Cloud Information Accountability Frameworks for Data Sharing in Cloud - A Review

Shraddha B. Toney[#1], Sandeep U.Kadam[*2]

[#] *Student, First Year, ME Computer Engineering, TSSM'S, PVPIT, Bavdhan,Pune-411031,MS,India*

[*] *Assistant Professor, TSSM'S, PVPIT, Bavdhan,Pune-411031,MS,India*

***Abstract*— The difficulty of how to provide proper security and privacy protection for cloud computing is very important, and as yet not solved. In this paper we review the cloud information accountability framework for the data sharing in which procedural and technical solutions are co-designed to demonstrate accountability by the various researchers to resolving privacy and security risks within the cloud. Cloud computing is a set of services that are provided to a end user over on a leased basis over a network. Usually cloud computing services are delivered by a third party provider who owns the infrastructure. It moves the application software and databases to the most data centers, where the controller of the data and services may not be fully trustworthy which have not been well understood. This paper presents a review on new way to supplement the current consumption and delivery model for IT services based on the Internet, by providing for dynamically scalable framework and often virtualized resources as a service over the Internet. By the time there are a number of notable commercial and individual cloud computing services, including Google, Microsoft and Yahoo. Details of the services provided are abstracted from the users who no longer need to be experts of technology infrastructure. Moreover, users may not know the machines which actually process and host own data. While enjoying the convenience brought by this new technology, end users also start worrying about security of their own personal and important data. The data processed on clouds are often outsourced, leading to a number of issues related to accountability, including the handling of personally identifiable information.**

***Keywords*— Infrastructure, IT, Security, Accountability, Thirt party auditor, Network issue, cloud computing and Privacy.**.

I. INTRODUCTION

Cloud computing is an emerging paradigm in the computer industry where the computing is moved to a cloud of computers. The cloud computing core concept is, simply, that the vast computing resources that we need will reside somewhere out there in the cloud of computers and we'll connect to them and use them as and when needed. Cloud computing is the next general step in the evolution of on-demand information technology services and products.Cloud computing is a means by which highly scalable and fully technology based services can be easily consumed over the internet on an as-needed basis. To a large extent, cloud computing will be based on virtualized resources. The convenience and efficiency of this approach, however, comes with security risks and data privacy. A significant barrier to the adoption of cloud services is thus user fear of confidential data leakage and loss of privacy in the cloud. Privacy is a important and fundamental human right that encompasses the right to be left alone, many techniques are proposed under different systems and security models. In all these works, great efforts are made to design solutions that meet various requirements: high scheme efficiency, stateless verification etc. Considering the role of the verifier in the model, all the schemes presented before fall into two categories: private audit ability and public audit ability. Although schemes with private audit ability can achieve higher scheme efficiency, public audit ability allows anyone, not just the client (data provider), to challenge the cloud server for correctness of data storage while keeping no personal and private information. Then, clients are able to delegate the evaluation of the service performance to an independent third party auditor (TPA), without devotion of their applying resources. In the cloud, the clients themselves are unreliable or may not be able to afford the overhead of performing frequent integrity checks. Thus, for practical use, it seems more rational to equip the verification protocol with public audit ability, which is expected to play a more important role in achieving economies of scale for Cloud Computing. Moreover, for efficiency consideration, the out-sourced data should not be required by the verifier for the verification purpose The other important concern among previous designs is that of supporting dynamic data operation for cloud data transfer and security applications. In Cloud Computing, the remotely stored private and personal data might not only be accessed but also updated by the clients such as through block modification, deletion and insertion, etc. Since then, everyone is talking about "Cloud Computing" Of course; there also is the inevitable Wikipedia entry [17]. This paper discusses the concept of "cloud" computing, some of the issues it tries to address, related research topics, and a "cloud" implementation available today. This discusses concepts and components of "cloud" computing. This also describes an implementation based on Virtual Computing Laboratory technology. Virtual Computing Laboratory technology has been in production use, and is a suitable vehicle for dynamic implementation of almost any current "cloud" computing solution. The other Section discusses "cloud"-related research and engineering challenges..

