Enhancing Cloud Security and Privacy: The Cloud Audit Problem

Bob Duncan
Computer Science
University of Aberdeen
Aberdeen, UK
Email: bobduncan@abdn.ac.uk

Mark Whittington
Accounting and Finance
University of Aberdeen
Aberdeen, UK
Email: mark.whittington@abdn.ac.uk

***Abstract*—Many people assume that cloud audit is no more difficult than IT audit in general. We provide an outline of the evolution of cloud, providing an explanation of how it differs from conventional IT. We then discuss some of the benefits and drawbacks of cloud, particularly in connection to audit challenges, highlighting the dangers and shortcomings of many approaches.**

***Keywords*—security; privacy; standards; compliance; audit.**

I. INTRODUCTION

Cloud computing offers the possibility of a substantial economic benefit to firms and governments, yet at the same time, increases complexity and risk. This results in an interesting dilemma. On the one hand, potential cost savings of 50 - 90% [1] are possible, which is highly attractive, but on the other hand, complexity can increase exponentially, placing significant increasing risk on business and government alike.

In previous work [2] on enhancing cloud security and privacy, we addressed issues of the cloud service provider's (CSP) lack of accountability in the standard service level agreement (SLA). We mentioned the importance of the role assurance plays, and the two main mechanisms used to achieve this, namely compliance and audit. In this paper, we will address some of the issues relating to audit. In order to understand how the use of cloud impacts on the audit process, and how it differs from conventional IT audit, we need to first understand what audit is, why we need to do it, who should be doing it and how it should be done. We must also understand what special difficulties the use of cloud brings to audit. We therefore revisit our definition of audit.

Audit (OED [3]: "To make an official systematic examination of (accounts), so as to ascertain their accuracy") requires outsiders who are deemed to be both objective and expert to form their own opinion of what is being audited and then to publicly state their confidence (or otherwise) in the reliability of what they have investigated. Auditing is not straightforward or easy. Just as with accounting auditors, objectivity is difficult when companies pay auditors directly and auditors would also like to be retained for the following year. Audit is also potentially very expensive if done well by the best experts in the field and there is a temptation to reduce the experts' role to one of advising, often writing checklists to be administered by qualified technicians.

We start by considering the purpose of audit, who should be carrying it out, and how it should be done, which we address in Section II. The remainder of the paper is organised as follows: Looking at past corporate computing models, Section III provides us with an understanding of how corporate computing has evolved over recent years, how these stages of evolution have developed, and how they compare and impact on cloud computing. In Section IV, we look at how audit is currently performed. In Section V, we question whether there are any weaknesses in this approach and; in Section VI, we touch on some of the cloud security compliance issues. Section VII, considers how to tackle these weaknesses; and finally, in Section VIII, we discuss our conclusions.

II. THE PURPOSE OF AUDIT

We consider three main purposes of audit, the most widely understood of which is the statutory requirement for financial statements to be audited by an independent external auditor, which has been a cornerstone of confidence in global financial systems since auditing was introduced. It provides assurance that company managers have presented a "true and fair" view of a company's financial performance and position, underpinning the trust and obligation of stewardship between company management and the owners of the company, the shareholders.

A second purpose of audit is IT systems audit. Traditional audit approaches often involved treating IT systems as "black box" systems, meaning trust was placed in the IT systems, and looking at the functioning of the IT system was not considered part of the statutory audit. The obvious shortcoming of this approach was addressed by conducting a specific IT based audit of the IT systems, to ensure these systems performed exactly as expected. These audits are usually conducted by IT specialists, often in conjunction with accounting audit professionals to ensure the functioning of these systems are properly understood. However, these are not mandated under statute, which presents a weakness. In addition, there is no requirement for an annual audit to be undertaken.

A third purpose of audit is compliance, either with regulations, or more often with standards. This is often undertaken to assure shareholders and other stakeholders that the company is using best practice in its operations. This is particularly the case in cloud computing, where systems are operated by third parties beyond the control of the cloud user. Currently, the difficulties associated with performing an adequate cloud audit present one of the key barriers to cloud adoption [33]. These audits are not mandated under statute, which presents a weakness, and there is no requirement for an annual audit to be undertaken.

Statutory audit is an area which is well understood and which benefits from over a century of research and experience. Despite this, there remain differences of opinion and a number of problems are yet to be resolved. Duncan and Whittington provide some useful background in [5]. One of the main issues concerns the independence of the auditor. The auditor is meant to be independent, yet is paid by the firm they are auditing.

