Achieving Regulatory Compliance for Data Protection in the Cloud

Enterprise Approaches to Distributed Encryption Management

Mark Rivis, Shao Ying Zhu
School of Computing and Mathematics,
The University of Derby,
Derby, United Kingdom.

***Abstract*—The advent of cloud computing has enabled organizations to take advantage of cost-effective, scalable and reliable computing platforms. However, entrusting data hosting to third parties has inherent risks. Where the data in question can be used to identify living individuals in the UK, the Data Protection Act 1998 (DPA) must be adhered to. In this case, adequate security controls must be in place to ensure privacy of the data. Transgressions may be met with severe penalties. This paper outlines the data controller's obligations under the DPA and, with respect to cloud computing, presents solutions for possible encryption schemes. Using traditional encryption can lead to key management challenges and limit the type of processing which the cloud service can fulfill. Improving on this, the evolving area of homomorphic encryption is presented which promises to enable useful processing of data whilst it is encrypted. Current approaches in this field have limited scope and an impractical processing overhead. We conclude that organizations must thoroughly evaluate and manage the risks associated with processing personal data in the cloud.**

Keywords—cloud computing; data protection legislation; Data Protection Act 1998; homomorphic encryption; data privacy; symmetric encryption

I. INTRODUCTION

In the UK, information relating to living individuals is regulated by some of the most rigorous privacy legislation in the world. The Information Commissioner's Office (ICO) regularly has cause to use its powers to enforce the Data Protection Act 1998 (DPA). Punitive fines can be imposed, often running to hundreds of thousands of pounds, depending on the nature and impact of the data breach [8]. There is at present no duty to disclose a data breach to the ICO [9]; however the obligation to adhere to the DPA is a serious one, with severe penalties for non-compliance [10].

Whilst managing their statutory obligations, most organizations are also duty bound to make cost effective use of their computing resources. One means of reducing costs is the move from traditionally hosted computing services to those present "in the cloud". Cloud computing can offer flexibility, convenience and resilience for essential business services, usually at a reduced total cost [2].

Martens, Walterbusch and Teuteberg [22] present a model to assess the total cost of ownership (TCO) of cloud computing services. By taking advantage of shared environments in a multitenant model, computing service providers can deliver systems over the Internet which often makes a compelling proposition.

However, as an evolving computing paradigm, the risks to data privacy must be carefully balanced with any *prima facie* benefits of cloud computing. Initial deployments of cloud computing systems have been secured using existing technology, such as secure sockets layer (SSL) and public key encryption. However, as the technical vulnerabilities of a shared data processing infrastructure become better known, it is apparent that new means of securing data in this environment must be sought.

Whether any business will take up public cloud computing services depends primarily on their appetite for risk, versus the expected cost savings. In many cases businesses are avoiding the uncertainty of using cloud services in preference for a more assured security posture [1]. To fully enable the take up of cloud computing, new approaches to storing and processing encrypted data in a shared environment must be developed.

This paper's contribution is in presenting details of UK privacy legislation in the context of cloud computing. Detailed research has been carried out in the computer science literature on the latest techniques for processing encrypted data in a shared computing environment. A critique of these approaches is offered and the conclusion drawn on the efficacy of these approaches. Final comments are made on the open issues which will be the subject of future work.

The rest of this paper is structured as follows. The background to current data protection legislation is presented in Section 2, with specific reference to the security principles of the DPA reviewed in Section 3. Concepts of cloud computing are discussed in Section 4. Following, in Section 5, the applicability of the DPA and implications of a data breach are considered. Measures to achieve data compliance are presented in Section 6 with a review of approaches to encryption. Anticipated future developments are discussed in Section 7, and final conclusions are drawn in Section 8.

II. DATA PROTECTION LEGISLATION

Legislative instruments are in place in parts of the western world giving individuals certain rights over the data which is held about them. Specifically in the European Union (EU), the Data Protection Directive of 1995 [23] required member states to enact their own local legislation, giving a consistent

approach to data protection across nations. As a consequence of this, the UK enacted the DPA [5]. It is this act which provides the basis for a discussion of data protection here, but of course the principles could apply in parallel across other EU member states.

