Application of a Secure Cloud Based Learning Environment for Inclusive Practice in Mainstream Education: A Higher Education Case Study

Nigel Beacham
Computing Science
University of Aberdeen, UK
Email: n.beacham@abdn.ac.uk

Bob Duncan
Business School
University of Aberdeen, UK
Email: robert.duncan@abdn.ac.uk

***Abstract*—In previous literature, an inclusive practice approach to counteract possible areas of concern regarding cloud-based security for virtual learning environments has been proposed. In this paper, the theoretical framework 'transformability theory' underpinning such a proposal is applied in the context of higher education. Practicalities and limitations applying to such an idealised approach in a real context are explored in the form of a case study. The case study includes both the multiple and mixed roles that learning analytics and usability play in cloud-based security. Whilst such roles provided by technology still rely on the need for a social and technical system approach based on a pedagogical focus aligned with educational beliefs, attitudes and practices, observations from the case study show that risks and threats can be managed on a perception and actual occurrence basis. Such encouraging findings from this pilot study support the need for a larger more substantial investigation into the theoretical approach. The proposal for this case study is very timely, due to the concerns surrounding both the cloud forensic problem and the potential impact of the provisions of the forthcoming EU General Data Protection Regulation. The case study will outline a workable approach to achieve high levels of both security and privacy, such that compliance with the new regulation can be achieved.**

Keywords–Inclusive education; security; privacy; cloud based systems; virtual learning environments; transformability theory.

I. Introduction

From a practical perspective, cloud presents an ideal basis for developing educational systems. It can be rapidly deployed, is eminently scalable, requires no massive capital outlay, and has no long lead time for delivery. Of course, no solution is ever completely perfect. The educational system will be running on someone else's hardware, and often software too. This means there will be additional concerns that will be necessary to contend with, such as security, privacy and accountability.

Of course, while it is sensible to deal with such issues, there is also the added concern and impact from legislation and regulation that will also have an impact. This means these issues must be dealt with rigorously. Legislation, such as the Data Protection Act [1], have substantial penalties that can be levied in the event of non-compliance. However, such penalties will pale into insignificance compared to the forthcoming EU General Data Protection Regulation (GDPR) [2], which comes into effect on 25th May 2018.

In the case of the GDPR, the maximum penalty, in the event of a significant breach where non-compliance of the responsible organisation is a contributory factor, can be the greater of €20 million or 4% of global turnover based on the previous year's accounts. This represents a serious amount of money, and in an area where budgets are already a big enough challenge, this would have a significant adverse impact on learning.

Human and social factors are important to consider when designing cloud-based security within education systems. As a consequence, there is a real lack of literature that has studied these factors and interventions from the perspective of inclusive social/technical systems. The realisation by others has led to an increased interest in researching systems to improve cyber-security [3]. One dilemma is the lack of theoretical rigour underpinning what amounts to a technological solution. Studies that have been conducted, whilst encouraging, nevertheless focus on the human factors of security systems [4] [5]. Such studies focus on the behavioural aspects using an experimental and empirical approach based upon behavioural psychology theories. Whilst these highlight strategies and provide insights into some of the key factors contributing towards the challenges of security, it remains to be seen whether in practice such strategies amount to real behavioural change and ultimately reduce security threats and risks in educational organisations.

In Section II, we discuss previous work in this area. In Section III, we next consider the security and privacy weaknesses in cloud systems, in order to understand the magnitude of the problem. In Section IV, we outline how we might approach we might take to attempt to find a way to try to resolve this problem. In Section V, we consider the technical strategies that ought to be deployed. In Section VI, we outline the manner in which the case study will be deployed. In Section VII, we consider and discuss the limitations of the work, and in Section VIII, we discuss our conclusions.

II. Previous Work

From an inclusive education perspective, much research exists on strategic and technological approaches to enhancing inclusion [7]–[9], but little if any account for the cybersecurity threats and risks. Some of the most interesting work has been undertaken by Young, which focuses on inclusive spaces. Young [10] explores how organisational spaces impact on the effectiveness of education strategies and practices. Whilst having a safe place to retreat to is an important factor, the

research does not address security aspects and in particularly cybersecurity.

The same can be said from the perspective of adopting inclusive strategies and practices through ICT. There is a growing body of research studying education inclusion using Information and Commuications Technology (ICT), which show encouraging results [11]–[14]. Whilst many of the studies tend to focus on the benefits, there is also evidence that ICT can inhibit inclusive education; albeit not from the perspective of using cybersecurity technologies [15]. This highlights the issue that little if any research considers the cybersecurity aspects in terms of whether inclusive strategies reduce the risks and threats of cybersecurity or whether cybersecurity technologies can enhance or inhibit inclusion?

Based upon Beacham and Duncan's [3] theoretical framework for considering inclusive cloudbased security for education, and possible ways in which such a framework may manifest its self in the context of an inclusive learning environment, the following sections of this paper explores in more detail how such theory and inclusive pedagogies can be used in practice through pedagogical strategies to bring about real change and improvement in reducing risks and threats of cybersecurity.

