence disclosure and verifiability", Journal of Economic Theory, Volume 118, Issue 1, September 2004, Pages 1-31, ISSN 0022-0531
12. Bernheim B. D., Whinston M., (1999), Incomplete contracts and strategic ambiguity, Amer. Econ. Rev., 88, 902–932.
13. PMBOK (2011) IEEE Guide--Adoption of the Project Management Institute (PMI(R)) Standard A Guide to the Project Management Body of Knowledge (PMBOK(R) Guide)--Fourth Edition.
14. Kalman R. E. (1961), "On the General Theory of Control Systems", Proc. 1st Int. Cong. of IFAC, Moscow 1960 1 481, Butterworth, London 1961
15. Zabczyk J. (1992), "Mathematical Control Theory: An Introduction", Birkauser Boston, 1992.
16. Filiz-Osbay, E. & Osbay, E.Y. (2012). Effect of an Audience on Public Goods Provision. May. http://econweb.umd.edu/~ozbay/audience.pdf (accessed on 23 December 2012).
17. Cloud Security Alliance (2012a) Privacy Level Agreement (PLA) Working Group, https://cloudsecurityalliance.org/research/pla/
18. Cloud Security Alliance (2012b) Cloud Trust Protocol (CTP), https://cloudsecurityalliance.org/research/ctp/

A Cross-Disciplinary Review of the Concept of Accountability

A Survey of the Literature

Nick Papanikolaou, Siani Pearson

Security and Cloud Lab
Hewlett-Packard Laboratories
{nick.papanikolaou,siani.pearson}@hp.com

Abstract. In this paper we discuss previous definitions of the concept of *accountability* from the literature. Accountability is a multidimensional, context-dependent concept that is gaining interest as a means of addressing a number of data protection problems, including global legal uncertainty and lack of trust.

1 Introduction

Accountability is a complex, multidimensional concept that is subject to many different interpretations across a variety of disciplines. The concept is gaining currency in the context of data protection, and a number of regulatory frameworks are adopting accountability as an established term. This paper attempts to bring together a number of different definitions from a variety of sources, ranging from social and political science all the way to computer science. As will become evident from this short survey, there are commonalities and links between the different definitions and, while it is unlikely to find conflicting or contradictory interpretations, there are subtleties and distinctions in existing definitions that are worthy of our consideration.

2 Definitions of Accountability from the Literature

First we will consider high-level definitions and perspectives of accountability from social and political science, which will help us to frame accountability in the broadest possible sense.

Next we will turn to regulatory frameworks which make use of the term, and examine the relevance of accountability to the handling of personal data within organisations – particularly in the light of European laws and regulations related to data protection. Section 2.3 discusses accountability from the IT management perspective, and this leads us to section 2.4, which focuses down on computer science and presents

adfa, p. 1, 2011.

the interpretations of accountability used in that field, particularly in connection with the implementation of accountable systems.

2.1 High-level Definitions and Perspectives from Social Science

We consider a selection of definitions of accountability, starting with high-level conceptual definitions and proceeding toward a more organizational, governance-related view. We will look at conceptions of accountability from diverse disciplines.

Webster's dictionary of 1828 defines accountability thus:

"1. The state of being liable to answer for one's conduct; liability to give account, and to receive reward or punishment for actions. 2. Liability to the payment of money or of damages; responsibility for a trust."

This definition has changed in the latest version of the dictionary to exclude the reward and punishment aspects, which nevertheless are relevant to our present purpose. Key ingredients of this definition include attribution of responsibility ('being liable to answer for…'), giving explanations, receiving a penalty for any misconduct (especially, being financially liable for damages). These same ingredients are echoed in Schedler's definition (Schedler, 1999):

"A is accountable to B when A is obliged to inform B about A's (past or future) actions and decisions, or justify them and to be punished in the case of misconduct."

Taking an organizational perspective, Koppell (2005) identifies five dimensions of accountability:

"1. Transparency: Did the organization reveal the facts of its performance?
2. Liability: Did the organization face consequences for its performance?
3. Controllability: Did the organization do what the principal desired?
4. Responsibility: Did the organization follow the rules?
5. Responsiveness: Did the organization fulfil the substantive expectation?"

Note that Koppell's definition identifies performance as the principal concern around which accountability is centred. Accountability is understood in relation to performance, which is the objective for which managers are held accountable. Jos and Tompkins (2004) explain that accountability processes can either be performance-based or compliance-based; most of the definitions of interest to us are geared towards compliance with prevailing laws and regulations.

The distinction between accountability and responsibility is made in the following definition (Galway, 2009): *"Accountability is the obligation and / or willingness to demonstrate and take responsibility for performance in light of agreed upon expectations. Accountability goes beyond responsibility by obligating an organization to be answerable for its actions"*. The Galway project's definition of accountability refers specifically to the handling of personal data: *"Accountability is the obligation to act as a responsible steward of the personal information of others, to take responsibility for the protection and appropriate use of that information beyond mere legal requirements, and to be accountable for any misuse of that information."*

From the social sciences we have, among others, Romzek and Dubnick's typology (1987) of public sector accountability; this is a classification of the different ways in which public sector officials are held accountable, and emphasizes the responsibility and liability aspects of the concept of accountability. The typology distinguishes be-

tween legal, political, bureaucratic and professional accountability regimes, each representing a form of responsibility to a particular audience (e.g. bureaucratic accountability being defined as responsibility to those higher up in a bureaucratic hierarchy).

The privacy-oriented definition of accountability given in ISO standard 29100 (ISO, 2011) expresses accountability in terms of the practices associated with it in organizations:

"Accountability: document policies, procedures and practices, assign the duty to implement privacy policies to specified individuals in the organization, provide suitable training, inform about privacy breaches, give access to effective sanctions and procedures for compensations in case of privacy breaches."

This definition clearly picks out privacy breaches as being the problem that accountability as a whole is intended to address, and identifies specific ways to respond to the problem. It gives clear guidance on how to actualize accountability, avoiding what it is. Clearly it is desirable to combine some of the operational aspects with a high-level conceptual description of the concept, in order to produce a definition that meets the needs of researchers and practitioners alike.

Accountability concepts are evolving as the current legal framework responds to globalization and new technologies, and indeed the current drafts of the proposed EU Data Protection Regulation (EC, 2012) and US Consumer Bill of Rights (The White House, 2012) include this concept, at least at a conceptual level (see further discussions in Section 3.2 below). Region block compliance tools such as the EU's binding corporate rules (BCRs) (ICO, 2012) and APEC's cross border privacy rules (CBPRs) (APEC Data Privacy Sub-Group, 2011) are being developed to provide a cohesive and more practical approach to data protection across disparate regulatory systems (Moerel, 2011). See also 'The future of privacy', from the Article 29 Working Party (EC, 2009; Article 29 Working Party, 2012), its opinion of July 2010 (EC, 2010), and the Madrid resolution's global data protection standards (ICDPP, 2009), which the International Conference of Data Protection and Privacy Commissioners adopted in October 2009. The Galway/Paris project started by privacy regulators and privacy professionals has been defining the concept of accountability for the last four years in the context of these latest regulations (CIPL, 2009) and refining its implementation, measurement and scalability.

2.2 Regulatory Frameworks

Accountability is a tool being used by more and more regulators around the world, especially as privacy legislation is enacted or changed in response to technical change and globalization. It is increasingly popular in common law jurisdictions such as Australia, Canada and US and has gained more visibility and acceptance in places governed by civil law. It is not only in the legislation referred to above but also a concept included within enforcement powers in Canada and in new laws being introduced in Latin America (see for example, Office of the Information and Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner for British Colombia, 2012).

Accountability as a notion established in guidance such as OECD (OECD, 1980), APEC (APEC Data Privacy Sub-Group, 2011) and PIPEDA (PIPEDA, 2000) essen-

tially means placing a legal responsibility upon an organization that collects and uses personal data to ensure that contracted partners to whom it supplies the personal data are compliant and equally accountable, wherever in the world they may be. Its notion as a data protection model is evolving towards being an 'end-to-end' personal data stewardship regime in which the enterprise that collects the data from the data subject is accountable for how the data is shared and used throughout its journey across the global and its lifecycle from collection to disposal.

The concept of accountability is enshrined in regulatory frameworks for data protection across the globe. The Organization for Economic Cooperation and Development privacy guidelines (OECD, 1980) do not only embrace the concept but also take a step forward, addressing it quite clearly by considering the data controller as accountable with regard to compliance with measures implementing the established principles. The concept of accountability is also present in the Asia Pacific Economic Cooperation's privacy framework (APEC, 2005), as well as in Canada's Personal Information Protection and Electronic Documents Act (PIPEDA, 2000). Basic elements of the concept can also be found in Convention 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data (Council of Europe, 1981). One expression of accountability that is common in all aforementioned documents are the obligations posed to the data controller for complying with that particular data protection legislation and, in most cases, the establishment of systems and processes which aim at ensuring such compliance.

Although the Data Protection Directive does not introduce explicitly the principle of accountability, it does embrace it in several provisions. The text of the Data Protection Directive as such is structured on the acceptance of relationships between the different entities involved in the processing of personal data. The relationship between data controllers and data subjects constitutes the main relationship provided on which further relationships are built. The Directive also addresses relationships from which accountability obligations derive between data controllers-data processors and data controllers-supervisory authorities. These relationships are characterized by a substantial imbalance of powers in practice in the course of processing between the data subject and the data controller, which justifies protection through accountability provisions (De Hert and Gutwirth, 2006). In his Glossary, the EDPS has defined accountability as follows: "accountability intends to ensure that data controllers are more generally in control and in the position to ensure and demonstrate compliance with data protection principles in practice (....)" (EDPS, 2012).

In January 2012 the European Commission presented a proposal for a draft Regulation that is suggested to replace the Data Protection Directive. Although the draft Regulation does not include the term accountability in its text, the Explanatory Memorandum explains that Article 22 of the draft Regulation, entitled 'Responsibility of the controller' "takes account of the debate on a 'principle of accountability' and describes in detail the obligation of responsibility of the controller to comply with this Regulation and to demonstrate this compliance, including by way of adoption of internal policies and mechanisms for ensuring such compliance".

The Article 29 Working Party in its opinion on accountability made use of the term 'accountability', but explained the reasons why it may be difficult to use the term in all European languages:

"21. The term "accountability" comes from the Anglo-Saxon world where it is in common use and where there is a broadly shared understanding of its meaning –even though defining what exactly "accountability" means in practice is complex. In general terms though its emphasis is on showing how responsibility is exercised and making this verifiable. Responsibility and accountability are two sides of the same coin and both essential elements of good governance. Only when responsibility is demonstrated as working effectively in practice can sufficient trust be developed.

22. In most other European languages, due mainly to differences in the legal systems, the term "accountability" cannot easily be translated. As a consequence, the risk of varying interpretation of the term, and thereby lack of harmonisation, is substantial. Other words that have been suggested to capture the meaning of accountability, are "reinforced responsibility", "assurance", "reliability", "trustworthiness" and in French "obligation de rendre des comptes" etc. One may also suggest that accountability refers to the "implementation of data protection principles".

23. In this document, therefore we focus on the measures which should be taken or provided to ensure compliance in the data protection field. References to accountability should therefore be understood as the meaning used in this Opinion, without prejudice to finding another wording that more accurately reflects the concept given here. This is why the document doesn't focus on terms but pragmatically focuses on the measures that need to be taken rather than on the concept itself." (European DG of Justice, 2010)

The Article 29 Data Protection Working Party, national Data Protection Authorities (Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 2010), the European Data Protection Supervisor (EDPS), as well as the data protection and privacy regulators at the 31st International Conference of Data Protection and Privacy Commissioners – see reference (ICDPP, 2009) - have paid special attention to the principle of accountability. The common ground of these approaches has been the need to "reinforce" (EDPS, 2012b) accountability implying clearly its existence under the Data Protection Directive. The Article 29 Data Protection Working Party has made use of the term "*reinforced responsibility*" in order to describe the meaning of accountability (European DG of Justice, 2010), implying both "responsibility" and "action" with respect to the specific responsibility. Both in the Opinion on the Future of Privacy (European DG of Justice, 2009) and in the Opinion on Accountability (European DG of Justice, 2010), the Article 29 Working Party examines primarily the "conformity in practice" of the processing conducted by data controllers with the applicable rules laid in the Directive. In this way, accountability seems to link the responsible actors with the implementation of certain measures.

2.3 IT Management

Governance and compliance frameworks such as ISO/IEC 27001/02 contain many of the elements of accountability defined above: the information security management system of an organization is meant to generate assurance, transparency and responsibility in support of control and trust. For instance controls within 27002 require attribution and separation of responsibility (e.g. ISO 27001 section A.8.1.1 states that "Security roles and responsibilities of employees, contractors and third party users

shall be defined and documented in accordance with the organization's information security policy."). Moreover, the increasing use of contractual arrangements and frameworks for monitoring the fulfilment of commitments made in those contracts affects liability (as breach of contract entitles the other party to some remedy at law. These remedies include payment of damages to compensate for the breach, termination of the contract, the ability to seek court orders requiring compliance, and a range of internal remedies such as reduction in charges, processes for negotiating consensual remediation without seeking court action, and so on).

Risk assessment is particularly important for accountability because it is a central part of the process used to determine and demonstrate that the policies (whether reflected in corporate privacy and security policies or in contractual obligations) that are signed up to and implemented by the organization (that is taking an accountability-based approach) are appropriate to the context. The type of procedures and mechanisms vary according to the risks represented by the processing and the nature of the data (CNIL, 2012; Catteddu, Hogben, 2009; Castelluccia et al., 2011). Automation can enhance this process (Pearson, 2011). Data impact assessment may also become an obligation for some high risk contexts within the forthcoming EU regulation (cf. Article 33: EC, 2012).

These elements of risk assessment, transparency and redress are captured within the core elements of implementing an accountability project within an organization specified within the Galway and Paris projects, which were (CIPL, 2009; CIPL, 2010):

- Policies that reflect current laws and relevant standards
- Executive oversight and responsibility for privacy
- Delegation of responsibility to trained resources; education of staff and suppliers
- On-going risk assessment and mitigation relating to new products or processes
- Regular risk assessment and validation of the accountability program
- Policies to manage major privacy events or complaints
- Processes to enforce policies internally
- A method of redress if privacy rights are breached

These core elements of implementing an accountability project within an organization (CIPL, 2010), are very similar to the guidance provided by the Privacy Commissioners of Canada, Alberta and British Columbia (Office of the Information and Privacy Commissioner of Alberta et al, 2012), which was influenced by that work.

2.4 Computer Science

Our interest is in bridging the gap between the high-level definitions and views of accountability that are found in legal, regulatory, and management texts, and those found in the computer science literature, in which there is to be found a stronger link to security controls and means of automating such aspects as assignment of blame, enforcement of policies and more.

The notion of accountability cuts across many domains of computer science, such as: digital forensics, computer security, distributed systems in general (including grid and cloud computing, the Internet and network applications) and natural language

processing. Except for a few references, esp. (Weitzner et al., 2008; Le Métayer, 2011; Pearson and Wainwright 2012), in computer science, there is not a general and interdisciplinary view of accountability. Most of the papers, due to the complexity of the concept, only address some properties or specific mechanisms related to accountability. One thing does become obvious though – namely the view that the preventive controls used extensively in classical IT security are not sufficient to achieve accountability. Full accountability requires mechanisms for information transparency, checking misbehaviour and responsibilities and then proceeding to punishment. There are already some proposals for frameworks integrating these aspects (Pearson and Wainwright, 2012) and formal models or logics for accountability (Cederquist et al., 2005; Le Métayer, 2009; Jagadeesan et al., 2009; Küsters et al., 2010; Feigenbaum et al., 2011).

Weitzner et al. (2008) consider that the usual "hide-it-or-lose-it" perspective on information is dominating but not adequate in a world where information should be communicated. They argue that a shift is needed from hiding information to ensuring only appropriate uses occur. They describe the ability to maintain a history of data manipulations and inferences (their interpretation of transparency) which can then be checked against a set of policies that govern them (their interpretation of accountability). For them, accountability is retrospective, in the sense that if actor *A* performs action *B* then we can review *B* against a predetermined policy to decide if *A* has done something wrong, and hence hold *A* accountable.

Lin (2010) claims that the key elements of accountability are: disclosure, liability and non-repudiation, and that the notion also includes collective responsibility and policy. Le Métayer (2011) discusses the interplay between legal and technical means to risks for citizens and consumers. Laws and contracts provide assurances and technology can help enforce legal commitments. Pearson and Wainwright (2012) take a global and interdisciplinary approach, which encompasses legal, regulatory and technical aspects. The principle is to provide a rich toolset rather than define a general, catch-all solution for all aspects of accountability. A distinction is made between *preventive*, *detective* and *corrective* mechanisms which can help in understanding, organizing and implementing accountability. Xiao (2012) is a comprehensive survey of research related to accountability in the computer science domain. The author does not give a precise definition for accountability but relates it to a number of uses in various areas of computer science. End-to-end accountability is generally not accomplished; these systems have four key characteristics: identities of events, a secure record of events, auditing and evidence.