The United States has no single piece of legislation providing a comparative basis for data protection. Instead, a "sectoral" approach is taken, with different business areas required to comply within their own framework of regulation. Examples are the Health Insurance Portability and Accountability Act of 1996 (HIPAA) [25], and Federal Information Security Management Act of 2002 (FISMA) [26], which apply to the health insurance industry and federal agencies respectively.

Given the differing approaches to privacy legislation, there would not ordinarily be a simple method of comparing the levels of data protection afforded by various industries in the US and EU. To smooth the path to global trade (where the sharing or export of data is required), the US and EU have worked together to develop the "Safe Harbor" scheme. The EU regulations have stricter privacy controls in general, so US companies can be assessed for Safe Harbor, which ensures they meet the EU "adequacy" requirement for data privacy [21].

III. United Kingdom Data Protection Act 1998

A brief summary of the DPA is presented here, with particular note being made of the act's relevance to cloud computing. All references are drawn from the online record of the legislation published by Her Majesty's Stationery Office [5].

The scope of the DPA is restricted to systems processing personal information which could be used to identify a living individual. With respect to cloud computing (or any other computing platform), this initial test of applicability will determine whether regulatory compliance is required for that system.

Three roles are defined by the act. They are the data subject (the person to whom the data relates), the data controller (who determines the purpose and manner of data processing) and the data processor (who carries out processing of the data on behalf of the data controller). In a cloud computing environment it is most commonly the case that the data processor will be a third-party company providing cloud services. It is essential then that the data controller and data processor have a clear understanding of the nature of their relationship, and their obligations under the act.

The act lists eight principles which define how data may be processed [24]. These can be summarized as follows:

1) Personal data shall be processed fairly and lawfully

2) Personal data shall be obtained and processed only for one or more specified and lawful purposes

3) Personal data shall be adequate, relevant and not excessive

4) Personal data shall be accurate and kept up to date.

5) Personal data shall be kept only for as long as necessary to fulfil the purpose for which it was obtained

6) Personal data shall be processed in accordance with the rights of data subjects under this Act

7) Appropriate security measures must be taken to prevent unauthorized access to data, and to prevent accidental loss, destruction or amendment of personal data.

8) Personal data shall not be transferred to any country outside the European Economic Area (EEA), unless that country has adequate levels of protection for processing personal data.

Most of the principles should be met through the operational business processes of the data controller. It can be seen that purely technical measures will not enable compliance with the act in respect of many of these principles. However it is principles seven and eight which warrant closer scrutiny in a cloud computing environment.

IV. Cloud Computing

A. Definition

Often described as an emerging computing paradigm, cloud computing is enabled by the conjunction of multiple maturing technologies. For some years it has evaded a clear and concise description; however this has evolved as the technologies used have become more established. A definition of cloud computing is provided by the National Institute for Standards and Technology (NIST) in their Special Publication 800-145 [14]. Five key attributes are present in their definition:

- On-demand self-service – the consumer is able to provision the service autonomously
- Broad network access – access is available from heterogeneous devices and network media
- Resource pooling – a multi-tenant model enables economies of scale for the service; location independence is often a feature here but in some cases the customer can restrict the physical location of their resources (e.g. by country or data centre)
- Rapid elasticity – depending on demand the resource available can be scaled up or retracted
- Measured service – the model enables pay-per-use accounting, with only the resources used being charged for.

As well as the defining cloud computing characteristics, [14] also offers definitions of three service models:

Software as a Service (SaaS) – access to an application is provided as part of the service. The customer has no control over the applications infrastructure or how it operates, other than processing their data (which may entail choosing some application level settings.) An example is the Customer Relationship Management (CRM) system provided by salesforce.com.