II. CLOUD COMPUTING AND ISSUES OF INFORMATION POLICY

Cloud computing raises a range of important policy issues, which include issues of personal, secure ,private, anonymity, telecommunications capacity, reliability, and liability, among others. This section of the paper introduces and examines these issues individually. While some of the trade press and popular media accounts of cloud computing have raised potential issues of privacy and intellectual property (i.e., Delaney & Vara, 2007; Ma, 2007), the range of policy issues raised by cloud computing merits significant consideration. A productive approach to begin analysis of the information policy issues related to cloud computing is to consider user expectations. At a minimum, users will likely expect that a cloud will provide:

• **Reliability and Liability.** Users will expect the cloud to be a reliable resource for security, especially if a cloud provider takes over the task of running "mission-critical" applications and will expect clear delineation of liability if serious problems occur.

• **Security, privacy, and anonymity**. In this the cloud provider will prevent unauthorized access to both data and secure data code, and that sensitive data will remain private. Users will also expect that the cloud provider. Siani Pearson [2] focus on privacy issue. According to him is a key business risk and compliance issue, as it sits at the intersection of social norms, human rights and legal mandates. Conforming to legal privacy requirements, and meeting client privacy expectations with regard to PII, require corporations to demonstrate a context-appropriate level of control over such data at all stages of its processing. The advantages of cloud computing is its ability to scale rapidly, store data remotely , and share services in a dynamic environment – can thus become disadvantages in maintaining a level of privacy assurance sufficient to sustain confidence in potential customers. For example:

-**Outsourcing**. Outsourcing of data processing invariably raises governance and accountability questions. Which party is responsible (statutorily or contractually) for ensuring legal requirements for PII are observed, or appropriate data handling standards are set and followed [3]? Can they effectively audit third-party compliance with such laws and standards? To what extent can processing be further sub-contracted, and how are the identities, and *bona fides*, of sub-contractors to be confirmed? What rights in the data will be acquired by data processors and their sub-contractors, and are these transferable to other third parties upon bankruptcy, takeover, or merger [4]? 'On-demand' and 'pay-as-you-go' models may be based on weak trust relationships, involve third parties with lax data security practices, expose data widely, and make deletion hard to verify.

- **Offshoring.** Offshoring of data processing increases risk factors and legal complexity [5]. Issues of jurisdiction (whose courts can/will hear a case, choice of law (whose law applies?) and enforcement (can a legal remedy be effectively applied?) need to be considered [6]. A cloud computing service which combines outsourcing and off shoring may raise very complex issues [7].

- **Virtualization.** There are security risks in sharing machines, loss of control over data location, and who has access to it. Transactional data is a by-product with ownership, and it can be hard to anticipate which data to protect. Even innocuous-seeming data can turn out to be commercially sensitive [8].

- **Autonomic technology.** If technological processes are granted a degree of autonomy in decision making means automatically adapting services to meet varying needs of customers and facility providers, this challenges the abilities to maintain consistent and continuous security standards, and to provide appropriate business continuity and back-up, not least as it may not be possible to determine with any specificity where data processing will take place within the cloud [9]. As cloud computing considers all the aspects above, privacy solutions need to address verities of issues, and this may require new and even unique mechanisms rather than just a combination of known techniques for addressing selected aspects. Let us consider an example of privacy problems when transferring PII across borders within a group of companies can be addressed via Binding Corporate Rules. This approach would not be available to a corporation seeking to adopt a cloud computing solution where PII will be handled by third party cloud service providers.

Overall, the speed and flexibility of adjustment to service provider vendor offerings, which benefits business and motivates cloud computing uptake, brings a major risk to data security and privacy. This is a key user concern, particularly for financial and health data.

III. ACCOUNTABILITY

Cloud computing is the style of computing where massively scaled IT related capabilities are provided as a service across the internet to multiple external customers and are billed and there is a considerable growth in the usage of this service. Microsoft, Google, IBM, Yahoo and Amazon have started providing secure cloud computing services. Amazon is the pioneer in this field. somer companies like Smug Mug has used cloud services for the storing all the data and doing some of its services.It is important to clearly define what is meant by 'accountability' as the term is susceptible to a variety of different meanings within and across disciplines. For example, the term has used for a number of years in computer science to refer to an imprecise requirement that is met by reporting and auditing mechanisms. In this paper the context of its use is corporate data governance i.e. the management of the availability, usability, integrity and security of the data used, stored, or processed within an organization , and it refers to the process by which a particular goal – the prevention of disproportionate harm to the subjects of PII – can be obtained via a combination of public law (legislation, regulation), private law (contract), self-regulation and the use of privacy technologies (system architectures, access controls, machine readable policies).