3 Summary

In this paper we have reviewed existing definitions of accountability from the literature and discussed related concepts and their interrelationships; the way that accountability has been interpreted in regulatory frameworks has been reviewed in some depth, and various interpretations of the concept from different disciplines, from law to computer science, have been presented. Thus we have seen a great number of related perspectives and formal models of accountability that can be used in IT systems.

The ongoing Cloud Accountability Project (A4CLOUD), funded by the European Commission, has been working (among other things) on bringing these perspectives and models together to produce a coherent, cross-disciplinary view of this complex concept.

Acknowledgement. We would like to acknowledge the contributions of our colleagues in the A4Cloud project and, in particular, Jean-Claude Royer and Giles Hogben, to the analysis presented here.

4 References

1. Schedler, A. (1999). Self-Restraining State: Power and Accountability in New Democracies. Lynne Reiner Publishers, pp. 13–28.
2. Koppell, J. (2005) "Public administration review," *Public Administration Review*, vol. 65, pp. 94–108.
3. Jos, P. and Tompkins, M. "The Accountability Paradox in an Age of Reinvention: The Perennial Problem." Administration & Society 36 (2004): 255.
4. CIPL, Accountability Project (Galway Project): http://www.informationpolicycentre.com/accountability-based_privacy_governance/.
5. Center for Information Policy Leadership (CIPL) (2009) 'Data protection accountability: the essential elements. A document for discussion', available at http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf (accessed on 1 March 2010).
6. Center for Information Policy Leadership (CIPL) (2010) 'Demonstrating and measuring accountability: a discussion document', Accountability Phase II – The Paris Project, available at http://www.huntonfiles.com/files/webupload/ CIPL_Accountability_Phase_II_Paris_Project.PDF (accessed on 2 July 2012).
7. Romzek, BS and Dubnick, MJ. (1987). "Accountability in the Public Sector: Lessons from the Challenger Tragedy." Public Administration Review. http://www.jstor.org/stable/10.2307/975901.
8. ISO/IEC 29100. (2011). Information technology – Security techniques – Privacy framework. Technical report, ISO JTC 1/SC 27.
9. European Commission (EC) (2012) 'Proposal for a directive of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data', January, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_en.pdf (accessed on 2 July 2012).
10. White House (2012). Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. Available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf
11. Information Commissioner's Office (ICO) (2012) Guidance on the Use of Cloud Computing, available at http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx
12. APEC Data Privacy Sub-Group (2011) 'Cross-border privacy enforcement arrangement', San Francisco, 18 September, available at http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_010.pdf (accessed on 2 July 2012).

13. Moerel, L. (2011) ‘Binding corporate rules’, PhD thesis, Tilburg University.
14. European DG of Justice (2009). Article 29 Working Party. ‘The future of privacy: joint contribution to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (WP168)’, December.
15. European DG of Justice (2010). Article 29 Working Party. ‘Opinion 3/2010 on the principle of accountability (WP 173)’, July.
16. European DG of Justice (2012). Article 29 Working Party. Opinion 05/12 on Cloud Computing, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf
17. ICDPP (2009). 31st International Conference of Data Protection and Privacy ‘Data protection authorities from over 50 countries approve the “Madrid Resolution” on international privacy standards’, available at http://www.gov.im/lib/docs/odps//madridresolutionpressreleasenov0.pdf (accessed on 2 July 2012).
18. Office of the Information and Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner for British Colombia. (2012). Getting Accountability Right with a Privacy Management Program.
19. Office of the Privacy Commissioner of Canada (2007). "Privacy Impact Assessments." Internet: http://www.priv.gc.ca/fs-fi/02-05-d-33-e.cfm, February 2007 [Nov. 5, 2009].
20. Office of the Information and Privacy Commissioner for British Columbia (2012). Getting Accountability Right with a Privacy Management Program. Available at: http://www.oipc.bc.ca/guidance-documents/1435
21. OECD (1980) ‘Guidelines for the protection of personal data and transborder data flows’, available at http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html (accessed on 2 July 2012).
22. APEC Data Privacy Sub-Group (2011) ‘Cross-border privacy enforcement arrangement’, San Francisco, 18 September, available at http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_010.pdf (accessed on 2 July 2012).
23. PIPEDA (2000) Available at http://laws-lois.justice.gc.ca/eng/acts/P-8.6/ (accessed on 2 July 2012).
24. De Hert, P. and Gutwirth, S. (2006). ‘Privacy, data protection and law enforcement. Opacity of the individual and transparency of power’, in E. Claes, A. Duff and S. Gutwirth (eds.), Privacy and the Criminal Law, Antwerpen/Oxford, Intersentia.
25. EDPS (2012). Glossary of terms. http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/71#accountability.
26. EDPS (2012b). Opinion on the Data Reform Package, 7th of March 2012.
27. EDPS (2012c). Opinion of the European Data Protection Supervisor on the Commission’s Communication on “Unleashing the potential of Cloud Computing in Europe”.
28. EDPS (2012d). “Responsibility in the Cloud should not be up in the air”. Article EDPS/12/15. Available at: http://europa.eu/rapid/press-release_EDPS-12-15_en.htm
29. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2010), ‘Ein modernes Datenschutzrecht für das 21. Jahrhundert’ (18 March 2010).
30. CNIL (2012) ‘Methodology for Privacy Risk Management’. Available at: http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf
31. Catteddu, D. & Hogben, G. (eds.) (2009) Cloud Computing: Benefits, Risks and Recommendations for Information Security. ENISA Report, November.

32. Castelluccia, C., Druschel, P., Hübner, S., et al. (2011). Privacy, Accountability and Trust - Challenges and Opportunities, ENISA.
33. Pearson, S. (2011). Toward Accountability in the Cloud. Internet Computing, IEEE, July/August issue, 15:4, pp. 64-69.
34. European Commission (EC) (2012) 'Proposal for a directive of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data', January, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_en.pdf (accessed on 2 July 2012).
35. Weitzner, D.J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., Sussman, G.J. (2008). Information accountability. Communications of ACM 51(6), p. 87, June.
36. Le Métayer, D. (2011). Formal methods as a link between software code and legal rules. Software Engineering and Formal Methods , pages 3-18, http://www.springerlink.com/index/980H052715W527GQ.pdf.
37. Pearson, S. & Wainwright, N. (2012). An Interdisciplinary Approach to Accountability for Future Internet Service Provision. International Journal of Trust Management in Computing and Communications (IJTMCC), 1:1.
38. Cederquist J.G., Corin J.G., Dekker M.A.C., Etalle S., and Den Hartog, J.I., (2005). An audit logic for accountability. pages 34-43. IEEE, http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1454301.
39. Le Métayer, D. (2009). A formal privacy management framework. Formal Aspects in Security and Trust , pages 1-15, http://www.springerlink.com/index/q7505648948p9710.pdf.
40. Jagadeesan R., Jeffrey A., Pitcher C., and Riely J. (2009). Towards a theory of accountability and audit. In Michael Backes and Peng Ning, editors, Computer Security ESORICS 2009 , volume 5789 of Lecture Notes in Computer Science , pages 152-167, http://dx.doi.org/10.1007/978-3-642-04444-1_10.
41. Küsters R., Truderung T., and Vogt A., (2010). Accountability: definition and relationship to verifiability. pages 526-535. ACM, http://dl.acm.org/citation.cfm?id=1866366.
42. Feigenbaum, J., Jaggard, A.D. and Wright, R.N. (2011) 'Towards a Formal Model of Accountability', In Sean Peisert, Richard Ford, Carrie Gates, and Cormac Herley, editors, NSPW , page 45-56. ACM, 2011, http://dl.acm.org/citation.cfm?id=2073276.
43. Lin K., Zou J., and Wang Y. (2010). Accountability computing for e-society. pages 34-41. IEEE, http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5474671.
44. Xiao Z., Kathiresshan N. and Xiao Y., (2012). A survey of accountability in computer networks and distributed systems. Security and Communication Networks, http://dx.doi.org/10.1002/sec.574.
45. Guagnin D., Hempel L., Ilten C., Kroener I., Neyland D., and Postigo H. (eds.) (2012) Managing Privacy through Accountability. Palgrave Macmillan.
46. Raab C. (2012). The Meaning of 'Accountability' in the Information Privacy Context. In [45].
47. Bennett C. (2012). The Accountability Approach to Privacy and Data Protection : Assumptions and Caveats. In [45].
48. Alhadeff J., Van Alsenoy B. and Dumortier J. (2012). The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions. In [45].

Evidence for Accountable Cloud Computing Services

Thomas Rübsamen[1], Christoph Reich[1], Aryan Taherimonfared[2], Tomasz Wlodarczyk[2], and Chunming Rong[2]

[1] Cloud Research Lab,
Furtwangen University of Applied Science,
D-78120 Furtwangen, Germany
{thomas.ruebsamen,christoph.reich}@hs-furtwangen.de
[2] Department of Electrical Engineering and Computer Science,
University of Stavanger,
N-4036 Stavanger, Norway
{aryan.taherimonfared,tomasz.w.wlodarczyk,chunming.rong}uis.no

Abstract. Evidence that allows assurance of accountability services, verification of compliance with the principles of accountability by service-providers and attribution of responsibility for breaches within the chain of accountability is essential. This paper defines how evidence may be required and proposes suitable ways of treating key accountability concepts. It shows the importance of verification and assurance, monitoring and auditing, and challanges of evidence in cloud computing. A discussion of logging and evicence gathering points complete the paper.

1 Introduction

Issues of transparency and control arise, when data moves from being stored locally to being stored remotely on the cloud. It becomes important to provision evidence for handling of confidential data in the Cloud by remote parties through whole lifecycle, also including deletion. However, this evidence is often not provided; transparency and verifiability are missing in the cloud context (especially at PaaS and IaaS levels). Moreover, there are additional related issues including cloud computing and globalization, increasing foreign government surveillance, the potential for light-touch self-regulation by the back door, weak certification for accountability, and weak links in terms of data protection along the service provision chain.

Currently, there is a lack of transparency and accountability from the provider side as for service provisioning/de-provisioning, tenant isolation, data processing and movement, privacy protection as well as many other aspects which used to be fully under the control and monitoring of the consumer. Even if key terms are being added into cloud contracts (Service Level Agreement), processes and techniques must be developed to continuously and automatically monitor and audit these terms and ensure adequate transparency. Cloud providers must be also prepared to provide adequate evidence about security and privacy provision.

A system for Evidence Collection that captures, integrates and processes the information including logs, policies and context in a way that preserves privacy and confidentiality and, supports audit and attribution is needed. An evidence framework for Cloud Computing does not exist yet. The main contribution of this paper is establishing necessary requirements for provisioning of evidence in a Cloud environment and how these requirements influence the tasks of monitoring and audit.

This paper is organized in the following way. In Section II we summarize existing related work. In this context, in Section III, we discuss general requirements necessary to provision evidence handling in a Cloud environment. In Section IV we discuss how these requirements influence the tasks of monitoring and audit. In Section V we summarize challenges of evidence provisioning in Cloud Computing. We conclude the paper in Section VI.

2 Related Work

One initiative towards evidence framework for Cloud Computing is an open architecture for digital evidence integration [1] by Schatz, B., and Clark, A. J. from the Common Digital Evidence Storage Format Working Group (CDESF). The architecture focused on digital evidence bags (DEB), a generalized method for collecting information about evidence and evidence metadata while keeping evidence integrity.

In Dykstra's paper [2] investigates how to obtain forensic evidence from cloud computing using the legal process by surveying the existing statues and recent cases applicable to cloud forensics. A sample search warrant is presented that could provide a sample language for agents and prosecutors who wish to obtain a warrant authorizing the search and seizure of data from cloud computing environments.

The paper from Haeberlen et al. [3], an accountable virtual machines (AVMs) has been introduced, which can execute binary software images in a virtualized copy of a computer system and can record non-repudiable information that allows auditors to subsequently check whether the software behaved as intended. Since this approach is basically VM logging and replaying, it is effectively the same as our full integrity checking, potentially with a lot of overhead.

In the paper of Poisel et al. [4] discuss digital forensics investigations at the hypervisor level of virtualized environments and introduce the topic of evidence correlation within cloud computing infrastructures.

The acquisition and analysis of digital evidence in cloud deployments is more complex, because data could be encrypted before being transferred to the cloud or it could be stored in different jurisdictions resulting in data being deleted before investigators have access to it [5].

Flaglien et al. [6] evaluated currently used storage and exchange formats for handling digital evidence against criteria identified in recent research literature. Formats intended for storing evidence from highly dynamic and complex sys-

tems are characterized by incorporating additional information, which can be processed by data mining tools.

Lu et al. [7] proposed to adopt the concept of provenance to the field of cloud computing by enabling a data object to report who created it and modified its contents, provenance could provide digital evidences for post investigations. Provenance information would have to be secured in cloud environments as leaking this information could breach information confidentiality and user privacy.

Marty's [8] approach utilize logging facilities to generate and collect relevant data to support the digital forensics investigation process.

The chain of custody documents how evidence was handled in the context of the digital investigations process [9]. The documentation describes how evidence was collected, analyzed, and preserved to be approved in court.

3 Accountability and Evidence

The A4Cloud FP7 research project [10] approach encompasses legal and regulatory mechanisms and a range of technological enhancements that can provide the necessary basis for trust. Customers, providers and regulators should be supported by preventive, detective, and corrective task (see [11]) and, for example, give cloud customers more control over their cloud services, ensure providers to meet their obligations, and enable cloud audits.

Technology can provide assistance in ensuring proper implementation of accountability. In particular, technology can be used to strengthen the enforcement and monitoring of policies and to help provide evidence, assurance and transparency. Hence, in accordance with Recommendation 5 from (Castelluccia et al, 2011 [12]), our approach is that privacy assessment, assurance, verification or enforcement should be evidence-based, and that these evidences might be derived from a number of sources, events and traces at different architectural layers.

The A4Cloud project identified a number of accountability attributes, like obligation, responsability, remediation, attributability, liability, sanctions, assurance, transparency, remediation, observability and responsiveness. These attributes have different importance from the perspective of a framework of evidence and identification of evidence types. We can divide these attributes into two general groups, those that reflect on accountability as a concept and those that reflect on how such concept should or could be implemented. Evidence of the following accountability attributes are of primary interest:

1. Attributability: Attributability describes a property of an observation that discloses or can be assigned to actions of a particular actor (or system element).
2. Observability: Observability is a property of an object, process or system that describes how well the internal actions of the system can be described by observing the external outputs of the system.
3. Assurance can take the form of evidence. An accountability system can produce evidence that can be used to convince a third party that a fault has

or has not occurred. In the context of accountability, assurance could refer to provision of ex ante evidence for compliance to governing rules, and possibly also to evidence that the governing rules and other factors provide appropriate grounds for trustworthiness .

4. Verifiability can be defined as the ability of an external party to observe a given aspect of a contractual relationship through the collected evidence. The quality or level of verifiability depends directly on the available evidence.

Remaining difficulties addressed by A4cloud is the development of mappings between the accountability contracts/SLAs and evidence available through logging. The framework should build an evidence base from which mappings of low level distributed remote IT logs can be mapped to high level policy requirements and service level agreements (SLAs). Evidence of accountability can therefore be provided and input to certification schemes or trustmarks. Figure 1 shows an overview of these relationships with log data being collected as evidence and evidence supporting auditing as well as assuring the previously mentioned accountability attributes addressed by the A4Cloud project.

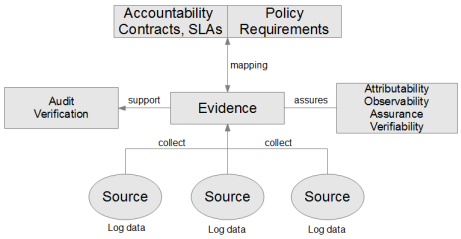

Fig. 1. Collecting Evidence and Mapping to Accountability

Environments in which there are diverse and heterogeneous service providers, make provision of protocols and models for trust verification and assurance difficult. The CloudTrust Protocol [13] defines some evidence categories, but has not covered other categories such as legal liability of the involved parties.

There are no efficient mechanisms available to gather convincing evidence from verified log data in distributed multi-tenancy environments, even if cloud providers would be willing to provide this. Although there are a number of existing logging approaches, they do not fit cloud computing very well. For example, EGEE LB log solution in grid computing is mostly used for debugging purposes only, as it keeps track of jobs. Even if verified log data is available, there are still challenges to make them compatible and interoperable. As different cloud providers implement and operate their systems differently, there is no guarantee that they all provide the same kinds of log information, which may expose weaknesses in their systems. There is currently no standard on log information to be delivered and there is no financial or regulatory incentive for the providers to provide such information. Furthermore, there is no accountability model for cloud, and therefore it is impossible to assign responsibilities even if the evidence exists. Neither are there any mechanisms for assigning responsibilities when the incident involves more than one provider based on gathered evidence in distributed systems.