Such insights will form the basis of a case study undertaken within Higher Education (HE). This case study will seek to highlight the difficulties in developing an experiment to measure the change in behaviour being encouraged. This case study will pilot the framework and obtain experimental and empirical evidence highlighting the benefits and challenges using such a framework in an authentic context. Lessons from the case study will be used to inform further investigations within real-world contexts.

III. Security and Privacy Weaknesses in Cloud Systems

All systems are the subject of serious penetration attempts by attackers. While resisting such attacks presents a huge challenge, where cloud is involved, the challenge is even greater. The attackers make no distinction between what kind of organisation, or individual they are attacking. They seek to get into the system, then dig themselves in, hiding themselves away to become a hidden intruder, with the goal of finding as much useful information as they can to extract for their own nefarious purposes.

This presents a serious challenge to defend an organisation properly from attack [16]–[19], but in the case of cloud, we also suffer from a fundamental, as yet unsolved, problem known as the cloud forensic problem. Once an attacker breaches a cloud system and becomes an intruder, there is nothing to then prevent them from escalating privileges until they are in a position to delete the forensic trail recording their ingress into the system, thus potentially turning them into an invisible intruder.

Once the intruder reaches this stage, they present a serious threat, since they are now in a position to help themselves to anything they want from the cloud system, and can also use this position as a springboard to attack other systems elsewhere within the organisation. They would also be in a position to completely shut down the running cloud instance, which would delete all data that had not been made persistent elsewhere. This could pose a serious challenge in trying to identify which information has been compromised, or stolen.

As if that were not bad enough, the forthcoming EU regulation, the GDPR [2], comes into effect on 25th May 2018. There is a requirement to report any breach within 72 hours of discovery. However, where forensic records have been destroyed, it may prove impossible to comply fully with this requirement. This would potentially expose the organisation to a fine, which in the worst case, could be the greater of €20million or 4% of global turnover, based on the previous year's accounts.

Duncan and Whittington [20] recently proposed a possible solution to this problem through the use of generating a full forensic and audit trail to be stored off site in an immutable database. We like this approach for its simplicity of application, there being nothing overly technical involved. Sadly, this will not be the only problem to contend with.

While there are a great many technical solutions, which have been developed to address technical issues [21]–[25], there are also other issues that need to be addressed. Many organisations forget that business architecture comprises a combination of people, process and technology, and not technology alone [26]. Thus, organisations who rely on technological solutions alone will be likely to fail to achieve a satisfactory level of security and privacy.

The weakest link of any organisation is usually the people involved in the organisation. Attackers have long recognised that people are very susceptible to attack via a wide range of social engineering attacks, malicious links in emails, spoof web sites, and a whole range of other attacks designed to target the weaknesses of the people of the organisation, rather than directly attacking the Information Technology (IT) systems of the organisation.

IV. The Approach

Whilst some general ways of enhancing the social and technical approaches to security and inclusion have been independently reported [3], this section highlights inclusive pedagogies and practices that can be used in computer science education. We selected computer science education because not only are students susceptible to the security threats and risk as students in general, but that these cohorts of students need to have knowledge and understanding about cyber-security if they are to engineer secure application systems in future.

Creating an authentic testbed in which to pilot such an investigation of this type is not without its difficulties. In the framework outlined by Beacham and Duncan [3], such systems would entail developing a socio technical system around an inclusive learning community involving pupils, teachers, parents, technicians, school management and administration, and staff within the local authority, to name but a few. Developing a socio-technical system for use within a real mainstream educational organisation such as a school or local authority would be fraught with educational and technical challenges; not to mention ethical and political issues.

For this reason, a smaller and more manageable system will be constructed, safe within the confines of a Higher Education Institution (HIE). The pilot system seeks to build a similar inclusive learning community but with a more manageable number of stakeholders. The inclusive learning community provides a framework in which to encourage inclusive strategies such as co-agency, everybody and trust,

TABLE I. DARE'S STRATEGIES [7]

Strategy to:	Co-agency	Everyone	Trust
Invite students to join different groups. Meeting the minds of learners to lift the limits posed by a security system.		X	X
Get to know each other. Find ways to connect with each other building on their strengths as opposed to differentiating tasks.		X	X
Avoid singling students out. Plan tasks to be open to all in learning community.		X	X
Help students with studying and finding solutions. Seek ways for tutors to learning from learners and building valued partnerships.	X	X	
Group sub-groups of students together or with buddies. Develop a community culture, which "not just facilitates access and engagement (to learning tasks) but to reinforce young peoples' active sense of their powers and competence as thinkers and learners that what they have to bring and contribute to their own learning is important, valued and welcome."		X	X
Use a problem based learning approach by dividing community into small and meaningful groups.		X	X
Insist on learners taking shared responsibility for **learning activities** and allow learners to make rules and decisions.	X	X	
Tutors focus is to "transform the context, the curriculum, and the conditions that sustain learning." In partnership with learners.	X	X	
Adopt security mechanisms that are accessible, afford well-being and achievement for all based on unity and solidarity learning.		X	X

but is formed and managed within the confines of a cohort studying within an HEI. This provides a more appropriate context and environment in which to undertake an initial pilot to empirically study the effectiveness of such a system.