 ISBN: 978-1-61208-460-2

There may also be additional links between the auditor and the firm, such as other non-audit consulting work undertaken by the auditor. An audit firm is keen to remain auditor of the firm for a long period of time to ensure continuity of income and enhancement of profit. The firm is often keen not to change auditor too frequently, lest their reputation suffer damage by being unable to retain an auditor, as well as trying to keep costs to a reasonable level. Audit firms are keen to undertake non-audit consultancy work in order to further maximise revenue and profits. The firm is generally keen for this practice to take place, due to perceived cost savings to the firm. These arrangements can potentially create tensions, which in some cases might affect the impartiality of the auditor, hence some jurisdictions seek to limit consultancy by auditors. Despite issues, financial auditors are heavily regulated, audits are mandatory and must be carried out every year.

Some industries are regulated and often the regulator will assure themselves of compliance with regulations through the use of audit. In the UK, organisations such as The Office of Gas and Electricity Markets (Ofgem); The Office of Water Services (Ofwat); The Office of Telecommunications (Oftel); The Postal Services Commission (Postcomm); The Civil Aviation Authority (CAA); The Office of the Rail Regulator (ORR); The Office for the Regulation of Electricity and Gas in Northern Ireland (Ofreg); and The Office of Communications Ofcom) will often use reports given by the company's auditor. These will generally be carried out based on the requirements of the licence granted by the regulator. The Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) usually take this view, although requirements here are often more onerous. Some regulators, such as those responsible for the regulation of professional services, may conduct the audit using their own auditors, and frequency of audit is usually less regular than with financial accounting.

Cloud audit difficulties have long been seen as a potential barrier to cloud adoption [33] [6], and there is certainly a belief that trust and privacy issues [7] [8] [9] [10] also need to be borne in mind. A common theme is the recognition that cloud audit is far harder to perform than for non-cloud systems.

Audit may be required to test internal control systems, particularly where they involve financial reporting. This can extend to IT audit, where rather than treat the IT systems as black box components of the company systems, the IT systems themselves are audited to provide assurance that they are capable of delivering what is needed by the company. Audit may also be required where a company is involved in a joint venture project with another company or companies. The audit requirements will usually be built in to the terms of the joint venture agreement, specifying who will have what rights to conduct the audit. Audit will not necessarily be mandatory, nor will the auditors and audit process necessarily be regulated.

Another facet of audit is internal audit, where a company seeks to assure itself of how well its internal processes are running. Often this is continuous in nature, rather than sporadic. It is not mandatory and there is no regulation of the auditors or the audit process. In previous work with Pym [11], we developed a cloud assurance model which uses continuous internal audit to help achieve the required security goals. Audit can be used to test for fraud. Forensic audit is used if fraud is discovered, to find and collect suitable evidence for presentation in a court case, whether criminal or civil.

While auditing in the accountancy world has enjoyed the benefit of over a century of practice and experience, cloud computing audit can not be considered a mature field, and there will be some way to go before it can catch up with the reflection and rigour of work done in the accounting profession. An obvious area of weakness arises when taking audit professionals from the accounting world out of their comfort zone, and placing them in a more technical field. Whilst the use of people with a computing background can overcome some of these issues, their lack of audit background presents another weakness. Clearly further research will be needed in this area.

Thus we see that there is more than one purpose for conducting audit. We can have: statutory audit, which might extend to audit of internal control over financial reporting and fraud audit; IT audit, which covers the audit of IT systems; and compliance audit, which will include regulatory compliance, standards compliance, joint venture compliance, internal audit and forensic audit. This list is not exhaustive. Of all the purposes of audit, statutory audit is the most rigorous and highly regulated, and for cloud, we could do well to learn from this wealth of experience and rigour. In today's world, information can be just as valuable as money. The impact of compromise, leakage, or theft of information can have a catastrophic impact on cloud users, thus it makes sense to consider applying equal rigour to the protection of information.