4 Monitoring and Audit

Accountability mechanisms must be justified and Bennett [14] points out that a important process is independent testing of practices, provision of evidence that is taken into account, including auditing against the ISO 27001 series and associated cloud security standards. Evidence is provided by tools into trusted third party auditing processes against such standards.

ISO standards cover audit requirements at a high levelwhich is to maximize the effectiveness of and minimize interference to/from the information systems audit process. These solutions are not currently linked to formally defined accountability models, as accountability models only currently exist in terms of regulatory frameworks or point technical solutions. Accountability (for complying with measures that give effect to practices articulated in given guidelines) has been present in many core frameworks for privacy protection, like the Organization for Economic Cooperation and Development (OECD)'s privacy guidelines.

A4Cloud provide an approach based around a model of accountability that is interdisciplinary in approach, in which we build an evidence repository that provides evidence for preventive, detective and corrective accountability mechanisms by means of associated mechanisms for obtaining and negotiating obtaining these events from remote monitoring parties, and mechanisms for mapping the low level IT logs to what is in our repositories to policies and service level agreements (SLAs). In this way we bridge from distributed remote logs to high level policy requirements, and can detect policy violations. Audit capabilities in conjunction with external audit frameworks should be enhanced in order to strengthen the obligation for compliance and improve detection of violations.

5 Challenges of Evidence in Cloud Computing

Cloud forensics refers to digital forensics investigations performed in cloud computing environments. The process of a digital investigation can be separated into different phases as defined in the National Institute of Standards and Technology, "Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders" [15] each having its own specific purpose:

1. Securing Phase: The major intention is the preservation of evidence for analysis. The data has to be collected in a manner that maximizes its integrity. As can be imagined, this represents a huge problem in the field of cloud computing where you never know exactly where your data is and additionally do not have access to any physical hardware.
2. Analyzing Phase: Data from multiple systems or sources is pulled together to create as complete a picture and event reconstruction as possible.
3. Presentation Phase: Reporting all results in a clear and understandable way.

Current techniques in computer forensics can only analyze the evidence left behind by a careless intruder. We will use a combination of legal, technical and regulatory approaches to provide traceability, logging mechanisms and tools for

determining information provenance in distributed systems. This will underpin liability assignment and validation of insurance claims made in case of data breach or data loss. Evidence provided by our tools will enhance existing and developing certification schemes within the cloud.

With respect to the notion of evidence, it is important to differentiate between accountability and forensics. Digital forensics looks for unintended evidence, i.e. evidence that some party was not planning to leave and which collection was not planned ahead.

5.1 Sources of Evidence by Logging

The sources for logging can be manifold reaching from business relevant logging and operational logging. Operational logging could cover errors that concern a single cloud customer, critical conditions that impact all users, system related problems (e.g., failed resource access) and all activity that is executed by privileged accounts.

Sources of evidence to log, based on requirements and attributes, should be strengthened through the use of formal methods (e.g., formal logic). This is necessary to ensure the evidence quality in a situation where the amount of evidence-related data exceeds human reasoning capabilities.

Logging will need to be carried out at various stages of abstraction, i.e. at the system level, at the data level, at the service level, at the business level to determine when data is accessed, shared, moved, etc. The type of things that need to be logged at the data level are:

- *data creation:* the creation of a new data item, and the policies associated with this new item. The new item may be created by a user, or may arise from the automated copying or processing of data already in the system.
- *data access:* who accessed which data, for what purpose, the role of a person accessing the data, whether consent was obtained for usage from the data subject
- *data flow:* where the data is sent (including the jurisdiction), who shared data with whom
- *data type:* the type of data (e.g., is it personal, sensitive, etc.)
- *data deletion:* when was the data deleted, which erase method was used (unlink, delete data, delete backup, etc.)
- *data handling:* how data is handled to check conformance with some policies (e.g., data is stored password-protected or encrypted), data policy changes by the service provider, timing information (for example, for conformance to data retention policies)
- *data notification:* triggering and satisfaction of obligations

Subsequently, this information can be used in order to analyse whether organizational, regulatory and legal policies have been followed (this is a detective control, as opposed to checks made within the system associated with access control, etc. which are preventive). More specifically, we may want to focus on the following:

– segregation of duties; trans-border data flow; assurance that access control policies have been met
– assurance that obligations have been met
– records about how information was shared, with the context and associated obligations/sticky policies

5.2 Evidence Gathering Points

There are various locations to gather evidential data. As seen in Fig. 2 data (log data, memory, databases, etc.) can be collected at the network, hardware, host OS, hypervisor, the VMs, the CMS, the network and evidence data across other cloud platforms.

Network: In a complex computing model, such as Cloud, several stakeholders are involved. It should be possible to monitor networking resources which are utilized by a particular stakeholder. Networking resources can be either physical or virtual. Moreover, these resources can be shared among stakeholders. For instance in IaaS, a single network card in the host machine is utilized by several VMs and they may belong to different customers. Distinguishing between customer's traffic, which are hosted in a common set of substrates, is a key issue for accountability. This can also be applied to other service models of cloud, when traces of stakeholders' network activities must be available as an evidence type. However, existing networking devices and monitoring solutions are not compatible and efficient for such a multi-tenant environment.

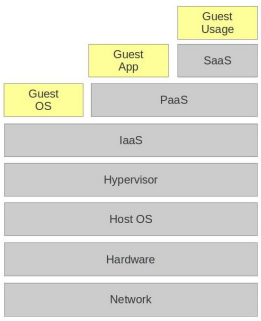

Fig. 2. Evidence Gathering Points

Hypervisor: The usage of data from hypervisors to prove various actual situations has been referred to as "virtual machine introspection" (VMI) and data gathered from this level of access supported the operation of Intrusion Detection Systems (IDS). It is suitable for investigating cloud infrastructures as long as there is access to the hypervisors.

VM: In order to obtain information from within VMs it could be helpful to install additional software inside the VMs. Carbone et al. [16] follow this approach by developing a secure and robust infrastructure called SYRINGE. The monitoring application is protected because it is put into a separate virtual machine as known from the out-of-guest approach. Nevertheless, it is possible to invoke guest functions by utilizing the function-call injection technique. The VM introspection make use of the guest OS knowledge of the deployed software architecture and can only be accessed with the customer's permission. A disadvantage arises from this component being susceptible to compromise from malicous entities.

CMS: The Cloud Management System (CMS) is a huge source for information gathering. It is the central controlling component of a cloud infrastructure and provides information about user logins, cloud service usage, access rights, configuration, resource provisioning, policies, etc.

IaaS: Except for traditional forensic acquisition at the virtual resources most interesting are VM snapshots which can accommodate preservation letters or serve as the acquisition image. Public clouds do not allow live forensics and access to volatile data. The storage is logical and focused on allocated space. Images can include data remnants or unallocated disk space. The logging may be co-located or spread across multiple and changing resources.

PaaS: In a web service PaaS the log data analysis can be carried out with the aforementioned methods, but relies on the cloud service provider. Multi-tanent log data must be separated or merged together from multiple resources.

SaaS: Access to application / authentication logs are possible to get and the SaaS application features may assist with network forensics. The logging information is located on the provider side and highly dependent of the application. The information may be inconsistent across API.

InterCloud: Cloud sources may be distributed over many providers and therefore collecting evidence over multiple sides is even more complex and difficult. There is a need of standardization of an evidence protocol, similar to the TrustCloud protocol.

6 Conclusion

The accountability approach taken in the EU FP7 A4Cloud project should help organisations meet their obligations and give cloud customers more control in cloud services. An evidence framework will be developed to assure accountability by building an evidence base gathering information. This information is collected at different level of the cloud stack and distributed in the infrastructure.

References

1. Schatz, B., Clark, A.J.: An open architecture for digital evidence integration. `http://eprints.qut.edu.au/21119/1/c21119.pdf`
2. Dykstra, J.: Seizing electronic evidence from cloud computing environments. In Ruan, K., ed.: Cybercrime and Cloud Forensics: Applications for Investigation Processes, Hershey, PA: Information Science (2013) 156–185
3. Haeberlen, A., Aditya, P., Rodrigues, R., Druschel, P.: Accountable virtual machines. In: Proceedings of the 9th USENIX conference on Operating systems design and implementation. OSDI'10, Berkeley, CA, USA, USENIX Association (2010) 1–16

4. Poisel, R., Malzer, E., Tjoa, S.: Evidence and cloud computing: The virtual machine introspection approach. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA) **4**(1) (3 2013) 135–152
5. George, E., Mason, S.: Digital evidence and cloud computing. Computer Law & Security Review **27** (September 2011) 524–528
6. Flaglien, A., Mallasvik, A., Mustorp, M., Årnes, A.: Storage and exchange formats for digital evidence. Digital Investigation **8**(2) (2011) 122–128
7. Lu, R., Lin, X., Liang, X., Shen, X.S.: Secure provenance: the essential of bread and butter of data forensics in cloud computing. In: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS '10), New York, NY, USA, ACM (2010) 282–292
8. Marty, R.: Cloud application logging for forensics. In: Proceedings of the 2011 ACM Symposium on Applied Computing. SAC '11, New York, NY, USA, ACM (2011) 178–184
9. Casey, E.: Digital Evidence and Computer Crime - Forensic Science, Computers and the Internet, 3rd Edition. Academic Press (2011)
10. Pearson, S., Tountopoulos, V., Catteddu, D., Sudholt, M., Molva, R., Reich, C., Fischer-Hubner, S., Millard, C., Lotz, V., Jaatun, M., Leenes, R., Rong, C., Lopez, J.: Accountability for cloud and other future internet services. In: Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on. (2012) 629–632
11. Pearson, S., Wainwright, N.: An interdisciplinary approach to accountability for future internet service provision. In Thampi, S.M., ed.: International Journal of Trust Management in Computing and Communications. Volume 1., INDERScience Publishers (2013) 52–72
12. Fischer-Hübner, S.: Transparency enhancing tools & hci for policy display and informed consent. In: Privacy, Accountability, Trust Challenges and Opportunities : ENISA Report. European Network and Information Security Agency, Technical Competence Department (2011)
13. Cloud Security Alliance (CSA): Cloud Trust Protocol. `https://cloudsecurityalliance.org/research/ctp`
14. Bennett, C.: 2. In: The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats. Palgrave MacMillan (August 2012) 33–48
15. National Institute of Justice (U.S.): Electronic crime scene investigation: an on-the-scene reference for first responders. U.S. Dept. of Justice, Office of Justice Programs, National Institute of Justice (2009)
16. Carbone, M., Conover, M., Montague, B., Lee, W.: Secure and robust monitoring of virtual machines through guest-assisted introspection. In: RAID. (2012) 22–41

Privacy & Security of Mobile Cloud Computing

Manmohan Chaturvedi[*,1] , Sapna Malik[2], Preeti Aggarwal[3] and Shilpa Bahl[4]
Ansal University, Sector 55,Gurgaon- 122011, India
[1]mmchaturvedi@ansaluniversity.edu.in [2] sapnadhankhar@gmail.com
[3] preetaggarwal@gmail.com,[4] gerashilpa@gmail.com

Abstract

The Indian government, like governments elsewhere in the world, has chosen mobile device as preferred platform to engage with citizens while offering various e-Governance services. Likewise there is huge market for mobile based e-Commerce applications across the globe. However uptake of these services is challenged by the security and privacy concerns of the end user. The limited processing power and memory of a mobile device dependent on inherently unreliable wireless channel for communication and battery for power leaves little scope for a reliable security layer. Thus there is a need for a lightweight secure framework that provides security with minimum communication and processing overhead on mobile devices. The security and privacy protection services can be achieved with the help of secure mobile-cloud application services. Taking support from a proximate cloud a security service could be devised for a mobile device which works as an interface and adaptively provides optimum security solutions based on communication channel capacity, available system resources both hardware and software and user-defined QoS parameters. We plan to explore and experiment with available options to recommend security and privacy enhancing approaches that may meet the security need for mobile application using automated sensing of the context.

Key Words: Mobile Security, Adaptive Security, m-governance, m-commerce, Privacy and Security

1. Introduction

Mobile Cloud Computing (MCC) is combination of two terms, mobile computing and cloud computing. Mobile computing is provision of applications on mobile devices. Cloud computing refers to getting paid services either in the form of infrastructure, platform or software through internet based cluster of distributed servers. Mobile cloud computing is provision of mobile applications using cloud to give more power to mobile devices towards computing, in spite of resource limitations in mobile devices. Mobile cloud computing is a concept that has been in use since 2009 and is still evolving.

There are various known challenges in the field of MCC viz. handover delay, bandwidth limitation, task division for offloading, reliability, integrity of data delivered, scalability of MCC without degradation in performance or change in infrastructure, security of data in mobile device within a cloud and in the communication channel, identity privacy, location privacy, etc. These challenges are the biggest obstacles in growth of mobile cloud computing. According to the literature [1,2] 74% of IT Executives and Chief Information Officers are not willing to adopt cloud services due to the risks associated with security and privacy. In MCC the security threats are likely in various segments viz. mobile device, communication channel or the cloud itself. So one has to provide protection from these threats by having secure cloud application services in mobile devices and cloud, secure routing protocols in communication channel and secure virtualization in cloud architecture. According to review of the current approaches in MCC [3], the security framework for MCC is divided into two categories; Data Security framework and Application Security Framework. Data Security frameworks are compared on the basis of their basic theory –mathematical principle or cryptographic principle, data protection –protection of data created or manipulate on device or data created or manipulate on cloud, data integrity, scalability, assumption of components-fully trusted, semi trusted or distrusted, data access automated or semi automated and authentication of originator of file. Application security framework can be compared on the basis of application type, security features like data security, integrity, identity privacy, location privacy, authentication, secure data access

[*] Corresponding author : MM Chaturvedi (email :mmchaturvedi@ansaluniversity.edu.in , +919871078151 (m))

management or secure routing, assumption of component trust levels, scalability of framework. Each security framework must be viewed with its security strength and resource usage. In security strength we take care of confidentiality, integrity, authentication parameters. In resource usage we consider memory usage, processing time and network overhead parameters [4].

In this paper, section 2 reviews the related literature on cloud computing, MCC and various security aspects of mobile and cloud computing. Section 3 deals with the overall architecture of the proposed plan elaborating on need of cloud computing in 3.1, features of mobile cloud computing in 3.2, objective in 3.3. Section 4 describes the possible validation approaches to test the design objective. Section 5 lists out the challenges involved in the research objectives whereas section 6 concludes the paper highlighting the possible outcome of this research work.

2. Related Work

Security and privacy issues of MCC have been discussed by many researchers. J. Oberheide et al [5] proposed Cloud AV platform, malware detection system for mobile device by moving detection capabilities to network service or cloud. Zhang et al [6] present security framework for elastic mobile application model by dividing an application into easily configurable weblets. Xiao and Gong [7] proposed scheme for mobile cloud environment to generate a dynamic credential for mobile user for their identity protection from hackers. Wang and Wang [8] have proposed privacy preserving framework for mobile devices while using location based scheme by spatial cloaking. Huan et al [9] presents framework –MobiCloud to enhance the functionality of MANET and cover security aspect in terms of risk management and secure routing. G. Portokalidis et al [10] proposed scheme for threat detection in a smart phone with Mobile Cloud Computing. H.Zhang and X Mingjun [11] proposed distributed spatial cloaking protocol for location privacy. P.Zou et al[12] propose Phosphor, a cloud based mobile digital right management scheme with Sim Card by designing License state word . R.Chow et .al [13] present policy based cloud authentication platform using implicit authentication for solving privacy issues. Itani et al.[14] proposed an energy efficient framework for mobile devices by using incremental message authentication code to ensure integrity of mobile users. Jia et al[15] presents proxy re-encryption (PRE) scheme and identity based encryption (IDE) scheme to achieve secure data service. Huangs et al.[16] proposed secure data processing framework for MobiCloud addressing issue of authentication on cloud. Hsueh et al [17] Proposed authentication mechanism to ensure security and integrity of mobile users files stored on cloud server. Yang et al.[18] extended the public provable data possession scheme with Diffie Hellman Key Exchange, Bilinear mapping and Merkle Hash Tree (MHT). Chen et al [19] present security framework for location based grouped scheduling services for identity privacy and authentication. Ren et al [20] proposed three schemes; encryption based, coding based and sharing based to ensure the confidentiality and integrity of user's file stored at cloud. Zhou and Huang [21] proposed a privacy preserving framework by offloading the processing and storage intensive encryption and decryption on cloud based on Cipher text Policy attribute. Current research initiatives seem to address only one or two parameters of security from the comprehensive set of authentication, integrity, confidentiality and privacy. These research approaches favor static security algorithms without considering changing demand for security, quality of service, and resource usage of mobile users.