3.1 What is Accountability?

Accountability is the term which is replacing to a variety of different meanings within and across disciplines. For example, the term has been used for a number of years in computer science to refer to an imprecise requirement that is met by reporting and auditing mechanisms. [13]. In this paper the context of its use is corporate data governance (the management of the usability, availability, integrity and security of the data used, stored, or processed within an organization), and it refers to the process by which a particular goal – the prevention of disproportionate harm to the subjects of PII – can be obtained via a combination of public law and regulation , private law such as contracts, self-regulation..

To date, various national and international privacy protection approaches have heavily influenced by public law, rules and regulations and premised upon command and control over the regulatory strategies. However, such legislative and regulatory mechanisms have declined in effectiveness as technological developments render the underlying regulatory techniques obsolete. Effective privacy protection for PII in some business environments is thus heavily compromised, and the ability of organizations to meaningfully quantify, control, and offset, their business risk is significantly impeded. It enjoins upon 'data controllers' a set of largely procedural requirements for their processing activities, and therefore conveys the impression that formal compliance will be enough to legitimise their activities. It encourages a box-ticking mentality, rather than a more systemic, and systematic, approach to fulfilling its values. [14]

The EU data protection regime, lacks effective regulatory responses for key developing technologies, such as mobile e-commerce and cloud computing [15]. Equally, self-regulation, in isolation, has failed to gain traction as a plausible alternative for effective privacy protection, with weak risk assessment and limited compliance checking [16].

Accountability in our sense will be achieved via a combination of private and public accountability. This term is derived from an active interaction between: subjects of PII; regulatory bodies, data controllers. It is premised upon highly transparent processes.

3.2 How Accountability might Provide a Way Forward for Privacy Protection within Cloud Computing

Solutions to privacy risks in the cloud involve reintroducing an element of control. For the corporate user, privacy risk in cloud computing can be reduced if organisations involved in cloud provision use a combination of privacy policies and contractual terms to create accountability in the form of transparent, enforceable commitments to responsible data handling . Specifically, accountable organisations will ensure that obligations to protect data (corresponding to user, legal and company policy requirements) are observed by all processors of the data with respect to the data processing occurs. Through contractual agreements, all organizations involved in the cloud provision would be accountable. While the corporate user, as the first corporate entity in the cloud provision, would be held legally accountable, the corporate user would then hold the initial service provider (SP1) accountable through contractual agreements, requiring in turn that SP1 hold its SPs accountable contractually as well. This is analogous to some existing cases in outsourcing environments, where the transferor is held accountable by regulators even when it is the transferee that does not act in accordance with individuals' wishes .

The following elements are key to provision of accountability within the cloud:

1. Individuals should be adequately informed about how their data is handled within the cloud and the responsibilities of people and organisations in relation to the processing of PII should be clearly identified. As with other disaggregated data environments, **transparency** in cloud computing is important not only for legal and regulatory reasons, but also to avoid violation of social norms.
2. The corporate user provides **assurance and transparency** to the customer/client through its privacy policy, while requiring similar assurances from the SP through contractual measures and audits.
3. Accountability helps **user trust**. When it is not clear to individual why their secure private information is requested, or how and by whom it will be processed, this lack of control will lead to distrust. There are also security-related concerns about whether data in the cloud will be adequately protected.
4. Most data protection regimes require a clear allocation of **responsibility** for the processing of PII, as existing regulatory mechanisms rely heavily upon user and regulator intervention with responsible parties. Such as. mobile e-commerce and cloud computing, can hinder determination of that responsibility. As information is shared and processed within the cloud, pre-empts perceptions of regulatory failure, which is also permits companies to assess their trading risks in terms of potential financial losses and data privacy data. This knowledge can be used to establish organisational and group privacy data and the available security standards, and to implement due diligence/compliance measures which conform to regulatory parameters, but which are otherwise negotiable between contracting organisations, based on relevant operational criteria.
5. Accountability helps ensure that the cloud service complies with laws, and also the mechanisms proposed in this **paper help compliance** with cloud provider organisational policies and auditing.