III. How did Cloud Computing Evolve?

Corporates have long understood the potential benefits to be gained from embracing information technology ever since the early days of computing, when expensive mainframes were the only option — open only to the largest corporates. Since those days, modern information systems have evolved considerably, leading to the development of complex, highly distributed information systems and the need to police them properly. The need to address traditional security issues of confidentiality, integrity and availability (CIA) has increased this complexity further, due to the need for scalability and redundancy. We have seen a relentless explosion in performance, cost reductions and wider accessibility for more and more corporates. Massive capital and operating costs no longer present the barrier they once did. Technology has brought about major change in operational efficiency. The invention of the internet has provided new opportunities and increased exposure to new markets, yet at the same time, threats to security and privacy have increased at a frightening rate. The following list highlights nine evolutions of corporate computing, with a brief explanation on each:

- Distributed Systems
- Business Process Management
- Service Oriented Architecture
- Grid Computing
- Utility Computing
- Virtualization
- Corporate Outsourcing
- Cloud Computing
- Economics of Cloud Computing

Distributed systems can be described as a software system in which components located on networked computers communicate and coordinate their actions by passing messages, in order to achieve a common goal. Early interest from military

 ISBN: 978-1-61208-460-2

and defence agencies has contributed greatly to the benefits to industry [12]. Early research effort from industry [13] [14] has also been evident. This is still an active research area today, with Lenk and Tai [15] addressing disaster recovery, Orgerie et al. [16] seeking to reduce energy costs of distributed systems, and Gottinger [17] who addresses the management issues of improving economic mechanism design of distributed systems.

Business process management (BPM) is a subset of operations management, which focuses on improving corporate performance by managing and optimising a company's business processes. Information technology (IT) can play an important role in helping with this continual process of improvement, in which three basic elements are involved — people, process and technology. This interaction between the three elements perfectly describes the business architecture of a company. Instead of adapting business processes to fit rigid and intractable software, software could now be developed to align with business practices. This allowed a better fit to the way a firm did business, ensuring greater efficiencies. A rich area of research for over three decades, from the early work of Zachman [18], Norman et al. [19] through to later work by Zhu et al. [20] and Herzberg et al. [21], it has attracted great interest from a wide range of disciplines. The opportunities offered by the development of business process architecture would lead to issues in trying to communicate with different computing systems. This lead to the development of the term "Service Oriented Architecture (SOA)" [22]. SOA was defined as *"a software architecture that starts with an interface definition and builds the entire application topology as a topology of interfaces, interface implementations and interface calls"*. SOA didn't get much traction until 2001 when web services technology became widely adopted. In many respects, web services gave SOA the foundation it needed to become widely accepted. Again a healthy research area, still very much active today, with Girbea et al. [23] addressing optimisation of industrial manufacturing processes and Picard et al. [24] presenting several alternative systems for enhancing collaboration at inter-organisational level.

Grid computing is a varied collection of computer resources spread over multiple locations designed to achieve a common goal. Grid computing differs from conventional high performance computing systems such as cluster computing. Grid computers have each node loosely coupled and highly distributed over a wide geographical area, whereas high performance cluster computing generally has all the nodes physically connected in the one location. Grid computers tend to be highly heterogeneous, whereas a cluster will usually comprise a set of identical hardware. Grid computing nodes can be owned by a diverse range of organisations who share access to these resources, whereas a cluster tends to be owned by a single organisation. Grid computing started to gain traction in the mid to late 1990s. Utility computing is a service provisioning model in which a service provider makes computing resources and infrastructure management available to the customer as needed, and charges them for specific usage rather than a flat rate. This model differs from grid computing as the service provision comes from a single service provider, rather than from a network of service providers. The model is not new, evolving during the 1960s and 1970s. To facilitate this business model, mainframe operating systems evolved to include process control facilities, security, and user metering. The model re-surfaced in the late 1990s with a number of large players offering their own flavour. The development of virtualisation software helped move the model towards cloud computing.

Virtualisation is the creation of a virtual (rather than actual) version of something, such as an operating system, a server, a storage device or network resources. It began in 1960s mainframe computers as a means of logically dividing system resources provided by mainframes between different applications, although its meaning has considerably broadened in scope since then. Virtualisation allows spare capacity in large server systems to be partitioned into self standing virtual servers, which can provide "Chinese walls" between instances to improve security where different customers use each of the virtual instances. By 2003, the process of virtualisation had become much more developed, yet few had offered resource isolation or performance guarantees; most provided only best-effort provisioning, risking denial of service. Large corporates have traditionally had a high focus on efficiency and maximising profits. Consequently, they have long explored the potential for cost savings to be had from outsourcing non core activities. Indeed, they have also used extended outsourcing techniques such as off-shoring which allow them to potentially reap far greater cost savings than with normal outsourcing methods. In the early days of mainframe computing, with no internet to worry about, security was much less of an issue. However, this would radically change with the arrival of the internet.