3. Architecture of the model proposed to be explored

3.1 Cloud Computing

The Cloud Computing is gaining popularity with its main advantage of reducing the computational burden of the client and thus reducing the complexity and other infrastructure requirements at the client end. However, it is important to realize that the market is still deprived of cloud service providers because of following important issues:

- Data replication
- Consistency
- Limited scalability
- Unreliability
- Unreliable availability of cloud resources
- Portability
- Trust
- Security
- Privacy

The commonly accepted definition of Cloud computing is an IT service being provided to users on demand and being paid for depending upon amount of usage. It can also be termed as a dynamic service being provided to users that can

add on to the available capacity and capabilities of user entity. Some of the key services of Cloud Computing as depicted in Figure 1 are:

- Infrastructure as a Service (IaaS)
- Data storage as a Service (DaaS)
- Communication as a Service (CaaS)
- Security as a Service (SecaaS)
- Hardware as a Service (HaaS)
- Software as a Service (SaaS)
- Business as a Service (BaaS)
- Platform as a Service (PaaS)
- Virtualization

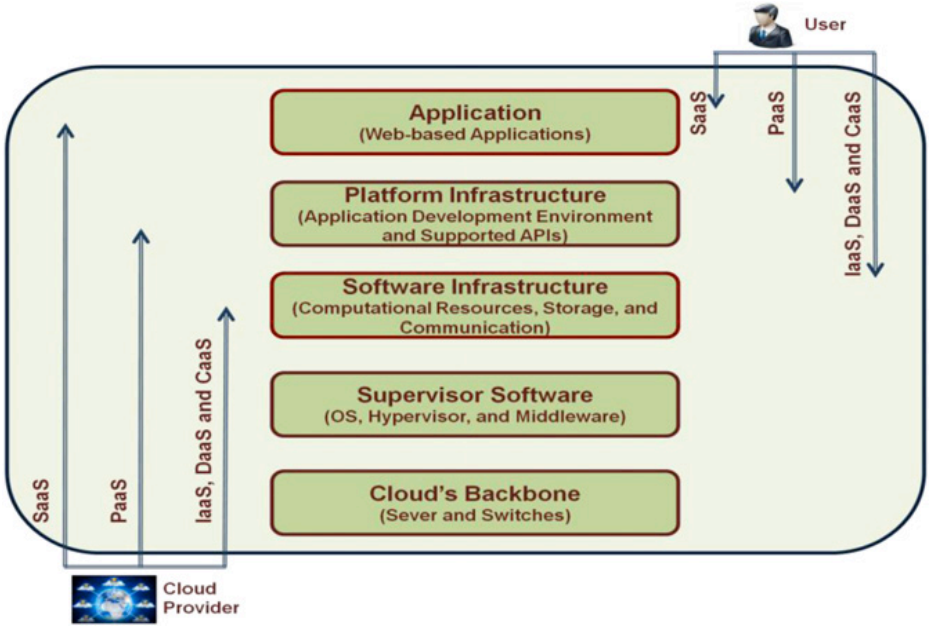

Fig. 1. Layered Architecture of Cloud Computing [3]

3.2 Mobile Cloud Computing

The application of cloud is possible in many domains. One of the domains of our current interest is that of mobiles. Hence, we will be focusing on utility of cloud computing environment for mobile usage and how can a cloud add value to the overall functionality and performance of mobile devices? According to Khan et al [3] as depicted in figure 2, MCC is a service that allows resource constrained mobile users to adaptively adjust processing and storage capabilities by transparently partitioning and offloading the computationally intensive and storage demanding jobs on traditional cloud resources by providing ubiquitous wireless access.

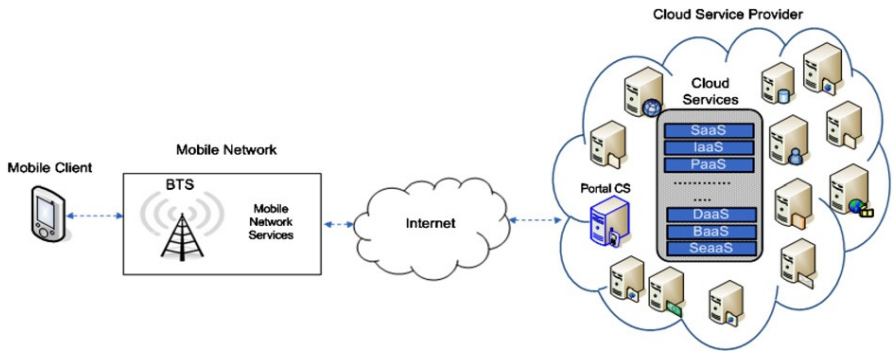

Fig. 2. Mobile Cloud Computing Architecture [3]

Some of the limitations of mobile devices which drive use of Cloud Computing for mobile devices are:

- Limited battery
- Limited processing power
- Low storage
- Less security
- Unpredictable Internet connectivity
- Less energy

3.3 Research Objective

Our research objective is to propose and develop a system in which security protocols can be decided for a mobile entity dynamically in a cloud. For this, we will be focusing on not just the mobile security parameters but also on the cloud security related issues and respective parameters. As suggested by Khan et al [3], the security and privacy protection services can be achieved with the help of secure cloud application services. Figure 3 describes the security services necessary at various layers of the supporting cloud. In addition to security and privacy, the secure cloud application services provide the user management, key management, encryption on demand, intrusion detection, authentication, and authorization services to mobile users. There is a need for a secure communication channel between cloud and the mobile device. The secure routing protocols can be used to protect the communication channel between the mobile device and cloud.

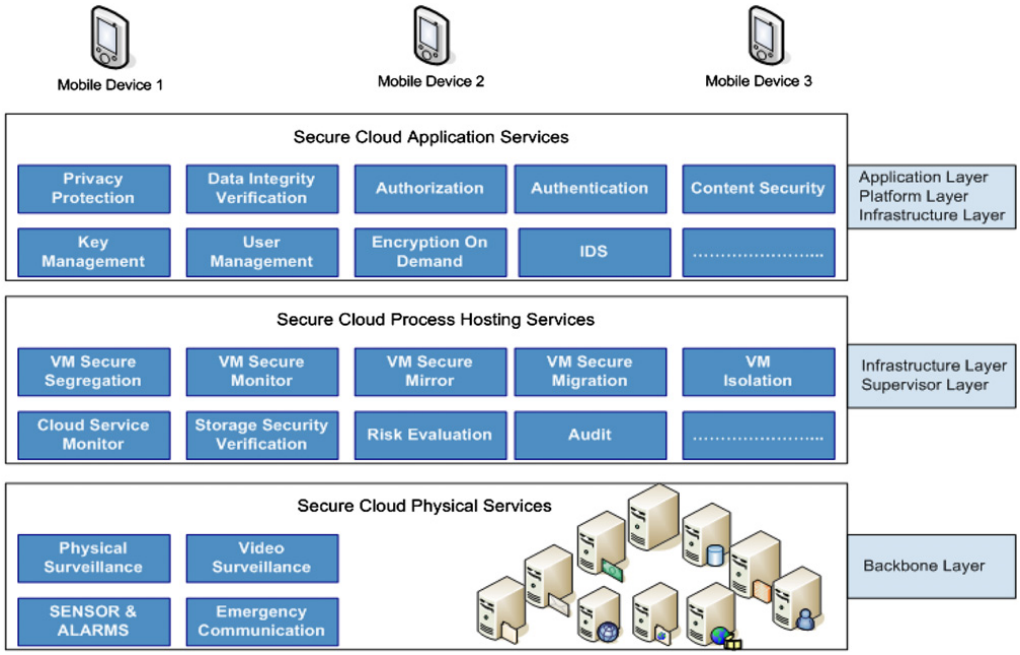

Fig. 3. Security services on different layers [3].

The key illustrative areas of proposed research are:

- Preparation of semantic data for security parameters
- Cloud Security attributes
- Mobile Security features and respective parameters
- Security protocols under different security requirements
- Platform Independent Security Architecture.

In the work of Khan et al [3], frameworks of various aspects of security features have been described in detail. As suggested by Rocha et al [4], a security service can be devised which works as a middleware with the ability to change the security protocols dynamically between two peers. In their work, domain is of independent mobile users.

We propose to expand this concept to a cloud where a number of mobile users will be acting as members of the cloud and will exchange information within the cloud. For this we need to define various levels of security. A mobile may require different levels of security at different times depending upon the service being used and the sensitivity of the data exchanged with the peer.
Broadly the proposed research could address following questions:

a) What could be semantic data for mobile and cloud security?
b) How the Protocol Selection Procedure can be made intelligent with option for static protocol selection when necessary?
c) How workload could be partitioned between mobile and cloud after factoring various related issues?

The following options need to be evaluated to arrive at a possible mix to answer the framed research questions:

a) As proposed by Zissis & Lekkas [22], a trusted third party could be tasked with assuring specific security characteristics within a cloud environment.
b) Identification of appropriate security parameters for a mobile and cloud with their dependency matrix to suggest a security metric towards security of a mobile cloud computing application.
c) Generation of semantic data which facilitates selection of the security protocol by the middleware. Intelligent protocol selection process would help conserve resources. This would permit use of already selected protocol if the semantic data values are unchanged.
d) If the security requirement between two peers is same over a period of time, then repeated overhead of security parameter collection and protocol selection for every information exchange can be avoided by choosing the relevant security protocol for stipulated time duration before entering dynamic protocol selection mode as necessary.
e) Security related work could be partitioned between the mobile and the cloud with computationally light tasks handled by the mobile itself and heavy tasks outsourced to the cloud.

4. Proposed Validation approaches

Validation is done at the end of the development process and takes place after verifications are completed i.e. determining if the system complies with the requirements and performs functions for which it is intended and meets the stated goals and user needs [23].
The validation of the proposed research is to establish that it is adaptive in nature for several contexts and leads to benefits both in performance and ease to use and according to the type of user dependent data transfer. The designed software should permit the application to determine different semantic values for each part of the data to be transmitted, and thus addresses the main concern of the user viz. enhanced security.

Cloud based Mobile Computing Testing practices:-

It is important to take into consideration the additional time and/or personnel needed to perform exhaustive tests on all the devices eg according to Rocha & Costa[4] in the proposed middleware which is a system software responsible for managing the transparent execution and interaction among the jobs running on the cloud servers, it is mandatory to test these system software like OS and Hypervisor of the cloud .So the types of testing that is to be planned for the cloud system software are, Performance Testing, Capacity Testing, Fail-over Testing, Browser testing[24]

- **Application security testing**. This type of testing is done to secure application software that is running on or being developed in the cloud.
- **Governance Risk Compliance (GRC) testing.** Its main focus is to list threats, vulnerabilities and risks that are associated to all three parts of Cloud Computing – Infrastructure as a Service (IaaS), Platform as a Service (PaaS) & Software as a Service (SaaS) and suggest controls which have been assimilated from the best practices prevailing in the Industry.
- **Latency Testing.** Cloud testing is utilized to measure the latency between the action and the corresponding response for any application after deploying it in the cloud.

Issues and Challenges in Cloud Testing

There are a number of issues and challenges in testing clouds and cloud-based software. Here we discuss them from the following four areas.

- *On-demand test environment construction* – How to set up a testing environment systematically (or automatically) for on-demand testing services in a cloud? Although the current cloud technologies support automatic provision of required computing resources for each SaaS (or application) in a cloud, there are no supporting solutions to assist engineers to set up a required test environment in a cloud using a cost-effective way. It is necessary to provide an on-demand test environment for TaaS customers, Iaas customers, Daas customers etc.

- *Scalability and performance testing* – Although many published papers discuss system performance testing and scalability evaluation in the past two decades, most of them address issues and solutions in conventional distributed software or web-based software systems. According to our recent literature survey on this subject, most existing papers focus on scalability evaluation metrics and frameworks for parallel and distributed systems.

- *Testing security and measurement in clouds* – Security testing has becoming a hot research subject with many open questions in current software testing community. Since security becomes a major concern inside clouds and security services become a necessary part in modern SaaS and cloud technology, engineers must deal with the issues and challenges in security validation and quality assurance for SaaS and clouds.

5. Key Challenges in the proposed research

The key challenges that we anticipate are:

a) During experimentation the simulator being used should acquire necessary information from both the OS and through the wireless medium.
b) Balance between security and maintaining communication quality and system performance.
c) We should provide a single security layer for different contexts of hardware, software and communication modes.
d) Need for the data semantics so as to determine different sensitivity levels of the data being transmitted, facilitating strong security mechanism only when they are actually needed rather than on the whole data.
e) In the proposed approach the appropriate metrics and the parameters should be defined to facilitate objective evaluation of our approach.
f) Design of a Platform Independent Security Architecture so that we can deploy lightweight part of security Framework on any Mobile device could pose interface issues.

6. Concluding Remarks

This paper has attempted literature review of various approaches for effective deployment of secure mobile cloud computing paradigm.
Challenges and possible options have been delineated while we try to explore and characterize an adaptable and dynamic framework providing configurable security interface at the application layer.
Issue connected with validation and testing of proposed solution have also been considered to help us formulate dependable testing and benchmarking of a security firmware in the context of mobile cloud computing.
The fallout of the proposed research is expected to be of interest to both E-governance and E-commerce applications and interlinking with Trust, privacy and security. The challenges in this evolving field of research are many and we plan to proceed in phases with first phase attempting to characterize the problem in formal terms and propose a lightweight mobile interface having limited dynamic capability. We look forward to international cooperation afforded by this BIC/DIMACS/A4Cloud workshop participation, leading to a later phase of expanding the objectives.

References

1. Subashini,S. ,Kavitha,V.: A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications 34 (1) 1–11 (2011).
2. Buyya,R.,Yeo C.S.,Venugopal,S., Broberg,J.,Brandic I.: Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems 25 (6) (2009) 599–616
3. Khan,A.,N.,Mat Kiah,M.,L., Khan S.,U.,Madanic,S.A. :Towards secure mobile cloud computing: A survey, Future Generation Computer Systems 1-22 (2012)
4. Bruno P.S.Rocha,Daniel N.O.Costa,RandeA.Moreira,ristianoG.Rezende,Antonio A.F.Loureiro, Azzedine Boukerche : Adaptive security protocol selection for mobile computing, Journal of Network and Computer Applications (2012)
5. Oberheide,J., Veeraraghavan,K., Cooke, E., Flinn, J., and Jahanian, F.. :Virtualized in-cloud security services for mobile devices, in Proceedings of the 1st Workshop on Virtualization in Mobile Computing (MobiVirt), pp. 31-35, (June 2008).
6. Zhang, X., Schiffman, J. , Gibbs ,S., Kunjithapatham, A., Jeong, S.: Securing elastic applications on mobile devices for cloud computing, in Proceeding ACM workshop on Cloud computing security, CCSW ’09, Chicago, IL, USA,(Nov. 2009.)
7. Xiao, S., Gong, W.: Mobility can help: protect user identity with dynamic credential, in: Proc. 11th Int. Conference on Mobile Data Management, MDM ’10, Missouri, USA,(May 2010)
8. Wang, S., Wang, X.S.: In-device spatial cloaking for mobile user privacy assisted by the cloud, in: Proc. 11th Int. Conference on Mobile Data Management,MDM ’10, Missouri, USA,(May 2010).
9. Huan,D., Zhang, X., Kang ,M., Luo ,J.: MobiCloud: building secure cloud framework for mobile computing and communication, in: Proc. 5th IEEE Int. Symposium on Service Oriented System Engineering, SOSE ’10, Nanjing, China,(June 2010).
10. Portokalidis,G.,Homburg,P.,Anagnostakis,K., Bos,H.: aranoid Android: versatile protection for smartphones, in Proceedings of the 26th Annual Computer Security Application Conference (ACSAC), pp. 347-356, (September 2010).
11. Zhangwei ,H. and Mingjun ,X., : Distributed Spatial Cloaking Protocol for Location Privacy, in Proceedings of the 2nd International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC), vol. 2, pp. 468,(June 2010.)
12. Zou,P., Wang,C., Liu ,Z., and Bao ,D.,: Phosphor: A Cloud Based DRM Scheme with Sim Card, in Proceedings of the 12th International Asia-Pacific on Web Conference (APWEB), pp. 459, (June 2010).
13. Chow, R., Jakobsson, M., Masuoka, R., Molina, J., Niu Y., Shi ,E., Song, Z. :Authentication in the clouds: a framework and its application to mobile users, in: Proc. ACM Cloud Computing Security Workshop, CCSW ’10, Chicago, USA,(Oct. 2010.)
14. Itani,W., Kayssi,A., Chehab, A.: Energy-efficient incremental integrity for securing storage in mobile cloud computing, in: Proc. Int. Conference on Energy Aware Computing, ICEAC ’10, Cairo, Egypt, (Dec. 2010.)
15. Jia,W., Zhu ,H., Cao, Z., Wei, L., Lin, X.,:SDSM: a secure data service mechanism in mobile cloud computing, in: Proc. IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS, Shanghai, China,(Apr. 2011).
16. Huang,D., Zhou,Z., Xu,L., Xing,T., Zhong,Y:Secure data processing framework for mobilecloud computing, in: Proc. IEEE INFOCOM Workshop on Cloud Computing, INFOCOM ’11, Shanghai, China, (June 2011.)
17. Hsueh ,S.,C., Lin ,J.Y., Lin, M.Y.,: Secure cloud storage for conventional data archive of smart phones, in: Proc. 15th IEEE Int. Symposium on Consumer Electronics,ISCE ’11, Singapore, (June 2011.)
18. Yang ,J., Wang, H., Wang, J., Tan, C., Yu1, D.: Provable data possession of resource constrained mobile devices in cloud computing, Journal of Networks 6 (7) 1033–1040 (2011).
19. Chen,Y.,J., Wang,L.,C.: A security framework of group location-based mobile applications in cloud computing, in: Proc. Int. Conference on Parallel Processing Workshops, ICPPW ’11, Taipei, Taiwan, (Sep. 2011.)
20. Ren,W., Yu,L., Gao,R., Xiong,F.: Lightweight and compromise resilient storage outsourcing with distributed secure accessibility in mobile cloud computing, Journal of Tsinghua Science and Technology 16 (5) 520–528 (2011).
21. Zhou,Z., Huang, D.: Efficient and secure data storage operations for mobile cloud computing, IACR Cryptology ePrint Archive: 185, (2011).
22. Dimitrios Zissis, Dimitrios Lekkas,: Addressing Cloud Computing Issues, Future Generation Systems (28) 583-592 (2012).
23. ISTQB Exam certification .com Webpage-http://istqbexamcertification.com/what-is-validation-in-software-testing-or-what-is-software-validation/

24.Belatrix cloud testing best practices, Belatrix Software Factory-White papers http://www.belatrixsf.com/index.php/outsourcing-case-studies/131

About The Authors

Manmohan Chaturvedi is a retired Air Commodore from Indian Air Force with PhD in Information Security domain from IIT Delhi. He has about 35 years of experience in managing technology for IAF. An alumnus of National Defense College, New Delhi, he has held various appointments dealing with operational and policy dimensions of Information and Communication Technology. He graduated from Delhi College of Engineering and completed post graduation from IIT Delhi. Currently he is a Professor at School of Engineering and Technology, Ansal University with research interests in vulnerability of evolving ICT infrastructure and protection of Critical Information Infrastructure.