IV. CHARACTERISTIC OF A GOOD CLOUD COMPUTING FOR ACCOUNTABILITY

1. Any application running in a cloud computing environment has the private property of **self healing**. In case of sudden failure in the applications, there is always a good backup of the application ready to take over without disruption. There may be multiple copies of the same application - each copy updating itself regularly so that at times of failure there is at least one copy of the application which can take over without even the slightest change in its running state.
2. With cloud computing, any application supports **multi-tenancy** - that is multiple tenants at the same instant of time. The system allows several customers to share the infrastructure allotted to them without any of them being aware of the sharing. This is done by vitalizing the servers on the available machine pool and then allotting the servers to multiple users.
3. Cloud computing services are **linearly scalable**. The system is able to break down the workloads into pieces and service it across the infrastructure. An exact idea of linear scalability can be obtained from the fact that if one server is able to process say 1000 transactions per second, then two servers can process 2000 transactions per second.
4. Cloud computing systems are all **service oriented - i.e**. the systems are such that they are created out of other discrete services. Some of the discrete services which are independent of each other are combined together to form this service. This allowsto reuse the different services that are available and that are being created. Using the services that were just created, other such services can be created.
5. Usually businesses have agreements on the amount of services. **Scalability and availability** issues cause customer or clients to break these agreements. But cloud computing services are SLA driven such that when the system experiences peaks of load, it will automatically adjust itself so as to comply with the service-level agreements. The services will create additional instances of the applications on more servers so that the load can be easily managed.
6. The applications in cloud computing are fully decoupled from the underlying hardware. The cloud computing environment is **a fully virtualized** environment.
7. Another feature of the cloud computing services is that they **are flexible**. They can be used to serve a large variety of workload types - varying from small loads of a small consumer application to very heavy loads of a commercial application.

V. RELATED WORK ON INFORMATION SECURITY

In this section we try to highlight the framework suggested by of Marco Casassa Mont, Siani Pearson, Pete Bramhall discussed some problems related with the personal information security. In order to describe some of the aspects involved by the problem, we refer to an e-commerce scenario. In no way are the issues and aspects we highlight limited to this sector, as they are common to financial, government and enterprise areas. Figure 1 shows a scenario where users deal with electronic transactions that span across multiple e-commerce sites In this scenario a person initially provides their digital identity and profile information to an e-commerce site in order to access their services, possibly after negotiations about which privacy policies need to be applied (description of such a negotiation process is beyond the scope of this paper). Then the user logs in and interacts with these services: it might happen that in so doing he/she needs to involve other web sites or organisations. The user might be conscious of this or this might happen behind the scenes, for example due to the fact that the e-commerce site interacts with partners and suppliers.

The e-commerce site might need to disclose personal data to third parties (such as suppliers, information providers, government and financial institutions, etc.) in order to fulfil the specific transaction. The involved e-commerce. sites do not necessarily have prior agreements or belong to the same web of trust. The above scenario highlights a few key issues: how to fulfil users' privacy rights and make users be in control of their information. At the same time users' interactions need to be simple and intuitive. In general, users have little understanding or knowledge of the privacy laws and legislation that regulate the management of their information and their implications. Privacy and data protection laws that regulate this area do exist but it is hard to enforce or monitor them, especially when private information spread across organisations and nations' boundaries. In addition, further complexity arises due to the fact that privacy laws can differ quite substantially depending on national and geographical aspects. For example in US privacy laws restrict what the government can do with personal data but they introduce few restrictions on trading of personally identifiable information by private enterprises.