Cloud computing offers the possibility of a substantial economic benefit to firms, yet at the same time, increases complexity and risk further. This results in an interesting dilemma. On the one hand, potential cost savings of 50 - 90% [1] are possible, which is highly attractive, but on the other hand, complexity can increase exponentially, placing significant increasing risk on business and government alike.

It will be useful to understand how the economics of cloud computing has helped it to achieve such rapid market penetration and deployment. While the incentives to use cloud are very attractive, it brings with it other issues, such as accountability, assurance, audit, availability, confidentiality, compliance, integrity, privacy, responsibility and security, all of which need to be properly addressed. Cloud computing is the most agile of these systems, yet the most technically challenging to secure, due to the multiplicity of relationships within the cloud ecosystem.

IV. How is Audit Currently Performed?

We provide a brief outline here of how the approach to financial audit evolved over the past century. Then, vouching was the common mechanism utilised to conduct an audit. Here, the auditor checked every single transaction in the company books to vouch its authenticity. This was extremely cumbersome, and expensive, to conduct, and in ignoring management control systems, proved to be very inefficient. As companies grew larger, this technique could no longer be supported.

A move to statistical sampling of transactions, together with consideration of the effectiveness of internal controls, allowed for a more efficient approach to the audit of larger companies. Sometimes, fraud audit would also be carried out to detect the possibility of fraud having occurred, whether from external or internal sources. The use of checklists became popular. Eventually companies started to use IT for their financial systems. At first, the IT systems were treated as black

 ISBN: 978-1-61208-460-2

box systems, where auditors merely considered how the input was transformed into the expected output. Ultimately, this led to the need to check the integrity of the systems themselves and these too, were audited, creating a need for auditors to broaden the scope of their learning. Over time, there was a move towards a more risk based approach, with a greater emphasis on performing due diligence, and less emphasis on the use of the checklist. Discussing financial audit in more detail is impossible within the constraints of this paper, but provides a brief outline of how things have changed.

IT audit is not the same as financial audit. Financial audit's purpose is to evaluate whether an organisation is adhering to standard accounting practices, and to ensure the financial statements present a true and fair view of the information contained in the financial reports. The purpose of an IT audit is to evaluate the system's internal control design and effectiveness, through studying and evaluating controls and testing their effectiveness. IT audit can be carried out by the company's internal audit department, an external agency, or by the company's own auditors. IT auditors are not regulated to the same extent as financial auditors. Many of the large auditing firms have set up specialised departments to handle IT audits, with the benefit that they have access to the financial audit expertise of the firm. Many IT audit firms do not have financial audit experience. In general, there is a greater move towards a checklist based approach in performing IT audits, as with compliance audit, including security standards audit, which traditionally use the checklist approach.

Joint venture audit is conducted in accordance with the terms of the joint venture agreement, often by the internal audit department of the partners, although some will use their external auditors for this. Internal audit is sometimes performed by employees with limited experience of how external financial audit is conducted, resulting in a less risk based approach. This can be useful in that their work can better inform the external auditors when they arrive to carry out their audit. Forensic audit will usually be carried out in response to the discovery of a systems breach, usually by forensic IT specialists.

V. Are there any weaknesses in this approach?

We address some of the cloud security standards issues in Section VI. The frequency of compliance auditing is generally quite relaxed, in that reassessment need take place only when system changes take place, or every few years, otherwise. This completely fails to grasp the rapidly evolving nature of security threats. There exists a clear need to employ some method of continuous monitoring when it comes to security management. Reports from global security companies, which do not differentiate between cloud and non-cloud using companies [25]–[27], suggest that over 85% of security breaches involve a low level of technical competence, facilitated instead by lack of understanding, lack of competence, or poor configuration of systems on the part of victims. It would be very useful to the research community if security breach reporting companies were to publish cloud specific data. While CSPs are very reluctant to publicise security breaches, last year's cloud breaches on iCloud, Target, Home Depot, Sony and the US Internal Revenue Service (IRS) may have more to do with slack security culture and poor internal control processes than cloud security weaknesses. Nonetheless, this clearly illustrates the importance of the link between people, process and technology.