Sapna Malik is a Ph.D. candidate at the School of Engineering and Technology, Ansal University,India. She holds a M.Tech in IT from GGSIPU, New Delhi,India and B.Tech in CSE from Mayarishi Dayanand University,India.She is working as Assistant professor in department of Computer Science Engineering in Maharaja Surajmal Institute of technology ,Delhi,India.Her
Research interest includes Cloud computing, Network Security and Virtualization.

Preeti Aggarwal holds an M.Tech in IT from GGSIPU, New Delhi, an M.Sc in Informatics and a B.Sc (H) in Electronics from University Of Delhi and is currently pursuing Ph.D. in Data Mining and Information Security from Ansal university, Gurgaon. She is working as an Assistant Professor in department of Computer Science Engineering in KIIT College of Engineering, Gurgaon. She is also a member of Computer Society of India.

Shilpa Bahl holds M.Tech in IT from UIET, Krukshetra university ,Kurukshetra and B.Tech in Electronics & communication From Kurukshetra university and is currently pursuing Ph.D. in Software testing and Information Security from Ansal university, Gurgaon. She is working as an Assistant Professor in department of Computer Science Engineering in KIIT College of Engineering, Gurgaon, having Six years of teaching experience in Computer Science department

Trust Management in Emerging countries: International cooperation research challenges for Horizon 2020

James Clarke[1], Marijke Coetzee[2], Manmohan Chaturvedi[3], Abhishek Sharma[3]

Karima Boudaoud [4], Mounib Mekhilef[5], Jan Eloff[6], Donovan Isherwood[2,6]

[1] Waterford Institue of Technology, Waterford, Ireland. jclarke@tssg.org

[2] University of Johannesburg, South Africa. marijkec@uj.ac.za

[3] Beyond Evolution Tech Solutions Pvt. Ltd., India, {mmchat@sify.com and abhishek.sharma@beyondevolution.in}

[4] I3S Laboratory - University of Nice Sophia Antipolis/CNRS, France, karima@polytech.unice.fr

[5] Ability Europe Ltd, United Kingdom, mounib.mekhilef@abilityeurope.com

[6] SAP Meraka UTD, CSIR, Pretoria, South Africa; Department of Computer Science, University of Pretoria, Pretoria, South Africa, jan.eloff@sap.com

Abstract. An international cooperation approach to trust management that considers cultural differences appears necessary if we would like to design multi-cultural trust models that can be understood and used by different cultures. The cultivation of trust is critical for the success of both the Internet economy and m-commerce. In this context, consumer trust is generally defined in a uniform manner, as if all participants behave in the same way. Current research indicates that culture has a major effect on the formation of consumer trust and the risks that consumers are willing to take. To ensure the successful uptake of m-commerce in emerging economies such as Brazil, India and South Africa, it is imperative to investigate culturally adapted trust requirements, properties and models. Countries in the EU, consisting of many different cultures, can also significantly benefit from this research. To this end, the BIC project has brought together researchers from different countries and cultures to collaborate on topics related to culture and trust. The common denominators and differences found amongst cultures can provide deep insights than can be applied to the design of useful security and privacy applications. This paper reports on the project development, provides some of the research perspectives of participants, and invites collaboration from interested parties for future collaborations. A combination of bilateral and multilateral approach may emerge as we traverse the research path.

Key Words: Trust models for online Transactions, International Cooperation, Cloud Computing, Privacy and Security.

1 Introduction

During the BIC workshop in June 2012, one of the Working group sessions (WG1 – Human Oriented approaches to Trust and security) held discussions on various trust aspects and how research between the EU and the emerging countries could enlighten more on potential solutions for trust management [1]. Trust models implemented in currently available technology are developed based on the principles of trust as a social phenomenon within the context of the western world. Indeed, the majority of the research on these topics has come from westernized or individualistic cultures, where consumer trust is facilitated through trust mechanisms such as institutional guarantees, laws and policies, information security

mechanisms, and social controls. Examples of such trust formation are manifested by the number of positive experiences and recommendations between entities in a trust community such as eBay. As stated by Jill Slay and Gerald Quirchmayr from the University of South Australia [2]: "It is therefore important to establish explicit conditions whereby the potential user can easily be assured that an application is trustworthy. A specification for and management of Trust is, therefore, necessary in the development of Internet-based services. Trust is specified by formal mathematical models and coded into software applications but current theoretical work has not led to the development of widely accepted tools and techniques for analysing trust [3]. Some authors have run surveys to capture trust challenges by the analysis of existing applications [26]. This gave a very IT oriented understanding of the real nature of trust-building in large networks. Others such as Abdul-Raiman, A. & al in [22] studied the way to establish trust in virtual communities; Butler J.K in [22] who considered from the management perspective the way to measure trust as a tool to build confidence from the end-users perspective. Dafoulas & al [25],Hofstede [26] and Hofstede [28] raised the issue about cultural differences for trust and the way to design software to tackle this challenge.

With the proliferation of mobile technology within emerging countries and the impetus it has already given to the formation of innovative business models, such as virtual co-operative buying ecosystems, there is already an acute need for technology that will instill trust within the user community. For example, the user community in Africa is characterized by small to very small enterprises conducting their whole business from a mobile phone [4] [5]. These enterprises run profit ecosystems rather than business units that interact with other ecosystems in a culturally involved manner to ensure that the ecosystem will survive in the face of adversity. Social capital and social ties support these ecosystems and communities in large parts of Africa where members of communities pool resources together in an attempt to meet economic and social needs for both individual members and the general community. The international research results to be delivered by this initiative should, therefore, aim in conceptualizing trust mechanisms that operate seamlessly in a mobile-cloud infrastructure supporting such ecosystem.

Within the BIC project, one of the objectives is to find trust and security topics of mutual interest and benefit to collaborate on. Trust management in emerging countries is of significant interest not only to those in the African context, but to any environment where different types of cultures exist, including the EU, and where an understanding of the influence of culture on trust is limited. Considerable amounts of research still has to be done on identifying the unique properties/requirements related to trust used by people in collectivist cultures and how this can be captured by mobile technologies in order to support and grow business ecosystems.

To move the topic forward from the June workshop, the BIC project organized an open workshop on 27th November 2012 [6] where the concentration was on this research topic to put us in a better position to form consortia that can work on research/development/implementation/ stages for this work. There were a number of participants showing particular interest in this area, especially from Africa, India and the EU and are already discussing the potential for setting up a consortium on the topic. This paper further elaborates on this topic from the perspective of the EU, India and South Africa and how these countries can help each other in carrying out the required research elements associated with the topic in the future as we move towards Horizon 2020.

2 Trust Management – Why do we need International Cooperation (INCO)?

The basic premise for studying the need of INCO for Trust Management is driven by the fact that individuals, communities, and groups, from practically every country across the globe, are heavily dependent upon electronic transparent solutions and services, originating from any part of the globe. Not only is the commonly known e-money or e-commerce used, but practically entire gamut of human needs such as e-health, e-learning e-government serviced through electronic means. Even social interactions between people and communities across the world, unknown or unconnected to each other through applications like Facebook are a common practice.

However the need of the people, their perception about and *acceptability* of these solutions, services or social interactions are not uniform across different countries, communities and cultures; and depend heavily on the "Trust Perception" of those people or that community. In all of these, the cultures of a country, community or group of people play a major role in the acceptability and Trust. Typically, vast countries like India, which has many culturally unique and independent communities within the country, also face a similar situation. Hence the simple question – can the same solution, service, literature, art, commerce, ideas or views be equally acceptable and useful across different communities with their different cultures? The answer to this simple but important question is obvious. There are bound to be significant variations, gaps and absence of uniformity in Trust perceptions. However the need is to moderate these variations, bridge the gaps and create a system that is aimed at providing maximum possible uniformity. This critical challenge of achieving a reasonable degree of uniformity in Trust perceptions could be made possible by exploring common factors that affect consumer trust in online transactions across the cultural diversity. In many cases, the base may be same common function e.g. e-money transfer, the way it needs to be pitched to the people to interact or utilize – the User Interface (UI) may need to be different to suit different "Trust Perceptions" of different cultures. This basic necessity, in our globalised world, to develop a "Trust model", factoring cultural variations suggests utility of international cooperation in "Trust Management" research.

Considering the question - "Why do we need INCO for Trust" - further, the first obvious response is that when talking about trust, we need to understand how trust develops and how the culture of a society or a nation impacts the trust-building process. This concept has not the same meaning in Europe or America and in Asia and South Africa due to the fact that in Europe and the United States, the predominate culture is of individualistic nature, whereas in Asia, India and South Africa, it is a more collectivist [4]. In addition to the fact that culture has a major influence on trust, culture is not the only criteria to consider when talking about trust, but societal values, language differences have also an impact on trust. Thus, trust needs can be and are different from a culture or a country to another one. One can refer to the work done by Hofstede's on cultural dimensions. Hofstede [7] defines culture as "the collective programming of the mind that distinguishes the members of one group or category of people from another". A trustor decides whether and who to trust based on the culture of the group he/she belongs to. He identifies the dimensions of power-distance (the level to which a society accepts the equality or inequality distribution of power), collectivism vs. individualism (relationship between the individual and the group), femininity vs. masculinity, uncertainty avoidance (how societies accept high levels of uncertainty and ambiguity) and long-term vs.

short-term orientation. One of the greatest impacts of culture is therefore on how information is used to make trust decisions. Developing an integrated model of trust to address this issue is particularly difficult, given the vagueness and peculiarities in defining trust across multiple cultures.

The next question raised is how to understand and manage trust for emerging countries. There is a need to develop trust models using a multi-lateral and multi-cultural approach that first involves the end-users and listens to their trust needs; and then translates these trust needs into parameters that makes sense to these end-users.

2.1 How to build trust models for emerging countries?

Several powerful trust models [8][9][10][11][12][13] have been proposed to model trust in different contexts (wireless networks, sensors networks, etc.). These models use mathematical models that can be enough for this kind of context. However, if we use them in other contexts that involve the Human, such as social networks, they are of no use, as they do not take into account cultural factors. A very good example is a study that has been conducted for online shopping and e-commerce where it has been proven that the trust model used by e-Bay does not suit Asian users' expectations [14][15].

In order to determine the effect of culture on trust, we need to understand how trust generally develops. Previous research [16] indicates that trust is initially formed by "hard" mechanisms such as certificates and algorithms, seen at the bottom of the Table 1, but as time passes and positive experiences are recorded, "soft" mechanisms such as human judgement increase trust levels. Initially, competence trust is formed on the basis of identity, implemented security mechanisms and best practice of partners as shown by information layers 1 and 2 at the bottom of the table. References and recommendations, shown in information layers 3 and 4, will further increase competence trust. Next, predictability trust is the result of established experience, as shown in information layer 5. Finally, after time, goodwill trust is formed, as is shown in information layer 6.

Table 1: Information layers and sources of trust formation

	Information Layer	**Source of information**
soft	**6.** Goodwill	Human judgment
	5. Experience	Volume of transactions, history, behavior, social network position
	4. Recommendations	Situation-specific values
	3. References	Certificates, assurances, licenses
	2. Technology	Security mechanisms, best practice
hard	**1**. Identity	Digital certificate, password, Kerberos ticket

A specific research question to be answered is how each of these layers are influenced by culture? One may assume that information layer 1, where "hard" mechanisms such certificates are used to establish trust, may not be much affected by the influence of culture. On the other hand it may be possible that layer 6, where human judgment resides, may culturally discount the impact of identity trust. Layers 4 – 6 are directly influenced by human behaviour, and will thus influence trust management in emerging economies.

A further research question to address is how the perspectives from e.g. Africa, India and Europe view this issue, what do they see as important to their environment? To date, trust models and mechanisms have been developed by researchers from cultures such as the USA, UK, Germany and others with a predominately individualistic approach. These models focus on environments with *low power distance* where citizens have equal rights, *individualistic* societies where citizens are self-reliant, more *masculine* societies where the winner takes all, where citizens are more *accepting of uncertainty* and more easily take risks and a *short-term oriented* culture that is very driven to achieve tangible and direct results. In contrast to this, trust mechanisms and models have to adapt to emerging economies by incorporating *high power distance* where hierarchy between people is important, *collectivist* society where citizens are strongly bound to a group that provides protection, more *feminine* societies that avoid conflicts and are more easy-going, *less accepting of uncertainty* by having many rules in place to ensure structure and security and have a *long-term oriented* culture with more tolerance for different truths.

In e.g. Africa, Asia, India and South America, structures embedded in the society are thus much more relevant. The principle of similarity from a societal point of view can be considered as one of potentially many different and important parameters in building trust models that are also of relevance to the developing world. A study [17] on acceptance of security solutions for the end-users and analysed through the well-known Schwartz circumplex (10 dimensions of values) puts into perspective values that matters to different cultures. Once their existence is by nature universal, the importance that we give depends on local perceptions. Hofstede in [29] run also a similar study to spot the cultural differences in values.

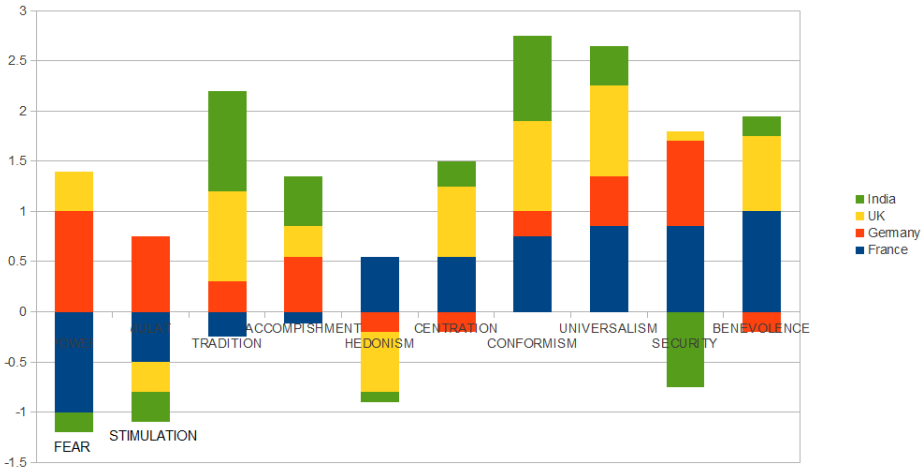

Figure 1. Differences in term of hierarchisation of values between some countries.