Platform as a Service (PaaS) – the consumer is able to deploy applications to the cloud infrastructure but is not able to influence the underlying architecture. System components can be implemented as middleware, harnessing the cloud-service processing power as they interact with other components. An

example is Google's AppEngine service where a range of web applications can be integrated using Application Programming Interfaces (APIs.)

Infrastructure as a Service (IaaS) – in this model the capability to provision lower level system components is provided to the user. Decisions can be made as to the size and type of resources such as processors, memory, network and storage. They may usually choose the type of operating system and application software which is deployed to the infrastructure. Amazon's Elastic Compute Cloud (EC2) is a prime example of an IaaS offering. Weinhardt, et al., [29] provided an early representation of this model in their Cloud Business Model Framework. Their work highlights the evolution of cloud computing, differentiating it from the earlier grid computing paradigm. A graphical representation of this is reproduced in Figure 1, which summarizes this layered approach to cloud platforms [29].

B. Data Protection Implications in Cloud Computing

Drawing together the requirements of the DPA and the definition of cloud computing, it can be seen that some challenges and risks to compliance in this environment are brought about. Introducing a third party as a cloud service provider changes the data processor role as defined by the act. Therefore the relationship between the data controller and data processor must be clearly defined and respective responsibilities well understood. A written contract is required by the DPA between the data controller and the data processor, requiring that "the data processor is to act only on instructions from the data controller" and "the data processor will comply with security obligations equivalent to those imposed on the data controller itself" [7]. In this guidance, the ICO also describes how organizations should be aware of the possible "layered" nature of cloud computing services. That is to say, a data controller may use an on-line web application from cloud provider A (as SaaS), however that provider may also be using cloud provider B to host its services (as IaaS.)

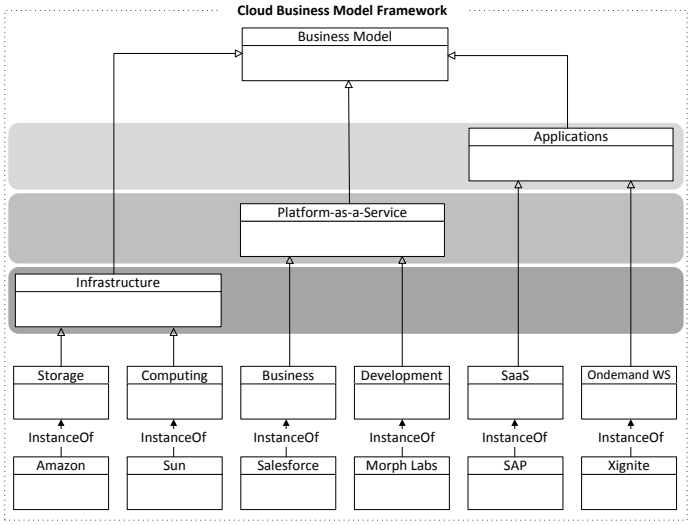

Fig. 1. Cloud Business Model Framework

These potentially complex relationships and roles (with respect to the DPA) must be well understood.

Principle eight of the DPA says that personal data may not be exported outside of the EEA, unless adequate data protection controls are in place. As noted, US companies may be accredited for the Safe Harbor scheme to demonstrate that their controls are adequate. Therefore when choosing a cloud service provider it is essential to understand broadly where personal data will be stored, restricted to territories within the EEA or others with "adequate" data privacy controls. This must be the subject of binding service agreement such that the data controller's obligations under the DPA can be met.

V. Implications of a Data Breach

Aside from the short term effect on staff productivity, the primary implications of a data breach against a business or other organization are twofold.

Firstly, if the entity was deemed to be negligent in contravening the DPA, the ICO has the power to act in some way. Its range of powers includes the criminal prosecution of those who contravene the act, and the issuing of monetary penalties of up to £500,000 for serious breaches. This would be the case where the security measures in place were not sufficient, counter to principle 7 of the act. It is recognized however that not all data breaches are equal; the ICO will take a different view of a breach due to poor procedural controls on the part of the data controller than it would where a criminal act is committed by a malicious attacker. Guidance published by law firm Pinsent-Masons states "a data controller will not be in breach of the Act if it can show that appropriate security measures were taken" [15].