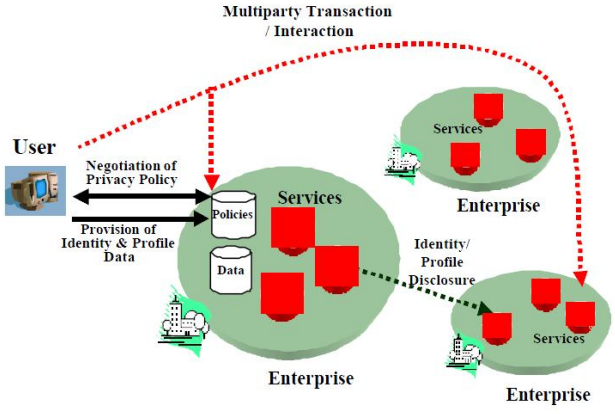

Fig. 1 : A Multiparty Transaction

In Europe (EU) people can consent to have their personally identifiable information used for commercial purposes but the default is to protect that information and not allow it to be used indiscriminately for marketing purposes. They suggested a problem to solve the related issues Figure 2 graphically shows how this model fits in the e-commerce scenario. In this model people use graphical tools (1) to: · Locally author their disclosure policies (i.e. sticky polices) in a fine-grained way; · Obfuscate their confidential data by directly using these disclosure polices; · Associate these policies to the obfuscated data. Some of the above activities can be automated by using predefined policy templates and scripts. Digital packages (2) containing obfuscated data along with their sticky polices can be provided to requestors such as e-commerce sites. These digital packages might contain a superset of the required information, to reduce the number of users' interactions. Selective disclosure of (part of) their contents will be authorised, depending on needs.

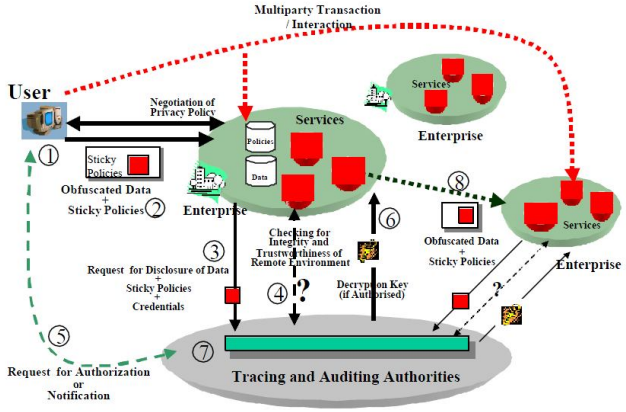

Fig. 2 : A proposed privacy Model by Marco Casassa Mont and others

A requestor (3) has to demonstrate to the Tracing Authority that he/she understands the involved terms and conditions. A Tracing Authority checks for the integrity and trustworthiness of the requestor's credentials and their IT environment (4), accordingly to the disclosure policies. The owner of the confidential information can be actively involved in the disclosure process (5) by asking for his authorizations or by notifications, according to the agreed disclosure policies.

In our model nothing prevents the owner of the confidential information from running a Tracing Authority. The actual disclosure (6) of any obfuscated data to a requestor (for example the e-commerce site) only happens after the requestor demonstrates to a trusted third party – i.e. the "Tracing Authority" - that it can satisfy the associated sticky policies. Disclosures of confidential data are logged and audited by the Tracing Authority (7). This increases the accountability of the requestors by creating evidence about their knowledge of users' confidential data. In particular this apply when confidential information is indiscriminately disclosed to third parties, as this evidence can be used for forensic analysis. In case a requestor sends the obfuscated data package to a third party (8), the same process, described above, applies. Multiple trusted third parties (Tracing Authorities) can be used in the above process in order to minimise the risks involved in the management of trust, for example having to rely only on one entity.Smitha Sundareswaran etc.al suggested a framework for cloud computing accountability

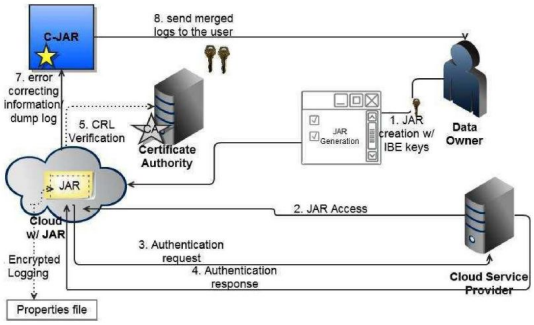

Fig. 3 : a framework for cloud computing accountability

Once the authentication succeeds, the service provider (or the user) will be allowed to access the data enclosed in the JAR. Depends on the settings defined at the time of creation, the JAR will provide usage control concerned with logging, or will provide only logging functionality. As for the logging, each and every time there is an access to the data, the JAR will automatically create a log record, encrypt it using the public key distributed by the data owner, and store it along with the data. The encryption of the log file prevents unauthorized changes to the file by attackers. The data owner could opt to reuse the same key pair for all JARs or create different key pairs for separate JARs. Using separate keys can enhance the security without introducing any overhead except in the initialization phase. In addition, some error correction information will be sent to the log harmonizer to handle possible log file corruption. To ensure difficulties of the logs, each record is checked and signed by the entity accessing the content. Further, individual records are coupled together to create a chain structure, able to quickly detect the data error and a missing records. The encrypted log files can later be decrypted and their integrity verified. They can be accessed by the data owner or other authorized stakeholders at any time for auditing purposes with the aid of the log harmonizer..