Vouk [28] suggests a key element of SOA is an ability to audit processes, data and results, i.e. the ability to collect and use provenance information. Since SOA is not always included in what is run on the cloud, there is a possibility that this may present a weakness if steps are not taken to address this shortcoming. Both Leavitt [29] and Wang et al. [30] suggest the use of third party auditors, yet many CSPs to this day are reluctant to offer this service. Armbrust et al. [33] suggest lack of cloud audit-ability presents the number three barrier to cloud take-up, and that more needs to be done to ensure compliance with new legislation such as Sarbanes-Oxley Act (SOX) and the Health and Human Services Health Insurance Portability and Accountability Act (HIPAA) regulations.

Chen and Yoon [31] suggest that an exceptionally robust approach to cloud audit is required in order to ensure compliance with all necessary legislation, regulation and standards. Ramgovind et al. [32] suggest the question of whether the CSP is willing to undergo audit represents a key security issue for cloud use. Wang et al. [34] propose a publicly audited cloud environment to ensure proper privacy is maintained. Zhou et al. [35] in conducting a survey of CSPs and SLAs suggest availability, audit, confidentiality, control, and data integrity should be added to standard SLAs.

Grobauer et al. [36] suggest that without proper audit provisions in SLAs, security and privacy will be compromised. Doelitzscher et al. [37] propose a technical solution to this issue using Security Audit as a Service (SAaaS) in conjunction with software agents and a neural network to detect anomalies and misuse of systems. Early results are promising, although the system has yet to run live. Ruebsamen and Reich [38] propose the use of audit agents to patrol a cloud environment to ensure proper accountability. Lopez et al. [39] propose the use of Somewhat Homomorphic Encryption (SHE) and Public-Key Searchable Encryption (PEKS) in conjunction with audit agents to ensure proper accountability in the cloud.

The approaches to financial audit and IT audit are well understood, subject to our earlier comments, and are generally perceived as fit for purpose. But, when using cloud computing, everything changes. Instead of working on systems under the control of the company being audited, these systems belong to others, such as the CSP and any one of a number of other actors involved in the cloud ecosystem. In previous work [2] on enhancing cloud security and privacy, we drew attention to the shortcomings in the standard SLA offerings of many CSPs. Most lack any serious level of accountability, assurance, audit, confidentiality, compliance, integrity, privacy, responsibility or security, merely concentrating on availability as the only measure of performance provided. Many are reluctant to allow third party auditors into their premises, making effective audit difficult, if not impossible.

One of the fundamental benefits of cloud computing, agility, presents auditors with a very difficult challenge. Maintaining an effective audit trail presents a serious challenge when cloud instances are spooled up or down, sometimes by the thousand, as needed. We address this specific issue in [40].

VI. Cloud Security Standards Compliance Issues

Cloud security standards compliance presents a number of interesting issues. First, in today's global economy, an effective

 ISBN: 978-1-61208-460-2

standard needs to be internationally accepted, which introduces jurisdictional problems to the mix, coupled with the fact that the pace of evolution of new technology far outstrips the capability of international standards organisations to keep up with the changes [41]. Second, standards compliance is not mandatory, but merely a voluntary practice. While many large organizations are keen to be compliant in order to provide assurance to their clients, there is no legal obligation to do so. Third, compliance with standards is also generally not required by regulators, although there are signs that this attitude may be changing. Fourth, compliance procedures will usually allow a degree of latitude to the compliant company in respect of the level of compliance they wish to achieve. Fifth, the audit mechanisms used by compliance auditors can be flawed [42]. Sixth, compliance auditors are not heavily regulated, as they are for financial audit. Seventh, there are a great many cloud security standards organisations in existence, often with differing agendas, or merely concerning themselves with an area of narrow focus. Eighth, no complete cloud security standard yet exists. Nine, very few early standards took a risk based approach, relying instead on the checklist approach to compliance. Ten, knowing that a prospective company is compliant is not enough. It is necessary to understand exactly what level of compliance has been achieved, and this detailed level of information is seldom disclosed.

Will compliance with a standard ensure security? In [5] we argued that compliance with a cloud security standard is more likely to ensure compliance with a security standard, rather than achieve a meaningful level of security. We take a brief look at some of the larger standards organisations.

The International Standards Organization (ISO) have done excellent work on global standards, yet the benefit of this approach is also a weakness. Seeking agreement across the globe, prevents them from keeping standards fully up to date, taking up to eight years to publish a fully agreed new standard. It has taken some time, but it is encouraging that the ISO has changed approach on ISO 27000 series standards to a risk based approach, which started to filter through in 2014, and this is very welcome. A few cloud standards are also starting to filter through, but a full range of cloud standards is still some way off. It is also encouraging to note that as new standards are published, they are adopting a risk based approach.