The second aspect of a data breach is the reputational damage which follows if (or when) the event becomes public knowledge. Note that there is currently no requirement in the UK for organizations to report data breaches [9]. Future legislation may change this. Draft EU legislation is being discussed which would enforce the requirement to notify local data protection authorities and the data subjects of a breach [3]. The reputational impact may have varied effects on the organization, including reduced customer loyalty, reduced amount of new business, increased customer turnover and potentially a reduced share price for stock market listed companies [16].

Clearly the impact of a publicly known data breach goes beyond the lost effort of resolving the immediate issues, and the financial penalty imposed by regulatory bodies. Organizations must therefore balance the risk of a data breach occurring, with the cost of any measures which are put in place to prevent such breaches.

VI. Measures to Achieve DPA Compliance in Cloud Computing

A. Symmetric Encryption

The use of encryption is recognized as a means to achieving DPA compliance by ensuring that only authorized parties can read the personal data in question. The suitability of solutions for encrypting data in the cloud depends on various factors

which include, *inter alia*, the number of users requiring access, the nature of data sharing between users, the level of computation the cloud system is required to perform and the quantity and structure of data in question.

In proposing a simple encryption scheme to protect data, a further challenge arises, since encrypted data cannot normally be processed in the cloud (as though it were stored in the clear.) Whilst this approach provides a good degree of security assurance, any agent that does not have the necessary key to decrypt the data is unable to interact with it. In this sense, the cloud is reduced to providing data storage at a third-party facility. This may be desirable in some cases, but the capability of providing some kind of remote processing of data may be required.

Puttaswamy, Kruegel and Zhao [17] identify that when processing data it is often the case that the actual value of some data elements does not need to be known. It is therefore feasible to encrypt some data and still carry out useful operations on it. This type of data they describe as functionally encryptable, that is, data which can be encrypted without affecting the functionality of the application. In their system "Silverline", they describe a multistage framework to achieve this. The method includes automatically identifying functionally encryptable data, managing keys to encrypt and decrypt data shared within role-based groups of users, and providing transparent data access through a scheme of trusted and untrusted web browser interface components.

Their results show that for some common web applications about 70-80% of data could be encrypted by this system. The focus on automation is designed to allow an easy transition for existing web applications to using this encryption model in the cloud.

There is however a significant drawback in the approach of partial encryption. Whilst it is convenient to take an existing application and automatically modify its behaviour to encrypt some of its data operations, there is no assurance that personal data would be considered functionally encryptable for the application in question. In that case there is no advantage to using the Silverline system as a means of increasing security to achieve DPA compliance.

A system relying on symmetric encryption key management is proposed by Litwin, Jajodia and Schwarz [11]. In their scheme, each user has their own symmetric key which is used to encrypt data uploaded to the cloud. All symmetric keys are also uploaded to the cloud but remain hidden by some means. If a user wants to share data with another, they unhide their symmetric key so that they are both able to decrypt the data. This approach, whilst sound in so far as can be applied, is limited in its potential. It works along the lines of traditional file sharing permissions, applying encryption, and using key management as a method of granting and revoking access. It does not leverage the computing capabilities of cloud systems beyond data storage and sharing.

An alternative approach to enabling cloud computing for security-sensitive businesses relies on separating data storage and data processing providers [28]. Interfacing between these services is an independent encryption/decryption service in the cloud. This approach enables service providers to be selected based on differing levels of trust, with processing being handled at a highly trusted cloud service, and (encrypted) data storage at a less trusted facility.

B. Homomorphic encryption

It is recognized in the field of cryptanalysis that the ability to process data whilst it is encrypted would open the way to new distributed computing models, with reduced risks to data privacy. In effect, the data processor would be able to carry out some operations on the data without actually being able to decrypt it. This was recognized by Rivest, Adleman and Dertouzos in [18] where a set such functions is described. Their work is an extension of the earlier paper which described the RSA public key cryptosystem [19]. The correlation comes about because RSA encryption is homomorphic for multiplication (but not addition).