As an example, it is shown that a value such as Fear is not considered equally important by different cultures. When designing for trustworthiness there are major challenges to be considered using these values such as the adaptation and parameterization of user interfaces, the nature of the services and the manner in which they need to be delivered. Solutions will not be optimal and efficient if they are suggested by a unique culture. While this could appear as a very constrained problem, we know also that innovations do not manifest in a non-constrained system. An innovative approach to capture this diversity and suggest approaches in "Trust Management" ,that thrive rather than get constrained by this phenomenon, could be an objective of proposed research.

This research now proposes a definition of trust management for emerging countries to guide its development, adapted from Grandison [18] "*The activity of collecting, encoding, analysing and presenting evidence relating to competence, honesty, security or dependability, with the purpose of making assessments and decisions regarding trust relationships, while at the same time considering the influence of culture and beliefs*."

As a consequence, to build trust models and mechanisms for emerging economies, we need to extend existing trust management models by cultural aspects.

A provisional set of trust management research challenges and criteria are now defined to guide this research project holistically as follows:

- Gain an understanding of existing cultural frameworks to determine the most suitable framework to use to extract cultural behaviors and beliefs.
- Determine how individualist cultures have influenced the development of trust management to date.
- Determine the manner in which current trust management systems not meet the needs of collectivist cultures at each of the identified layers of the trust development framework.
- Identify specific trust mechanisms that can be adapted for collectivist cultures to better suit their needs.
- Define and develop culturally specific trust mechanisms and models to address the needs of a cultural group.

Having observed and analysed the above described information layers which are influenced by cultures and hierarchy of values at different countries and societies, there is another aspect of the cultures and societies that is apparently left untouched by the researchers is the existence of "Culture Revolutionaries (CR)". In every culture and society, there are invariably a small section of people who think and act differently than the thinking and behaviour of the rest of the society and its culture. The attributes of these people can be briefly described as:

a Logical and Bold.

b Logical but Timid.

c Logical but Indifferent.

Keeping in mind the primary objective of the INCO in "Trust & Management" is to bridge the gaps in the thinking and behaviour between cultures. Is it possible to bring about a certain degree of uniformity in their thinking and behaviour towards "Trust Aspects", particularly in the fields of Technology utilization such as e-commerce and others. Areas where the acceptability of any useful technology gets adversely affected due to cultural influences on the aspects of Trust on Technologies can be examined to develop an organic approach across the different cultures. It is this context that we need to look at these "Culture Revolutionaries" who can work as "Change Agents". It is these CRs who, being part of the same cultural background but of different thinking and beliefs could be the most effective and can bring about significant change in the desired direction.

Out of the three categories of the CRs described above, the common element is the "Logical Thinking". The first one "Logical & Bold" are of immediate and maximum relevance, however those in the second and third categories can also be motivated and transformed to various degrees to make some contribution to the objective.

In view of this additional angle of the analysis of people belonging to a culture, the aim of finding ways and mechanisms for initiating the organic of transformation and later possibly achieving a wave of change, one more element in the above set of trust management and research challenges may be listed as follows:

- Make special effort to locate and identify such "Culture Revolutionaries" within a target culture/ society and
- Create a motivating environment for such CRs to become the Change Agents (CA) and prime drivers for bridging the culture gaps and bringing about the necessary uniformity.

2.2 How INCO can help and how to best move forward?

From an international point of view, different actions are required [19].

Collaboration is needed with international security experts that have a user-centric approach regarding trust, privacy and security (Brazil, India, South Africa, Canada, USA, France, etc.), international experts from different disciplines to take into account the differences in terms of culture, laws, etc and collaboration with international standardization organisations such as W3C, ETSI, IETF, etc. These collaborations can start through the creation of multidisciplinary working groups in each targeted country (right experts from each discipline). This is already started in the BIC project WG1 and more participants are most welcome to participate.

Organization of international multidisciplinary workshops in targeted countries (involving wider public) is needed. As far as we know, a World Wide trust model does not exist and this is mainly due to the complexity of the problem as it implies Human and cultural factors which can only be investigated comprehensively by involving people and researchers from different cultures.

This kind of model requires the coverage of various regions in the World (India, China, South America, South Africa, etc.) to suit different cultural regions and languages. The only way to be able to do it is to create and strengthen collaboration between trust experts from different cultures. This can be done through international cooperation and more specifically, international workshops and working groups.

We believe that using an international cooperation approach for a trust taking into account cultural differences is mandatory if we would like to design a multi-cultural trust model that can be understood and used by different cultures.

3 Cultural perspectives on trust research

At the BIC workshop in November 2012, a number of perspectives documenting the ongoing research being carried out (or needs for) on this topic were presented for two of the BIC countries – South Africa and India. Those efforts are summarized here.

3.1 South Africa

3.1.1 Introduction – the need for INCO

A research topic identified for international cooperation is the development of trust requirements, properties, models and mechanisms to support business ecosystems in rural Africa that are supported by mobile and cloud technology [4][5]. For these systems, it is important that trust management takes into account the culture of the target group, namely the collectivist rural African culture.

3.1.2 Research challenges

The research challenges needed to address trust models for collectivist rural African cultures are defined to address the research challenges of this project:

- A study of the work of Hofstede on culture to extract cultural behaviors and beliefs that are applicable to the rural African consumer;
- A study of state-of-the-art peer-to-peer trust models to identify properties and mechanisms that can be used by mobile and cloud-based applications supporting business ecosystems in collectivist rural Africa;
- The identification of new trust requirements, properties and models to support cultural behaviours and beliefs of collectivist African communities;
- The implementation and evaluation of a prototype system to determine if a culturally adapted trust model can successfully be used in collectivists rural African communities.

3.1.3 Objectives

The main focus of this research on trust focuses on layers 4-6 of Table 1. The focus is on identifying how rural collectivist African consumers understand and use trust information such as recommendations and assurances, and to build into trust evaluation the social position of consumers, retailers and suppliers. This research is not so much focused on technology

trust, but rather on how culturally specific behaviour influences the development of trust to ensure the growth of a business ecosystem. These research objectives are of interest not only to the African context, but to any environment where different types of cultures exist, and where an understanding of the influence of culture on trust is limited. It is therefore a topic that is ideal for collaboration between parties found in different countries in Europe, Africa, India and Brazil. The long-term expected outcome of this work would be a more generic framework that supports the ability to adapt trust models to culture, in a very generic manner, thereby complementing other research conducted in the trust research community.

3.1.4 Stakeholders

Within South Africa, there is significant work being carried out in this area by the University of Johannesburg and SAP research Pretoria, South Africa. Within the BIC workshops, a number of future collaborators have been identified already from India and the EU, but more are welcomed to mobilise in a bid for funding of a joint project within Horizon 2020 or elsewhere of relevance to investigate the manner in which each partner country can benefit from this research.

3.1.5 Benefits and success metrics, and need for INCO

A project of this nature will bring significantly more understanding to the role of culture on the different layers of consumer trust. A success metric for this work would include a working prototype, evaluated in a real life context in one or more of the countries. There would need to be INCO funding available to carry out investigations on cultural behaviours and norms, and consumer trust in different contexts. It would also enable the setting up and evaluation of the prototype in a real community such as India and South Africa.

3.1.6 Approach

Parallel approaches are needed – both bilateral (country to country) and multilateral (multiple countries) – because different countries have different perspectives on this problem, which needs to be understood individually and then brought together into an interoperable framework.

3.1.7 Timeline

An initial estimate of a timeline for this work would be:

- Completion of basic model developed in South Africa - by end of 2014;
- Evaluation of prototype - start of 2014 – 2016;
- Continuous adaptation of trust model based on prototype evaluation - 2014 – 2016;
- Investigation of culture on consumer trust – on-going till 2016;
- This timeline fits quite well with the onset of Horizon 2020.

3.2 India

3.2.1 Introduction – the need for INCO

The potential uptake of mobile computing in tandem with the cloud paradigm, offers possibilities that can spur a huge market in the developing Indian economy. However, the privacy and security concerns arising because of the storage and handling of data at indeterminable locations in the Cloud appears an inhibitor for both corporations and individuals [20].

In a globalised world, there is a case to undertake a research in the construct of "Online trust" models as applicable to the adoption of these emerging mobile applications in Indian context. By international cooperation between different nations on this research, the common denominators and differences amongst the researched cultures would provide deep insights while designing security and privacy applications.

3.2.2 The research challenges

The psychology of trust has deeper connotations and is influenced by the cultural backdrop of the people being investigated**.** For ensuring adequate uptake for the mobile cloud applications**,** we need to package them with due sensitivity to the trust dynamics of the target consumers**.** Different segments of large Indian population seem to have different perception about the security and privacy issues. The urban–rural divide is a reality of Indian ecosystems. The necessity to bridge the digital divide and achieve inclusive growth for all segments of Indian society has resulted in following three initiatives by Indian government:

a The Central Government, the State Government and public authorities are mandated to deliver all public services by electronic mode within five years of the commencement of an empowering act (The Indian Government THE ELECTRONIC DELIVERY OF SERVICES BILL 16th November 2011).

b In an endeavor to increase citizens' trust in the online environment and to enable the various government agencies to choose appropriate authentication mechanisms, the Department of Information Technology, Government of India has conceptualized the National e-Authentication Framework (NeAF) (Draft National e-Authentication Framework (NeAF) by Indian Government, 01 Sep 2011).

c The m-Governance framework of Government of India aims to utilize the massive reach of mobile phones and harness the potential of mobile applications to enable easy and round-the-clock access to public services, especially in the rural areas. The framework aims to create unique infrastructure as well as application development ecosystem for m-Governance in the country (Framework for Mobile Governance by Indian Government, Jan 2012)**.**

The challenge is to design a trust model factoring the defining characteristics of various identifiable segments in Indian society. We would use the layered approach to trust formation as described in Table 1 to research various segments in Indian context.

3.2.3 Objectives

This research on trust proposes to focus on higher layers (4 to 6) dealing with social aspects in Table 1. The focus is on identifying how various segments of consumers within Indian context understand and use trust information such as recommendations and assurances, and to build into trust evaluation the social position of consumers, retailers and suppliers. This research is focused on how culturally specific behaviour influences the trust model. The lower layers of Table 1 dealing with technology issues would be minimized. The long-term expected outcome of this work would be a more generic framework that supports the ability to adapt trust models to culture, in a very generic manner, thereby complementing other research conducted in the trust research community.

3.2.4 Stakeholders within the evolving Indian Government Policy

The Indian government and industry would be interested to understand the dynamics of online trust models as applicable to various identifiable segments to implement e-Governance and e-Commerce projects. A proposal by the Department of Management Studies at IIT Delhi to Indian government for modelling the online trust construct is under active consideration. Under the aegis of BIC project collaboration with willing international partners would provide deep insights about this phenomenon factoring the effect of cross national cultural diversity.

3.2.5 Benefits, success metrics, and need for INCO

A project of this nature will bring significantly more understanding to the role of culture on the different layers of consumer trust as elaborated in Table 1. A success metric for this work would include a working prototype, evaluated in a real life context in rural and urban segments of India. We could also segment the consumers based on other demographic details like monthly income, age group, sex etc.

The collaboration with willing nations of BIC would facilitate sharing of the commonality and differences across the varied cultural diversity of participating nations. INCO funding would be necessary to investigate the trust dynamics of the target segments within India and to collaborate with partner nations. Indian government would also be approached for supplementary funding after the collaborative research framework is agreed upon.

3.2.6 Approach

While initial focus would be to capture the diversity inherent in various segments in Indian society as viewed through the layered framework of Table 1, a combination of bilateral and multilateral approach may emerge as we traverse the research path to facilitate insights into cultural diversity across the participating nations.

3.2.7 Timelines

The research may be undertaken in phases. The research plan and deliverables at end of each phase would need preliminary study by the collaborating agencies. A timeline of 3 years for useful deliverables is considered realistic. This fits within the scope of the Horizon 2020 programme.

3.3 European perspective

The European Union has launched several projects or initiatives to cover this area. We develop here a summary of them. Part of these works can become building blocks of an integrated and international framework that could be built.

Several programs and initiatives have been launched in Europe within the frame of the European effort to generate a trustworthy environment for commerce, communication and generally speaking interactions on internet. It has also been the case for regional studies. As an example one can point the work done within the BATE project that covers the Nordic countries [21].

The authors derive a set of questions that we should consider when designing for all:

- How can we investigate into the effects of culture in understanding computer security?
- How should we define "culture" in this context? What is it, exactly, made of?
- How should we define security-related concepts, such as privacy, or trust, for multi-cultural environments?
- How can we make cultural comparisons across users from various countries? What is relevant for the study of cultural effects?
- How "weighty" are cultural considerations for the overall design of security-prone systems?
- What will the future culture of secure Internet and secure and private mobility be like?

From the international cooperation programs to the European Union, we can consider the extensive analysis of the cultural differences in term of the value perception of an offer (product or service) by different cultures. We can confirm from this study that while Trust is an universal value, it is not perceived in the same way in different cultures. Moreover, factors that influence this perception are not similar. From the disciplinary approaches we face the same situation: development are scattered. Table 2 illustrates the benefits gained from the specific programs that the European Commission funded upon which the BIC initiatives is building an integrated paradigm.

Acronym	Full Title	Objectives
Start 2011-01-01 **End** 2013-12-31	*Building International Cooperation for Trustworthy ICT*	The European Commission's CNECT H4 project BIC – Building International Cooperation in Trustworthy ICT works with the international community to solicit feedback, comments and ideas for further progress towards future international cooperation (INCO) on trust and security areas that inherently need to be addressed at the global level. The goal of the BIC project is to bring together the global research community with the aim of determining mutually beneficial and urgent topics for international collaboration on the research and development of Trustworthy ICT between the EU and emerging countries, specifically Brazil, South Africa and India.

Acronym	Full Title	Objectives
Start 2010-09-01 **End** 2013-02-28	*European Framework for Future Internet Compliance, Trust, Security and Privacy through effective clustering*	Provides a coordination service for R&D for Trust, Security, Privacy and Compliance (TSPC) in the Information Society and the Future Internet (FI) coordination of project contribution to the development of Future Internet; (1) coordination of project contribution to the development of Future Internet; (2) coordination of project activities through Project Clustering; (3) coordination and integration of the results and findings from (1) and (2), feeding them into an ongoing roadmap that contributes to the agenda for future European research, development, and practice. To date, there has been no overall co-ordination of Future Internet Assembly (FIA) work with early T&S project clustering.
ATTPS **Start** 2012-07-01 **End** 2015-06-30	Achieving The Trust Paradigm Shift	ATTPS addresses four pillars, which include business, legal, social and technical challenges. The objectives of ATTPS are: (1) Enforcement of the trust paradigm shift (2) Create awareness at industry, institutes, governments across member states (3) Contribute to interoperability and standardisation at European level on trustworthy ICT.
ETRUST **Start** 2007-04-01 **End** 2009-03-31	E-democracy technologies and the problem of public trust	The aim of e-democracy tools is to give people more choice about how they can participate and to give them the feeling that their input makes a real difference, eventually resulting in more trust in government. This project aims at answering the question "Does e-democracy increase trust in government, and under what conditions?"
REPUTATION **Start** 2003-11-01 **End** 2005-10-31	Using trust and reputation to Improve security in virtual societies	(1) Improve the reliability and security in e-Commerce environments. (2) Provide a common metrics to compare computational trust and reputation models. (3) gives a common experimental environment where to compare all computational trust and reputation models under the same conditions and allows to clearly determine the strengths and weaknesses of each model. (4) Increase people's confidence in multi-agent systems technology. Improving the reliability and security of e-Commerce environments by means of better trust and reputation models.
ITRUST		(1) Facilitate the cross-disciplinary investigation of fundamental issues underpinning computational trust models by bringing together expertise from

Acronym	Full Title	Objectives
Start 2002-08-01 **End** 2005-07-31	Working Group on Trust Management in Dynamic Open Systems	technology oriented sciences, law, philosophy and social sciences; (2) Facilitate the emergence of a widely acceptable trust management process for dynamic open systems; (3) Facilitate the development of new paradigms in the area of dynamic open systems which effectively utilise computational trust models; (4) Facilitate the harmonisation of regulatory and legislative frameworks and facilitate their evolution so as to support the fast take-up of the emerging technologies in the area of dynamic open systems; (5) Incorporate trust management elements in existing standards and prepare the ground for the standardisation of emerging technologies by submitting recommendations to the appropriate standardisation bodies.
GRIDTRUST **Start** 2006-06-01 **End** 2009-05-31	Trust and security for next generation grids	The overall objective of the GridTrust project is to develop the technology to manage trust and security for the Next Generation Grids (NGG). The project proposes to set a vertical approach tackling issues of trust, security and privacy (TSP) from the requirement level down to the application, middleware and foundation levels. The resulting tools will be of a generic nature and will be validated on innovative applications from different application sectors. The tools will not be specific to the applications considered in the GridTrust project.
SOCIALREP **From** 2006-03-01 **End** 2007-02-28	Toward the next generation of computational trust and reputation models	1. improving the state-of-the-art of current computational trust and reputation models. 2. Provide a common metrics to compare computational trust and reputation models. 3. Increase people's confidence in multi-agent systems technology.
TRUSIS **Start** 2010-06-07 **End** 2011-06-06	Trust in Social Internetworking Systems	1. To define a simple mathematical model of social internetworking and analyze factors influencing the computation of trust and reputation with a special emphasis on some typical Web 2.0 features. 2. To extend the basic model with context-awareness functionalities in order to specify trust/reputation of users in concrete domains. 3. To build an ontology capable of representing trust and reputation data in multiple social networks. 4. To carry out long-term iterative testing and validation activities on real users.