The National Institute of Standards and Technology (NIST), who produced one of the earliest clear definitions of what cloud computing is, have long been of the view that a risk based approach to cloud security would be more effective. The US government finally accepted last year that this was a sensible approach [43], and NIST have developed an excellent risk based security standard. NIST produce excellent work, but compliance with NIST standards often only extends to US companies and those doing business with the US.

The Cloud Security Alliance (CSA) have been very active in promoting cloud security standards. Their work is good, but the weakness lies in the approach used for the method of achieving compliance.

AICPA have produced a number of standards, including for cloud. Their SOC2 standard for cloud has seen many CSPs attain compliance, including across the globe. However, this does not cover the case where the cloud service will potentially affect the statement of financial information, for which a SOC 1 will be required. Where assurance on trust is required, a SOC 3 report should be sought. While these standards apply the same criteria for both cloud and non-cloud situations, it would be naïve to believe that non-cloud security measures would be suitable for a cloud deployment.

Considerable work has been done on addressing legal issues with cloud deployment [44] [45] [46] [47] [48]. With the global reach of both cloud users and CSPs, this will help to tackle outstanding issues of sovereignty and jurisdiction.

VII. How do we tackle these weaknesses?

There needs to be a proper understanding of precisely why a cloud audit is being performed. Different types of audit require different approaches and it is important not to forget the fundamental rationale for an audit. No matter what type of audit is being carried out for whatever purpose, the auditor needs to keep the fundamental requirements of the audit firmly in mind throughout the audit.

The cloud security standards issue is a particularly difficult challenge. We address this challenge in future work and make some helpful suggestions here to address this problem.

The CSP problem with the standard SLA needs to be addressed as an area of added risk. It is important to realise just what this additional risk will mean to the company under review. While it can be said that the standard SLA can offer a better level of security than is available to the average small to medium sized enterprise (SME) [49], it cannot be considered foolproof. Companies, and their auditors, should recognise the weaknesses inherent in the standard SLA and address these specifically as an added risk to the company. We hope that, in time, the changes we seek in [2] will come to pass.

The audit trail issue requires companies and their auditors to recognise that the problem exists. In [40], we address this issue and make some useful suggestions on how to tackle these weaknesses.

VIII. Conclusion

Even centuries of experience of financial audit have not solved all the problems of conflict of interest, or the clear understanding and interpretation of the role of audit, hence the need to consider some of the more fundamental issues facing companies today. We must bear in mind that information is now as valuable to companies as money, and deserves serious thought and action to safeguard it.

We have looked at some of the challenges facing companies who seek to obtain good cloud security assurance through audit. We have seen how weaknesses in standard CSP SLAs can impact on cloud security. We have identified issues with cloud security standards, and how that might impact on cloud security. Achieving compliance with cloud security standards is a worthwhile goal, but success will only guarantee compliance with the standard, not necessarily a useful level of security. We have considered how the lack of accountability can impact on security. We have also considered how misconceptions in the purpose and scope of audit can also impact on security.

We have touched on how these difficult areas of security might be approached as part of a comprehensive security solution based on our proposed framework. Clearly, companies could benefit from further research in several of these areas. In particular, cloud audit could benefit from applying the rigour

 ISBN: 978-1-61208-460-2

used by auditors in the accounting world when carrying out statutory audit. However, we would caution that action is needed now, not several years down the line when research reaches a more complete level of success in these areas. The threat environment is too dangerous. Companies have to act now to try to close the door, otherwise it may be too late.

REFERENCES

[1] P. Mell and T. Grance, "Effectively and Securely Using the Cloud Computing Paradigm," Tech. Rep., 2009.

[2] B. Duncan and M. Whittington, "Enhancing Cloud Security and Privacy: Broadening the Service Level Agreement," in Trustcom/BigDataSE/ISPA, 2015 IEEE. Vol. 1. IEEE, 2015, pp. 1–6.

[3] OED, "Oxford English Dictionary," 1989. [Online]. Available: www.oed.com [Retrieved: Feb 2016].

[4] M. Armbrust et al., "A view of cloud computing,"Commun. ACM, vol. 53, no. 4, 2010, pp. 50–58.