Homomorphic operations can be carried out on data without decrypting it in the conventional sense. An inherent limitation is noted in [18], however, in that comparison operations would not be allowed under such a model. If that were the case, then a malicious user would be able to carry out a simple binary search of encrypted data, and once a comparison match was found, would be able to deduce the unencrypted value. In identifying the possibility of privacy homomorphisms, Rivest, Adleman and Dertouzo [18] opened the way for further work to find computationally practical implementations.

A fully homomorphic encryption (FHE) scheme is one where arbitrarily complex operations can be carried out against encrypted data.

Gentry [4] described such a scheme based on ideal lattice cryptography. It is recognized however that this is computationally impractical as the amount of effort required increases rapidly as the security level increases.

Attempts to refine and enhance FHE schemes continue. In addition to new cryptanalysis techniques, some trials attempt to speed up the encryption and decryption processes with massively parallel programming techniques using graphics processing units (GPUs). Single-digit improvements in performance are reported [27]. Whilst providing some improvement, this does not in itself make such techniques practically useful.

A somewhat homomorphic encryption (SwHE) scheme can carry out some set of defined operations on encrypted data. Naehrig, Lauter and Vaikuntanathan [12] describe a SwHE scheme based on the "ring learning with errors" problem, which exhibits good performance. They also describe some real-world cloud computing scenarios where the limited functionality of SwHE could be employed.

Research continues into developing a comprehensive fully homomorphic encryption system which can be implemented using practical computation resources. López-Alt, Tromer and Vaikuntanathan [13] describe how multiple parties can encrypt their own data for collaborative processing in the cloud, whilst retaining privacy over their original data. This is implemented using an enhancement of NTRU encryption, an efficient public

key cryptosystem based on lattices, originally developed by Hoffstein, Pipher and Silverman [6]. NTRU is fast and scalable when compared to other public key crypto systems; it is claimed that for increases in the message length *n*, the encryption and decryption requirements of NTRU increases with n^2, where RSA increases with n^3 [6].

When encryption is applied to cloud computing systems the matter of key management becomes problematic. Some challenges around user access management become apparent in this case:

- How do we revoke access to data for some users without having to re-encrypt data?
- How do we avoid collusion between users and the cloud provider?
- How are changes to user privileges managed?

Samanthula, Howser, Elmehdwi and Madria [20] propose a scheme to handle such key management challenges using homomorphic encryption and proxy re-encryption, whereby encrypted data is re-encrypted for a new recipient without having to decrypt it first. This approach gives some benefits in handling user management for data sharing but their focus neglects the need to process data in the cloud. For example, if encrypted data is written to a database, the database process itself would either need to decrypt the data or carry out FHE operations on it to do any useful work. In the former case the same risk is present, in that the database process may be compromised allowing a malicious attacker to read the data. It is the latter case, that is, finding a workable FHE scheme which remains elusive.

The future implications of being able carry out computational operations on encrypted data are not yet clear. It seems likely that if an encryption scheme is available which has low management overhead, yet retains privacy amongst untrusted third party service providers, the potential for enterprise take up of cloud computing will greatly increase. However the current restriction of being unable to carry out comparison functions seems to limit the actual usefulness of this approach in processing information.

VII. Future Work

In the field of cryptography, work continues with the focus of finding either a FHE scheme which is computationally efficient, or a SwHE scheme which is sufficient to meet specific use cases. In both scenarios the goal is to find a system which is effective and has a manageable overhead in terms of its operational processes, for example, key management.

When applied to cloud computing, techniques which rely on encrypting partial data attributes or managing symmetric encryption keys require a certain amount of application customization. They may provide some assurance that DPA compliance can be achieved but the development overhead means such approaches are largely bespoke.

For organizations concerned with DPA compliance, current approaches to cloud computing are primarily based on risk management. This requires consideration of factors in three areas.