Acronym	Full Title	Objectives
TRUSTREP **Start** 2006-10-18 **End** 2008-10-17	Creation and use of trust in virtual communities through reputation Management	This project examines how reputation management schemes can be used to monitor and manage systems in a decentralized fashion. Reputation management is not a replacement of traditional security solutions and is instead a complementary strategy that works through establishing trust between members of a virtual community allowing them to collaborate so that they can provide each other with robust services and services that would otherwise not have been possible.
ACTOR **Start** 2010-06-01 **End** 2012-05-31	ACcelerate Trust in digital life Organisation and Relations	Establishing a multidisciplinary partnership Broad support to the TDL research roadmaps for longer-term research in the field of trustworthy ICT Bundling and coordinating the effort of the Partnership members to develop a promising and ambitious SRA and Work plan for TDL. Identification of a balanced portfolio with concrete project ideas for public funded research and innovation projects.
DEL **Start** 2011 **End** continuous	Digital Enlightenment Forum	http://www.digitalenlightenment.org/ The DIGITAL ENLIGHTENMENT FORUM stimulates and organises debate among representatives of science and technology, law and policy. It provides guidance on the rapid changes in digital technologies and their perceived impact on society and its governance.

Table 2. Summary of the European projects/initiatives dealing with trust management

4 Conclusions

This paper has highlighted the necessity of considering the cultural context while evolving the construct of online Trust. As online transactions in our global village go beyond the various cultural contexts, the necessity to factor the effect of cultural diversity while proposing Online Trust models appears relevant. The ongoing and proposed research on this important theme at two of BIC partner countries viz. South Africa and India have been described. The paper makes a case for evolving an Online Trust model that factors the cultural diversity as a dimension for research model.

There is definitely a revised if not new understanding of the real challenge about trust and security in our open and global society. The BIC project, through its working groups, managed to turn this general issue into tangible statements that should be considered for further development, in a way that policy makers can build upon the real-field description of the societal challenges, industrials to better design services and products, users to get a culturally-adapted awareness about trust and security. Several steps need to be considered in

our path for global trustworthiness. We believe that an urgent agenda need to be set considering the following:

- Building a framework for culture analysis within the frame of trust and security;
- Characterization and understanding of the cultural differences using this framework;
- Co-creation of culturally-adapted indicators for trust and security for a better efficiency of awareness actions;
- Construction of an International Reputation Index for trust and security that allows transparency;
- Building a methodology to transform user requirements into real industrial requirements;
- Feeding policy makers and standardisation bodies with these constraints coming from multi-disciplinary, multi-cultural and end-users needs.

This agenda needs to be adopted internationally within an EU program that, by now, is the only potentially realistic host and run by a multidisciplinary group of experts in an "open innovation" methodology way rather than in separate groups.

Acknowledgments. The BIC project is supported within the portfolio of the European Commission's DG-CNECT Unit H.4, Trust and Security, and has received funding by European Commission's Seventh Framework ICT Programme under grant number 25258655 for the period January 2011 to December 2013. The authors have come together to develop this work as part of BIC Working Group 1, Human Oriented approaches to Trust and Security.

5 References

1 Clarke, J., et. al.: BIC Working Groups Workshop report, June 2012, Online: http://www.bic-trust.eu/events/bic-workshop-on-the-cross-domain-coordination-of-international-cooperation-day-1-and-technical-themes-in-trustworthy-ict-and-inco-day-2/

2 Mezzetti, N. (2003). Towards a Model for Trust Relationships in Virtual Enterprises, TrustBus´03 Prague, Czech Republic, September 1-5, 2003

3 Gambetta, D. (1990). Can We Trust Trust? In Gambetta, D (ed.), Trust: Making and Breaking Cooperative Relations , Basil Blackwell. Oxford, pp.213-237.

4 Isherwood D., Coetzee M. and Eloff, J.H.P.: Towards Trust and Reputation for E-Commerce in Collectivist Rural Africa, International Symposium on Human Aspects of Information Security & Assurance (HAISA 2012), 6-8 June 2012 in Crete, Greece.

5 Coetzee, M.: Trust models addressing cultural differences between communities, BIC Workshop November 2012: Online: Full presentation of this paper can be found at http://www.bic-trust.eu/files/2012/10/BIC-trust-and-culture-SA.pdf

6 Clarke, J., et. al.: BIC IAG Annual Forum and workshop report, November 2012: Online: http://www.bic-trust.eu/files/2013/01/BIC-Annual-forum-2012-report-Final.pdf

7 Hofstede, G. Cultures and Organizations: Software of the Mind. New York: Mcgraw-Hill, 1991

8 Maña A., Koshutanski, H., Pérez E.J.: A trust negotiation based security framework for service provisioning in load-balancing clusters, Computers & Security, Volume 31, Issue 1, February 2012, Pages 4-25

9 Boukerche, A., Ren, Y.: A trust-based security system for ubiquitous and pervasive computing environments, Computer Communications, Volume 31, Issue 18, 18 December 2008, Pages 4343-4351

10 Martinelli, F., Petrocchi, M.: A Uniform Framework for Security and Trust Modeling and Analysis with Crypto-CCS, Electronic Notes in Theoretical Computer Science, Volume 186, 14 July 2007, Pages 85-99

11 Bahtiyar, S., Ufuk, M., Çağlayan: Extracting trust information from security system of a service, Journal of Network and Computer Applications, Volume 35, Issue 1, January 2012, Pages 480-490

12 Nagarajan, A., Varadharajan, V.: Dynamic trust enhanced security model for trusted platform based services, Future Generation Computer Systems, Volume 27, Issue 5, May 2011, Pages 564-573

13 Lenzini, G., Bargh, M.S., Bob Hulsebosch, B.: Trust-enhanced Security in Location-based Adaptive Authentication, Electronic Notes in Theoretical Computer Science, Volume 197, Issue 2, 22 February 2008, Pages 105-119

14 An, D., Kim, S.: Effects of National Culture on the Development of Consumer Trust in Online Shopping, Seoul Journal of Business, Volume 14, Number 1, June 2008.

15 Chong, B.: Why culture matters for the formation of consumer trust? A conceptual study of barriers for realizing real global exchange in Hong Kong Asia Pacific Management Review 8(2), 217-240, 2003.

16 Coetzee M. (2006) WSACT - a web services access control model incorporating trust, PhD Thesis, University of Pretoria, Department of Computer Science

17 Mekhilef, M., Page, Y., Bel, M., Moessinger, M.: Designing for Unrevealed Values, International Design Conference – Design 2012, Dubrovnick, Croatia, May 21-24, 2012.

18 Grandison T.W.A. (2003) Trust Management for Internet Applications, PhD Thesis, Imperial College of Science, Technology and Medicine, University of London, Department of Computing.

19 Boudaoud, K.: International Cooperation for Trust Management, BIC Workshop November 2012: Online - A full presentation can be found at http://www.bic-trust.eu/files/2012/10/BOUDAOUD_BIC_WS27Nov2012.pdf

20 Chaturvedi, M.M.: Online Trust in the India Context, BIC Workshop November 2012: Online: full presentation at http://www.bic-trust.eu/files/2012/10/Chaturvedi_BIC_27Nov20121.pdf

21 Kristiina Karvonen , Lucas Cardholm , Stefan Karlsson. Cultures of Trust: A Cross-Cultural Study on the Formation of Trust in an Electronic Environment (2000). In Proceedings of the 3rd Nordic Workshop on Security (NordSec 2000) (Reykjavik)

22 Abdul-Raiman, A. & Hailes, S. (2000) Supporting Trust in Virtual Communities, Proceeding of HICCS 2000.

23 Butler J.K. (1991) Toward Understanding and Measuring Conditions of Trust: Evolution of a Conditions of Trust Inventory , Journal of Management, 17(3), 643-663.

24 Cobern, W.W. (1998). Science and a social constructivist view of science education. In W.W. Cobern (Ed.), Socio-Cultural Perspectives on Science Education: An International Dialogue. Dordrecht, The Netherlands: Kluwer Academic Publishers.

25 Dafoulas, G. & Macaulay, L. (2001). Investigating Cultural Differences in Software Teams. Electronic Journal on Information Systems in Developing Countries , 7(4), 1-14.

26 Grandison, T., & Sloman, M. (2000). A Survey of Trust in Internet Applications. IEEE Communications Surveys . Fourth Quarter. 2000

27 Hofstede, G. (1980). Culture's Consequences: International Differences in Work related Values. Newbury Park, CA: Sage.

28 Hofstede, G. (1983). Dimensions Of National Cultures In Fifity Countries And Three Regions. In J.B.

29 Hofstede, G. (1998). A Case Study for Comparing Applies and Oranges: International Differences in Values. In M. Sasaki (Ed.). Values and Attitudes Across Nations and Time. Leiden, Netherlands: Brill.

Further reading materials

30 Khare, R., & Rifkin, A. ((2000). Trust Management of the World Wide Web. Peer-reviewed journal on the Internet. Vol 3, no 6. Accessed online at http://www.firstmonday.dk/issues/khare

31 Klein, H.A., Pongonis, A., & Klein, G. (2000). Cultural Barriers to Multinational C2 Decision Making. Proceedings of 2000 Command and Control Research and Technology Symposium, Monterrey, CA.

32 Quirchmayr, G. & Slay, J. (2002). The Role Of Culture In the Development of Global E-Commerce Systems. IFIP WCC 2002, Montreal, August 25th- 29th 2002.

33 Slay, J. (2001). Culture And Sensemaking In Information Warfare. 2nd Australian Information Warfare & Security Conference 2001, Perth.

34 Slay, J. (2002). Human activity systems: the impact of culture on technological learning environments. Journal of ETS and IEEE Learning Technology Forum. 5 (1), 93-99.

35 Straub, D., Loch, K., Evaristo, R., Karahanna, E. & Strite, M. (2002). Toward a Theory-Based Measurement of Culture. Journal of Global Information Management. 10 (1), 13-23.

Strategy for Coordination of the Cross Domain Activities & Multi-Lateral Approach in International Cooperation

BIC Presentation Paper

1 May 2013

Abhishek Sharma[1]

James Clarke[2]

[1] Abhishek Sharma, BIC International Advisory Group (IAG) member, Co-founder, MD & CEO, Beyond Evolution Tech Solution Pvt. Ltd., India

[2] Waterford Institute of Technology, Ireland

This project is supported within the portfolio of the European Commission's DG-CNECT Unit H.4, Trust and Security, and has received funding by European Commission's Seventh Framework ICT Programme under grant number 25258655 for the period January 2011 to December 2013.

Introduction

The purpose of the European Commission funded BIC coordination action project (http://www.bic-trust.eu/ is to foster cooperation between the EU and the international programme agencies and researchers in India, Brazil and South Africa within the focus areas of Trustworthy ICT, including trust, privacy and security, in order to:

(a) Understand the activities and planning of the target countries; and

(b) Carry out a mapping of the European Commission's planning to them, such that a common technical and policy alignment is viable.

The project is also working with the communities in a coordinating role in reflecting on a longer term strategy for international cooperation and this discussion paper summarises its findings to date. The project held a workshop entitled *Cross domain coordination of International Cooperation and technical themes in Trustworthy ICT and INCO* [1] in June 2012 and during this two day workshop, a number of international cooperation (INCO) projects participated and this discussion paper reflects on the results from this workshop and proposes a potential approach to follow based on the findings. The BIC Annual Forum and IAG meeting - November 2012, followed up the actions of June 2012 workshop.

The need for INCO

From the European perspective, cooperation with third countries and international organisations has been and will be promoted with the following objectives:

- Strengthen EU's excellence and attractiveness in research and innovation;
- Strengthen EU's economic and industrial competitiveness;
- Jointly address global societal challenges;
- Support EU's external policies.

The Strategic INCO approach

In order to examine the challenge of moving from a bi-lateral to a multi-lateral approach, the project had held a workshop in June 2012 [1] bringing together a majority of the projects engaged in international cooperation to enable the following outcomes:

1. sharing their experiences and insights in order to brainstorm a strategy to move forward on international cooperation in future calls for collaborative research;
2. developing the current bi-lateral (and potentially overlapping) country to country cooperation into a comprehensive and coordinated global cooperation.

In addition to BIC, a wealth of experience was represented from the following international cooperation projects: IST Africa, EuroAfrica-P8, FEED, AUS-ACCESS4EU, PACE-Net, EU – India Spirit, Synchroniser, Euro-IndiaGrid2, OpenChina-ICT, FIRST, FORESTA, PAERIP, SEACOOP, EuroAfrica-P8 and AMERICAS. A full report of the BIC workshop can be found at [2]. The BIC Annual Forum and IAG meeting - November 2012 [6] followed up the papers and proposals of June 2012 workshop, ratified some of those and also discussed subsequent actions and additional papers.

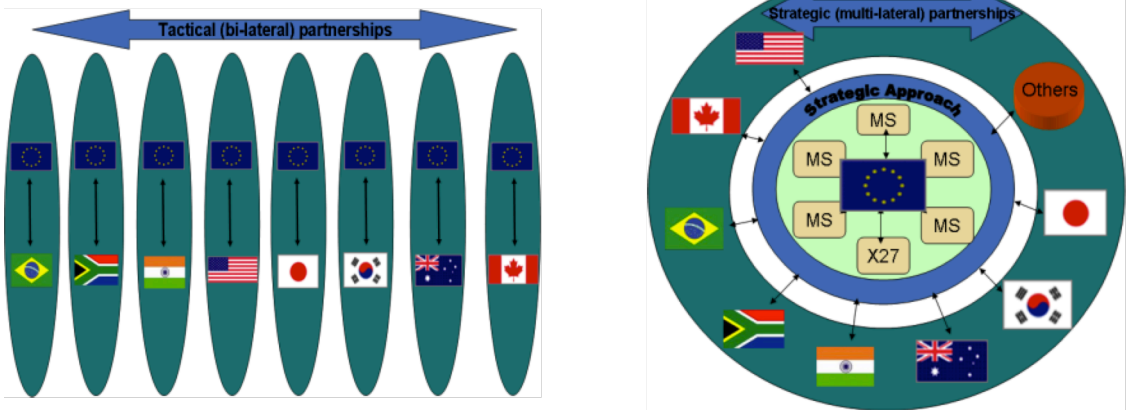

Figure 1 – Tactical (bi-lateral) approach *versus* Strategic (multi-lateral) approach

These projects gave their insights on their experiences and suggestions for improvement and the main point was agreement that it is a very good idea to move towards a more multi-lateral strategic position. However, in the discussions, it wasn't very clear how this strategy shift could occur within the current mechanisms that focus bi-laterally on seven (7) distinct regions.

In order to address this further, the BIC project are examining how the combination of their International Advisory Group and supporting working groups could assist in a move towards a more multi-lateral strategic approach.

The majority of the current INCO mechanisms support regional bi-lateral activities as shown in Figure 1. While this regional approach may work for higher level themes, the main difficulty arises when a particular research topic, for example, cyber security, needs to be addressed globally and multi-laterally amongst many regions and the bi-lateral approach is not suited for this type of longer term strategic activity.

Therefore, the BIC project is examining the feasibility of a more strategic approach based on multi-lateral partnerships as shown in figure 1.

BIC International Advisory Group (IAG)

The BIC project has established an international advisory group (IAG) with the following terms of reference.

The IAG will be the forum bringing together the countries representatives in a more strategic way;

- To facilitate collaborations between national ICT Trust and Security constituencies and related ICT trust and security related constituencies from other countries;
- To review the situation on International collaboration strategy in ICT trust and security on a regular basis providing advice on the priorities for international cooperation between the respective research communities, providing directions to the project and recommendations for improvement;
- Assist in the building of the working groups to enable BIC to structure relationships and linkages and facilitate contacts for theme based workshops or other networking events.

The IAG has representation from all the participant countries from both the researcher communities and programme management (funding agencies). The IAG is there to suggest and formulate the policies, processes and mechanisms to achieve international cooperation in the area of the ICT Trust and Security community. Three independent working groups, WG1, WG2 & WG3 with specific objectives as defined in the BIC WG Terms of Reference [3], have been formed comprising specialists from different countries and different specializations. The areas and scope of the three BIC working groups are the following:

1. WG1. Human oriented /citizen trust, privacy and security, which will focus on topics related to a multi-disciplinary approach for international cooperation amongst all stakeholders;

2. WG2. Network Information security / Cybersecurity, which will focus on topics related to the need for international cooperation for enabling the protection of networks and systems;

3. WG3. Programme /funding focus/ identify community, which will focus on the requirements, processes, mechanisms and barriers to enable collaboration opportunities.