[5] B. Duncan and M. Whittington, "Compliance with Standards, Assurance and Audit: Does this Equal Security?" in Proc. 7th Int. Conf. Secur. Inf. Networks. Glasgow: ACM, 2014, pp. 77–84.

[6] H. S. Herath and T. C. Herath, "IT security auditing: A performance evaluation decision model," Dec. Supp. Sys., vol. 57, 2014, pp. 54–63.

[7] R. K. L. Ko, P. Jagadpramana, and B. S. Lee, "Flogger: A File-Centric Logger for Monitoring File Access and Transfers Within Cloud Computing Environments," Proc. 10th IEEE Int. Conf. Trst. Sec. Priv. Comp. Com. Trst., 8th IEEE Int. Conf. Emb. Soft. Sys. ICESS, 6th Int. Conf. FCST 2011, pp. 765–771.

[8] R. K. L. Ko, B. S. Lee, and S. Pearson, "Towards achieving accountability, auditability and trust in cloud computing," Commun. Comput. Inf. Sci., vol. 193 CCIS, no. Part 4, 2011, pp. 432–444.

[9] S. Pearson, "Taking Account of Privacy when Designing Cloud Computing Services 2 . Why is it important to take privacy into," Chall. Cloud Comp., 2009, pp. 44–52.

[10] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," 2010 IEEE Second Int. Conf. Cloud Comput. Technol. Sci., 2010, pp. 693–702.

[11] B. Duncan, D. J. Pym, and M. Whittington, "Developing a Conceptual Framework for Cloud Security Assurance," in Cloud Comput. Technol. Sci. (CloudCom), 5th Int. Conf. (Vol. 2). IEEE, 2013, pp. 120–125.

[12] J. Parker et al., "Detection of Mutual Inconsistency in Distributed Systems," in IEEE Tra. Soft. Eng., vol. SE-9, no. 3, 1983, pp. 240–248.

[13] J. Kramer and J. Magee, "Dynamic Configuration for Distributed Systems," IEEE Trans. Softw. Eng., vol. SE-11, no. 4, 1985, pp. 424–436.

[14] F. Mattern, "Virtual Time and Global States of Distributed Systems," Event London, vol. pages, no. 23, 1989, pp. 215–226.

[15] A. Lenk and S. Tai, "Cloud Standby: Disaster Recovery of Distributed Systems in the Cloud," Serv. Cloud Comput., 2014, pp. 32–46.

[16] A.-C. Orgerie, M. Dias de Assuncao, and L. Lefevre, "A Survey on Techniques for Improving the Energy Efficiency of Large Scale Distributed Systems," ACM Comput. Surv., vol. 46, no. 4-47, 2013, pp. 1–35.

[17] H. W. Gottinger, "Internet Economics of Distributed Systems," in Soc. Sci. Educ., vol. 2, no. 6, 2015, pp. 55–70.

[18] J. A. Zachman, "A Framework for Information Systems Architecture," IBM Syst. J., vol. 26, no. 3, 1987, pp. 454–470.

[19] T. J. Norman, N. R. Jennings, P. Faratin, and E. H. Mamdani, "Designing and Implementing a Multi-Agent Architecture for Business Process Management," in PreProceedings ECAI96 Work. Agent Theor. Archit. Lang. ATAL96, N. R. Müller, Jörg P and Wooldridge, Michael J and Jennings, Ed., vol. 1193. New York: Springer, 1997, pp. 261–275.

[20] W. Zhu, L. Vizenor, and A. Srinivasan, "Towards a Reference Architecture for Service-Oriented Cross Domain Security Infrastructures," Internet Distrib. Comput. Syst., 2014, pp. 275–284.

[21] S. Bülow, M. Backmann, and N. Herzberg, "Monitoring of Business Processes with Complex Event Processing," Bus. Process Manag. Work., 2014, pp. 277–290.

[22] W. R. Schulte and Y. V. Natis, "Service Oriented Architectures, Part 1," Gartner, SSA Res. Note SPA-401-068, 1996.

[23] A. Girbea, C. Suciu, S. Nechifor, and F. Sisak, "Design and Implementation of a Service-Oriented Architecture for the Optimization of Industrial Applications," IEEE Trans. Ind. Informatics, vol. 10, no. 1, 2014, pp. 185–196.

[24] W. Picard, Z. Paszkiewicz, S. Strykowski, R. Wojciechowski, and W. Cellary, "Application of the service-oriented architecture at the inter-organizational level," Stud. Comput. Intell., vol. 499, 2014, pp. 125–201.