Technological risks of using cloud systems. Resources are available which highlight some technological risks [1] but this is an area which continues to evolve. Periodic assessment of the weaknesses of cloud computing and the capabilities of threat agents should be undertaken.

Legal obligations. Notwithstanding the operational and reputational impacts of a data breach, there is a requirement to provide security which is 'good enough' for the organization. Measures must be taken to ensure data privacy based on the perceived risks and appropriate to the nature of the data.

Organizational relationships. Cloud computing simplifies the deployment of technology, but adds complexity in organizational relationships. Multiple third parties may be involved, either at inception or in the future. There must be a clear understanding of the responsibilities and obligations of all parties.

VIII. Conclusion

Cloud computing presents a valuable opportunity to organizations, enabling services which are not only cost effective, but flexible, resilient and accessible from anywhere on the Internet.

There is of course no variation in the legal framework with respect to cloud computing; organizational obligations remain consistent in this regard. Clarification on the applicability of the DPA is available from the ICO and supporting resources are published by proponents of cloud initiatives.

Encryption of sensitive data is recommended by the ICO as a means to preserve data privacy. However using traditional methods limits the applications where cloud computing can be used effectively, and presents major challenges in key management.

The evolving field of homomorphic encryption appears to offer promising opportunities here. By using specific encryption schemes, it is possible to carry out useful operations on encrypted data without ever having access to the unencrypted data. Early work has demonstrated the principle, but resulted in impractical computational workloads. The secure processing of encrypted data by a third party is not yet practicable.

Organizations must be cognisant of the implications of using cloud computing services, taking a risk based approach specific to their circumstances.

References

[1] Cloud Security Alliance, 2010. Top Threats to Cloud Computing V1.0. Available at: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, accessed 2 December 2012.

[2] Cloud Security Alliance, 2011. Security Guidance for Critical Areas of Focus in Cloud Computing v3.0. Available at: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf, accessed 2 December 2012.

[3] European Parliament, 2009. Directive 2009/136/EC of the European Parliament. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:01:EN:HTML, accessed 6 December 2012.

[4] C. Gentry, "Fully homomorphic encryption using ideal lattices," Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC '09), ACM, pp. 169-178, Jun. 2009, doi:10.1145/1536414.1536440.

[5] Her Majesty's Stationery Office, n.d. Data Protection Act 1998. Available at: http://www.legislation.gov.uk/ukpga/1998/29/contents, accessed 2 December 2012.

[6] J. Hoffstein, J. Pipher, J. H. and Silverman, "NTRU: A ring-based public key cryptosystem," Proceedings of the Third International Symposium on Algorithmic Number Theory (ANTS-III), Springer-Verlag, Jun. 1998, pp. 267-288, doi:10.1007/BFb0054868.

[7] Information Commissioner's Office, 2012. Guidance on the Use of Cloud Computing. Available at: http://www.ico.gov.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx, accessed 7 December 2012.

[8] Information Commissioner's Office, 2012. Monetary penalty notices. Available at: http://www.ico.gov.uk/enforcement/fines.aspx, accessed 7 December 2012.

[9] Information Commissioner's Office, 2012. Notification of data security breaches to the Information Commissioner's Office (ICO). Available at: http://www.ico.gov.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/breach_reporting.ashx, accessed 6 December 2012.

[10] Information Commissioner's Office, n.d. Taking action: data protection and privacy and electronic communications. Available at: http://www.ico.gov.uk/what_we_cover/taking_action/dp_pecr.aspx, accessed 6 December 2012.

[11] W. Litwin, S. Jajodia, and T. Schwarz, "Privacy of data outsourced to a cloud for selected readers through client-side encryption," Proceedings of the 10th Annual ACM Workshop on Privacy in the Electronic Society (WPES '11), ACM, Oct. 2011, pp. 171-176, doi:10.1145/2046556.2046580.

[12] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?," Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop (CCSW '11), ACM, Oct. 2011, pp. 113-124, doi:10.1145/2046660.2046682.