CONCLUSION

It is more and more important to defend and preserve people's privacy on the Internet, against unwanted and unauthorised disclosure of their confidential data. Despite laws, legislations and technical attempts to solve this problem, at the moment there are no solutions to address. Throughout this paper, the authors have systematically studied and review the security

and privacy issues in cloud computing. We have identified the most representative security/privacy attributes (e.g., confidentiality, integrity, availability, accountability, and privacy-preservability). Cloud computing is a new term that is introduced in business environment where users can interact directly with the virtualized resources and safe the cost for the consumers. Some security issues and their counter measures are discussed in this paper. It has several models to protect its data for the business users. An organization used private clouds within its organization to prevent from loss of data. Security in cloud computing consist of security abilities of web browsers and web service structure. We also discussed the cloud information accountability framework for data sharing in the cloud.

ACKNOWLEDGMENT

The authors would like to thanks the Department of Compute Engineering, TSSM's Padmabhooshan Vasantdata Patil Institute of Technology, Bavdhan, Pune, MS,IndiaFor the guidance and cooperation.

REFERENCES

[1] Solove, D.J.: A Taxonomy of Privacy, University of Pennsylvania Law Review, vol. 154, no 3, p. 477-564. (2006)

[2] Siani Pearsonand Andrew Charlesworth" Accountability as a Way Forward for Privacy Protection in the Cloud"

[3] Elias Nhoustis, John R. Rice, Efsrafstratiosgallopouls,Randall Bramley (Editors), Enabling Technologies for Computational Science Frameworks, Middleware and Environments, Kluwer-Academic Publishers, Hardbound, ISBN 0-7923-7809-1, 2000.

[4] A Cloud Com 2009, Beijing, Springer LNCS, December 2009.5. Ackerman, M., Darrell, T., Weitzner, D.: Privacy in Context. Human Computer Interaction, vol. 16, no.2, pp. 167-176 (2001)

[5] The Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud

[6] Computing.http://www.cloudsecurityalliance.org/guidance/csaguide.pdf (2009)

[7] Mr.Gellman, R.: Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing. World Privacy Forum, http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf (2009)

[8] Mr.Marco Casassa Mont, Siani Pearson, Pete Bramhall , Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services HPL-2003-49 March 19th , 2003*

[9] MRr.Abrams, M.: A Perspective: Data Flow Governance in Asia Pacific & APEC Framework. http://ec.europa.eu/justice_home/news/information_dossiers/personal_data_workshop/speeches_en.htm (2008)

[10] Kohl, U.: Jurisdiction and the Internet, Cambridge University Press (2007

[11] Mr. Mowbray, M.: The Fog over the Grimpen Mire: Cloud Computing and the Law. Script-ed Journal of Law, Technology and Society, vol. 6, no.1, April (2009)

[12] Mr. Hall, J.A. & Liedtka, S.L.: The Sarbanes-Oxley Act: implications for large-scale IT outsourcing. In: Communications of the ACM, vol. 50, no.3, pp. 95-100 (2007)

[13] Mr. McKinley, P.K., Samimi, F.A., Shapiro, J.K., Chiping T.: Service Clouds: A Distributed Infrastructure for Constructing Autonomic Communication Services. Dependable, Autonomic and Secure Computing, IEEE, pp.341-348, (2006)

[14] Conn,R. ,Cederquist, J.G., Dekker, M.A.C., Etalle, S., den Hartog, J.I.: An audit logic for accountability. In: Policies for Distributed Systems and Networks, IEEE, pp. 34-43 (2005)

[15] UK Information Commissioner's Office A Report on the Surveillance Society (2006)

[16] Charlesworth, A.: The Future of UK Data Protection Regulation. Information Security Technical Report vol. 11, no.1. pp. 46-54 (2006)

[17] Charlesworth, A. Information Privacy Law in the European Union: E Pluribus Unum or Ex Uno Plures. Hastings Law Review, vol. 54, pp. 931-969 (2003),

[18] Conn R. Dekker Cederquist, J.G., , M.A.C., Etalle, S., den Hartog, J.I.: An audit logic for accountability. In: Policies for Distributed Systems and Networks, IEEE, pp. 34-43 (2005)