[25] PWC, "UK Information Security Breaches Survey - Technical Report 2012," PWC2012, Tech. Rep. April, 2012.

[26] Trend, "2012 Annual Security Roundup: Evolved Threats in a 'Post-PC' World," Trend Micro, Tech. Rep., 2012.

[27] Verizon, "2013 Data Breach Investigation Report: A study conducted by the Verizon business risk team." Tech. Rep., 2013.

[28] M. Vouk, "Cloud computing - Issues, research and implementations," ITI 2008 - 30th Int. Conf. Inf. Technol. Interfaces, vol. 16, no. 4, 2008, pp. 235–246.

[29] N. Leavitt, "Is Cloud Computing Really Ready for Prime Time?" Computer (Long. Beach. Calif)., vol. 42, no. January, 2009, pp. 15–20.

[30] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," in IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5, 2011, pp. 847–859.

[31] Z. Chen and J. Yoon, "IT Auditing to Assure a Secure Cloud Computing," in 2010 6th World Congr. Serv., 2010, pp. 253–259.

[32] S. Ramgovind, M. M. Eloff, and E. Smith, "The management

[33] M. Armbrust et al., "A view of cloud computing,"Commun. ACM, vol. 53, no. 4, 2010, pp. 50–58.of security in cloud computing," in Proc. 2010 Inf. Secur. South Africa Conf. ISSA 2010, 2010, pp. 1–7.

[34] C. Wang, S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage in Cloud Computing," in IEEE Trans. Comput., vol. PP, no. 99, 2012, pp. 1–14.

[35] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and Privacy in Cloud Computing: A Survey," in 2010 Sixth Int. Conf. Semant. Knowl. Grids, 2010, pp. 105–112.

[36] B. Grobauer, T. Walloschek, and E. Stöcker, "Understanding cloud computing vulnerabilities," IEEE Secur. Priv., vol. 9, no. 2, 2011, pp. 50–57.

[37] F. Doelitzscher, M. Knahl, C. Reich, and N. Clarke, "Anomaly Detection In IaaS Clouds," in CloudCom, 2013, pp. 387–394.

[38] T. Ruebsamen and C. Reich, "Supporting cloud accountability by collecting evidence using audit agents," in Proc. Int. Conf. Cloud Comput. Technol. Sci. CloudCom, vol. 1, 2013, pp. 185–190.

[39] J. M. López, T. Ruebsamen, and D. Westhoff, "Privacy-Friendly Cloud Audits with Somewhat Homomorphic and Searchable Encryption," in Innov. Com. Serv. (I4CS), 14th Int. Conf., 2014, pp. 95–103.

[40] B. Duncan and M. Whittington, "Enhancing Cloud Security and Privacy: The Power and the Weakness of the Audit Trail," in press.

[41] G. T. Willingmyre, "Standards at the Crossroads," StandardView, vol. 5, no. 4, 1997, pp. 190–194.

[42] B. Duncan and M. Whittington, "Reflecting on Whether Checklists Can Tick the Box for Cloud Security." in Cloud Comp. Tech. Sci. (CloudCom), IEEE 6th Int. Conf. Singapore: IEEE, 2014, pp. 805–810.

[43] R. Holland et al., "Quick Take : 12 Lessons For Security & Risk Pros From The US OPM Breach," 2015, pp. 1–10.

[44] C. Millard, K. Hon, and I. Walden, "The Problem of ' Personal Data ' in Cloud Computing - What Information is Regulated ?" 2011.

[45] W. K. Hon, C. Millard, and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2,"Leg. Stud., no. 77, 2011, pp. 1–31.

[46] W. K. Hon, J. Hörnle, and C. Millard, "Data Protection Jurisdiction and Cloud Computing When are Cloud Users and Providers Subject to EU Data Protection Law?" Leg. Stud., 2011, pp. 1–40.

[47] J. Prüfer, "How to govern the cloud? Characterizing the optimal enforcement institution that supports accountability in cloud computing," Proc. Int. Conf. Cloud Comp. Tech. Sci., vol. 2, pp. 33–38, 2013.

[48] J. Prufer, "Trusting Privacy in the Cloud," 2014.

[49] M. Quinn, E. Strauss, and G. Kristandl, "The effects of cloud technology on management accounting and business decision-making," Fin. Man., vol. 10, 2014, pp. 54–55.

 ISBN: 978-1-61208-460-2