[13] A. López-Alt, E. Tromer, and V. Vaikuntanathan, "On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption," Proceedings of the 44th Symposium on Theory of Computing (STOC '12), ACM, May 2012, pp. 1219-1234, doi:10.1145/2213977.2214086.

[14] National Institute of Standards and Technology, 2011. The NIST Definition of Cloud Computing. Available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, accessed 2 December 2012.

[15] Pinsent Masons, n.d. Data Security. Available at: http://www.pinsentmasons.com/en/media/published-articles/data-security/, accessed 6 December 2012.

[16] Ponemon Institute LLC, 2012. Aftermath of a Data Breach Study. Available at: http://www.experian.com/assets/data-breach/brochures/ponemon-aftermath-study.pdf, accessed 6 December 2012.

[17] K. P. Puttaswamy, C. Kruegel, and B. Y. Zhao, "Silverline: toward data confidentiality in storage-intensive cloud applications," Proceedings of the 2nd ACM Symposium on Cloud Computing (SOCC '11), ACM, Oct. 2011, article no. 10, doi:10.1145/2038916.2038926.

[18] R. L. Rivest, L. Adleman and M. L. Dertouzos, "On data banks and privacy homomorphisms," in "Foundations of Secure Computing," pp. 169-180, edited by DeMillo, R., Dobkin, D., Jones, A. and Lipton, R., New York: Academic Press, 1978.

[19] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, iss. 2, Feb. 1978, pp. 120-126, doi:10.1145/359340.359342.

[20] B. K. Samanthula, G. Howser, Y. Elmehdwi, and S. Madria, "An efficient and secure data sharing framework using homomorphic encryption in the cloud," Proceedings of the 1st International Workshop on Cloud Intelligence (Cloud-I '12), ACM, Aug. 2012, article no. 8, doi:10.1145/2347673.2347681.

[21] US Department of Commerce International Trade Administration, 2012. Welcome to the U.S.-EU Safe Harbor. Available at: http://export.gov/safeharbor/eu/eg_main_018365.asp, accessed 7 December 2012.

[22] B. Martens, M. Walterbusch, F. Teuteberg, "Costing of cloud computing services: a total cost of ownership approach," Proceedings of the 2012 45th Hawaii International Conference on System Sciences (HICSS '12), IEEE Computer Society, Jan. 2012, pp. 1563-1572, doi:10.1109/HICSS.2012.186.

[23] European Parliament, 1995. Directive 95/46/EC of the European Parliament. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML, accessed 4 February 2013.

[24] Information Commissioner's Office, n.d., Data protection principles. Available at: http://www.ico.gov.uk/for_organisations/data_protection/the_guide/the_principles.aspx, accessed 4 February 2013.

[25] US Government Prinitng Office, n.d., Public Law 104 - 191 - Health Insurance Portability and Accountability Act of 1996. Available at: http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/content-detail.html, accessed 4 February 2013.

[26] The Library of Congress, n.d., E-Government Act of 2002. Available at: http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.2458.ENR:, accessed 4 February 2013.

[27] Wei Wang; Yin Hu; Lianmu Chen; Xinming Huang; B. Sunar, "Accelerating fully homomorphic encryption using GPU," High Performance Extreme Computing (HPEC), 2012 IEEE Conference on, 10-12 Sept. 2012, pp.1-5, doi: 10.1109/HPEC.2012.6408660

[28] Jing-Jang Hwang; Hung-Kai Chuang; Yi-Chang Hsu; Chien-Hsing Wu, "A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service," Information Science and Applications (ICISA), 2011 International Conference on, 26-29 April 2011, pp.1-7, doi: 10.1109/ICISA.2011.5772349

[29] C. Weinhardt, A. Anandasivam, B. Blau, N. Borissov, T. Meinl, W. Michalk, and J. Stößer,"Cloud computing – a classification, business models, and research directions," Business and Information Systems Engineering (BISE), vol. 1, no. 5, pp. 391-399, 2009.