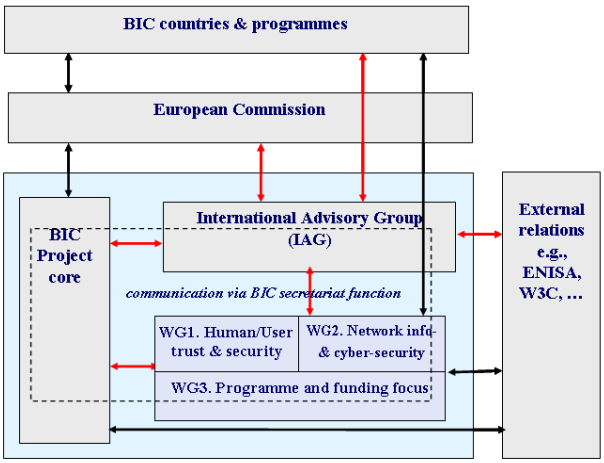

Figure 2 – Overall structure of BIC

Indeed, as shown in Figure 2, these WGs form the backbone of the Project; however, they alone would not be enough to take the entire project forward to its logical conclusion. They would, therefore, need to be supported by additional Groups and Sub-Groups in a structured manner at the management and functional level with defined focus area, roles and responsibilities.

A proposed strategy for Coordination and multi-lateral approach in International cooperation

Since the nature of an international project requires interactions amongst all participant countries to share the information, resources, etc., the approach for the formal interactions, flow of information and smoothness of actions, it becomes natural that the groups and sub groups working for the project work closely with each other. Accordingly at international management level, it requires a change in approach from the existing bi-lateral approach i.e. EU-India, EU- Brazil, EU- SA, U.S, Japan, … to multi-lateral approach where each participating country develops a formal system for direct multi-lateral communication and interacts with each other besides interacting centrally as well. Of course, the existence and role of a central body is essential for ensuring that the focus of the projects are not digressed and there is proper coordination amongst all adhering to the core principles and objectives of the project.

The terms of reference of BIC working Group specify that WG3 will focus on a multi-disciplinary approach towards international cooperation amongst all

stakeholders. Having recognized the importance and relevance of International cooperation on addressing the critical issue of "Trust & Information Security", it is essential to appreciate that such a project needs special treatment to identify and define the objectives and manage its execution to achieve the desired results. This paper aims at highlighting various key elements that are essential to be considered from the start to define the objectives and manage the project, duly taking into consideration the challenges associated with a project of Global dimension and Cross-Domain activities. International Cooperation is an essential aspect that the IAG needs to address consciously. In this context it would be appropriate having a look at the resolution adopted at the UN General Assembly (Resolution adopted by the General Assembly: 57/239. Creation of a global culture of cyber security) placed at Annexure 'A' to this paper.

Key Elements

The strategy behind the success of a project of such dimensions and complexities, needing international cooperation critically hinges upon certain key elements, as described below that should necessarily be taken in to account through the life of the project.

1. Inclusive & All Pervasive Approach should be the essential theme for building up the right team and the scope of the project. Further since the project needs the international participation with involvement of individuals and bodies from different countries and organisations of diverse background, voluntary participation should be considered as a preferable criteria if not essential for participating organisation. It would be more effective and hence the same must be encouraged. Wider exposure to the project, through special efforts & mechanism, would be required to attract volunteers.
2. Scope of Work (SOW) Defining SOW with clarity is the next essential part for smooth progress of work and avoiding any ambiguity at later date.
3. Management Structure Commensurate with the SOW and deliverables with unambiguously defined hierarchy of Role and Responsibilities is another key element to help ensure Effective Management.
4. Focus: Projects of such diverse dimensions are prone to getting digressed from the original path / objective. Caution against such pitfalls and constant reviews are essential to stay focussed.
5. Vision, Mission & Targets: A management approach with well defined Vision, Mission & Targets is essential. While the project objectives should have a vision beyond an estimated period of time say five years, there has to be mission oriented approach for achievements in medium length of time, say 3-5 years. At the same time the progress of the project must also define short term action plans and targets that must be achieved within the time blocks of 3 months, 6 months and one year.
6. Project Management: The project would also need to follow established principles of Project Management with special emphasis on following aspects:
   a. Planning of resources, costs and time (time lines & mile stones) and a clear roll out plan.
   b. A suitable monitoring mechanism associated with regular Review of Processes, People and Benchmarks.
   c. Provision for Course Corrections of the project activities may also be required at times after the reviews.
7. Long Term Strategy: The threat to Trust & Security being an issue with constant possibilities of new types of threats coming up with time, the Project also needs to have long term strategy and provision for *Inclusion of Future Projects*.
   a. Metrics: It would also be essential to measure the progress in definite terms and suitable metrics are essential to assess the state of the project at any point of time.
   b. The project Roadmap: The nature of BIC project would not allow the classical approach to define the roadmap right in the beginning. A flexible approach with regular reviews at some defined milestones would be more appropriate to maintain a meaningful direction.
   c. Conclusive & Smooth Closure: A good project needs to have a time bound closure in tune with the defined deliverables. *Metrics for Goal setting & Achievement* for assessing proper *implementation* and *Provisions for Carry Forward* to enable the project to smoothly roll on to the next level are essential elements for the concluding stage.

Main Stakeholders

The Project has three main stakeholders:

1. Researchers: These are the specialists of the field who are expected to explore various options, carry out necessary research and design the proposed solutions.
2. Govt. Bodies related to the area of research are required to examine and evaluate the proposals, allocate the funds, formulate the process of regulating the required funds and disburse the same in accordance with the defined process.
3. Industry: Role of the industry shall be to develop the products and solutions based on the designs provided by the researchers and take the developed products/ solutions to the market, to the people.

Way Forward

1. A lot of work and research studies in the area of "Trust & Security" are already going on across

different parts of the world. Many individuals and organizations- research institute/ corporate are busy doing work independently. Unfortunately most of the work is happening in isolation, in a disjointed manner with no systematic coordination and cooperation amongst each other. They are only accessing each other through open access methods of published papers, journals etc. Therefore, there is strong need to create a platform and associated mechanism which can bring all such work together in such a fashion that there is systematic and regular information exchange and mutual support. This cooperation platform would facilitates the work to become well-coordinated and consolidated such that combined and consolidated work is very comprehensive and becomes a formidable defence against the regular threats emerging across the globe and also ensures that duplication of work is minimized.

Structured Multi-Lateral Approach:

a. At present, the International Advisory Group (IAG) formed under BIC, to formulate the policies and process to achieve international cooperation in the area of the work. Three independent working groups, WG1, WG2 & WG3 with specific objectives as defined in the BIC IAG TOR, have been formed picking up specialists from different countries and different specializations. Indeed, these WGs form the backbone of the Project; they alone would not be enough to take the entire project forward to its logical conclusion. They would, therefore, need to be supported by additional Groups and sub groups in a structured manner, at the management and functional level with defined focus area, role and responsibilities.

b. Since the nature of the project requires interactions amongst all participant countries to share the information, resources etc, the approach for the formal interactions, flow of information and smoothness of actions, it becomes natural that the groups and sub groups working for the project work closely with each other. Accordingly at international management level, it requires a change in approach from the existing bi-lateral approach i.e. Eu-India, EU- Brazil, EU- SA etc to multi-lateral approach where each participating country develops a formal system for direct multi-lateral communication and interacts with each other besides interacting centrally as well. Of course the existence and role of a central body is essential for ensuring that the focus of the projects are not digressed and there is proper coordination amongst all adhering to the core principles and objectives of the project.

2. Working Group Structure: The proposed Multi-Lateral structure should have three main layers as shown in figure 3 :

a. Core Working Group (CWG) ;

b. Extended Working Groups(EWGs) - specific for each participating country and

c. Special Function Groups – To be under EWGs as specialists at functional level.

3. The suggested role and function of this structure is as follows:

a. The CWG is at present constituted with three working groups WG1, WG2 and WG3 with representation from all participant countries and people chosen from different specialization. The composition of the CWG, with the three WGs at present, may be reviewed from time to time to assess if these WGs are adequate to cover all aspects of the projects or if any new aspects have emerged or any gaps are being observed for which additional WGs would be needed.

b. ***The role of the CWG*** is to address Strategy formulation, define high level objectives of the project and create a high level management structure and work flow processes to guide the project in the desired direction duly providing required support and assuming the overall leadership cum ownership position.

c. The CWG should be supported by Extended Working Groups (EWGs) which needs to be formed at each member country. The CWG should define the eligibility criteria for EWG members. The country representatives within the CWG should then take up the responsibility of forming the EWG of the respective countries selecting out of the eligible individuals, Research Institutes and the companies, mainly SMEs. *Voluntary participation* should be one of the main criteria to join the EWG.

d. ***The EWG members*** would be the key functional entities whose primary role would be to steer the project within the country and organize coordination with other member countries. In doing so, EWG would undertake the ownership of the following responsibilities:

i Identify local functionaries: Researchers, Govt., Industry

ii Form a country specific consortium of functional entities with defined objectives, functions and deliverables. This consortium of functional entities may be labelled as Special Function Group (SFG)

iii Explain & Promote CWG Objectives & specific requirements to SFG by various means e.g. organizing regular workshops, seminars, events, interacting personally with other researchers and Govt. bodies thereby help forming a wider community.

iv Prepare the project plan, in accordance with Project Objective and with emphasis on Project Cost, Resource Requirements and time frame/ time lines with the major involvement and support of the SFG.

v Function as operational link between the CWG and SFG.

vi Monitor & Manage In-Country progress through regular meetings/ Conferences.

vii Gather Inputs & Process them: Analyze, Filter & Forward.

viii Become a functional element for Multi-Lateral Cooperation, in that:

a. Interact closely with CWG and EWGs of other countries

b. Establish effective cooperation with other EWGs to share the work and resources mutually, in sync with the CWG.

c. Encourage and Support SFGs for multi-lateral cooperation.

ix Help prepare & consolidate Budgetary Estimates. If required, they will also help initiating the Proposals duly coordinating with CWG.

x Act as Committed Process Owners.

d. CWG then undertakes the role of

i. Identifying, coordinating and consolidating the Research and Technology Development (RTD) work of EWGs

ii. Monitoring the progress of EWGs and ensuring sustained focus.

The proposed management structure is given below in Figure 3.

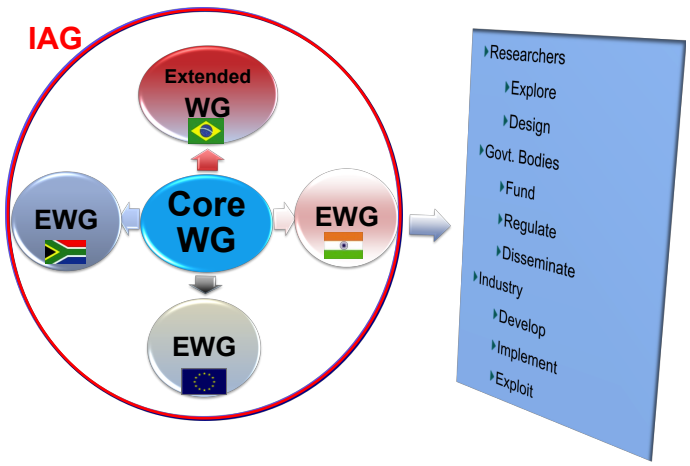

Figure 3 – BIC Multi-lateral IAG/WGs structure

4. Priority Areas for Research & Development (PARD):

a. Having formed the EWGs, CWG creates a high level list of Priority Areas for Research & Development (PARD) work and provides this list to EWGs for their respective assessment and opting for topics for the projects.

b. EWG interacts with SFGs, analyses the list of research area provided and reverts to CWG with their Proposed List of the Projects of Interest (PLPI).

c. CWG analyzes the PLPI, selects the priority projects and consolidates all such project lists to prepare the List of Selected Projects.

5. Project Assignment & Planning :

a. On finalization of the Selected Project, assignment of the same to EWGs is done by CWG where the commitment of EWGs is obtained. Having assigned the projects, the next steps are:

i Prepare High Level Action Plan (HLAP)

ii Develop Macro Project Plan (MPP): Services of experienced Project Management professionals are obtained who are inducted at the CWG and EWG level at this stage. The MPP is prepared based on the micro level project plan obtained from EWGs.

iii Consolidate and finalize the MPP for each EWG.

iv Analyze & Approve Project Resources as duly analyzed and proposed by EWGs.

v Budgetary Estimates are consolidated. Process for Allocation & Release of Funds and Disbursement Mechanism are also finalized along with the criteria and plan for disbursement. This may be done in sync with EC standards and processes.

b. Monitoring & Review Process: Define the process specifying Schedule, Milestones & Benchmarks

c. Prepare Long Term Strategy: This should incorporate the following:

i Provision for New Challenges & Threats,

ii Policy Review & Course Correction,

iii New Projects and

iv Backup provisions for Management Team.

Conclusions

Strategy plays the most crucial role for the success of any project. When the size and complexities of the project assumes international dimensions, it is incumbent upon the main body to work out a proper strategy and define structures and processes. However, while on one hand it is essential to observe strict discipline to execute the projects as per plan, despite taking all care and precautions, possibility of unexpected future developments and new projects/ prospects cannot be ruled out. It would therefore be wise to incorporate provisions for flexibility and future changes in case of such wide and complex projects.

The building of international cooperation is difficult when using a bi-lateral approach as it takes significant time for all of the parties to come together to try to align their activities and priorities. Therefore, it is even more difficult for a multi-lateral approach when building a longer term strategy as proposed within this paper. The BIC project has proposed a strategy and will follow up in the near future with interested countries as exemplars.

Acknowledgments

The BIC project [4] is funded by the European Commission's DG-CONNECT Unit H.4: Trust and Security [5].

References

[1] BIC Workshop June 2012. Site - http://www.bic-trust.eu/events/bic-workshop-on-the-cross-domain-coordination-of-international-cooperation-day-1-and-technical-themes-in-trustworthy-ict-and-inco-day-2/

[2] Clarke, J., et. al., BIC Workshop on *Cross domain coordination of International Cooperation and technical themes in Trustworthy ICT and INCO.* Online report - http://www.bic-trust.eu/files/2012/04/BIC_D4.5_Report-of-Workshop.pdf

[3] BIC Deliverable D2.3 - Interim report of the Working groups activities (restricted).

[4] BIC Web site http://www.bic-trust.eu/

[5] DG CNECT Unit H.4 web site http://cordis.europa.eu/fp7/ict/security/

[6] BIC Annual Forum and IAG meeting - November 2012. Site - http://www.bic-trust.eu/files/2013/01/BIC-Annual-forum-2012-report-Final.pdf

About the Authors

Abhishek Sharma is founder, MD & CEO of Beyond Evolution Tech Solutions Pvt Ltd(beTS). Abhishek has built beTS from scratch developing many mobile application and Solutions offering niche Utility VAS as ASP to large mobile users through many large Telcos like Vodafone, BSNL, MTNL, Idea, Airtel etc in India and abroad. Prior to founding beTS, Abhishek has worked for Indian Air Force for about 22 yrs and then for large corporate in India and abroad such as Programme Manager, GSM Backhaul/ Microwave Services, Tata Telecom, India; Country Head – Telecom SBU at TCS/ Tata Infotech, India; MD at Globacom Cellular, Nigeria etc where he managed large ICT Projects & Operations such as Radar, Telecom NW, BSS, OSS etc. Abhishek is also a renowned consultant on Mobile VAS, Telecom Network, Radar Data Systems & Avionics. Abhishek is B.E. in Electronics & Telecommunications, M.Tech Computer Sc (IISc) & M.B.A. in Marketing.

James Clarke has been working for the Waterford Institute of Technology (WIT) in the Telecommunications Software and Systems Group (TSSG), since February 2005. Prior to joining WIT-TSSG, Mr. Clarke worked at LAKE Communications in Ireland for eight years and Grumman Corporation in the United States for eight years. Since January 2011, Mr. Clarke has been the project coordinator of a European Framework Program 7 Co-ordination action entitled 'BIC', which stands for Building International Cooperation for Trustworthy ICT: Security, Privacy and Trust in Global Networks & Services. Previous to this, Mr. Clarke coordinated the successful FP7 INCO-Trust project. More information can be found at **http://www.tssg.org/about/people/james-clarke/.**

Workshop Organizers:

James Clarke, Waterford Institute of Technology - TSSG, (co-chair)
Rebecca Wright, Rutgers University, (co-chair)
Aljosa Pasic, AtoS Spain SA
Siani Pearson, HP Labs Bristol
Keyun Ruan, University College Dublin