A. Inclusive strategies

Before undertaking the pilot, it was important to ascertain what strategies increase inclusion within learning communities [6]. These strategies were then applied in the context of the case study with the intention of collecting evidence, which showed an inclusive learning community can reduce security threats and risks.

The strategies considered relate to the three principles of transformability theory. They consist of:

- Co-agency strategies that encourage tutors and students to work together and view each other as equal partners in the teaching and learning process;
- Everybody strategies that promote collaboration with stakeholders, such as parents, Local Authorities and education agencies;
- Trust strategies that seek to develop effective scaffolding for tutors and learners.

As shown in TABLE I, such principles were implemented by using the inclusive strategies listed in the table.

Such overlapping strategies underpin criteria, which will be used to evaluate the effectiveness of the intervention covered in the case study.

In the next section, we discuss the technical strategies that should be deployed in the framework.

V. Technical Strategies

In order to construct a realistic learning environment, a closed prototype has been developed containing the following features:

- Authentication, by using access control, passwords or multi factor authentication;
- Monitoring/logging/reporting can be carried out in real-time, providing a transparent system;
- Auditing will be carried out using an independent, read-only closed system;
- Privacy will be achieved through a combination of actions/activity based focus and encryption.

In Figure 1, we outline how the various components of the system will fit together. We consider how each type of strategy addresses threats and risks outlined in the theoretical framework, mapping strategies to practice — this is the focus of the pilot study.

Thus, we require to include a simple mechanism whereby we collect ALL the forensic data and audit trail data that we are likely to need, in addition to what the cloud system can already collect, and store this into an "append-only" database. This immutable database must be stored off-site from the cloud instance in order to make it more difficult for the attacker to understand what is going on.

This immutable database must run on a server with no other function, other than to solely concentrate on the retention of the forensic data and the audit trail for the cloud instances it is designed to protect. We must remember that it will be necessary to actively provide a means of collecting both the forensic data and the full range of audit trail data we require, since as Duncan and Whittington note, many of these functions are switched off by default from a great many database systems [27] [20].

This data collection should include additional material to identify the specific cloud instance identifying number (ID), a timestamp to indicate generation time of the data collected, and if we want to take a paranoid approach, we could also serialise the data collected ID using a centrally generated number, which would assist in post hack event analysis. Indeed, the central ID generator could be monitored to seek out anomalous numbering sequences from which alerts could be generated to instantly warn of a developing situation.

This solution will provide us with the one fundamental means of being able to answer the big GDPR question in the event of a breach — namely we can identify which information, if any, that was compromised in the breach. While it is not a regulatory requirement, encryption of Personally Identifiable Information (PII) [2] will go a long way to help mitigate any liability in the event of a breach.

In the next section, we outline the rationale and methodology for the pilot case study.

VI. The Pilot Case Study

The socio component of the system involves the forming of a learning community. The community consists of students and

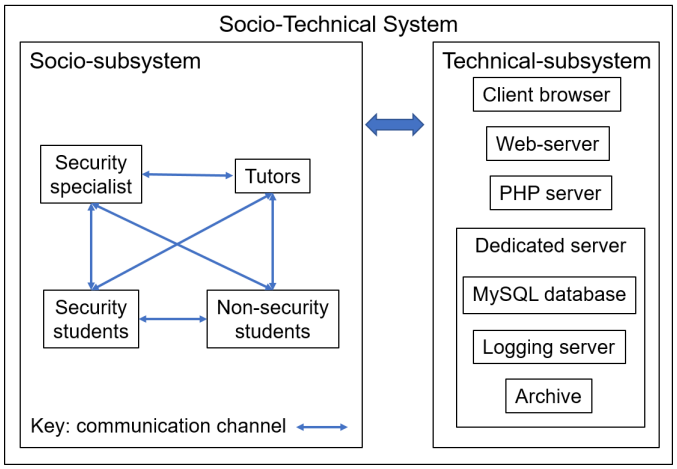

Figure 1. Socio-technical system approach to an inclusive cloud-based security learning environment.

tutors co-working together on achieving learning outcomes of a course studying Human Computer Interaction (HCI). Whilst the course covers conventional topics, it also includes the additional topic of usable security.

The students consist of two campus-based cohorts studying for a Master of Science (MSc) in Information Technology degree programme. One group of students form part of a September intake and have studied cyber-security in the previous term. The second group of students form part of a January intake beginning their programme.

Both cohorts of students are taught together on the HCI course. The course involves two one-hour lectures and one two-hour practical session. The lectures include materials that help students enhance their knowledge about usability with the aim of them understanding its relevance to usable security. In the practical sessions, they work in teams to complete tasks targeted at applying such knowledge and understanding. Students are also provided with additional materials and encouraged to undertake further reading and study around the usability aspects of security.

Although some of the students will have studied aspects of cyber-security, more broadly, students are not expected to know or understand the technicalities of cyber-security. For example, they do not need to know how to develop systems which require users to have a username and password, only that such process places usability constraints to use an application, such as having to recall authentication details.

The students are expected to use their knowledge and understanding to outline the types of data gathering approaches they would use as part of an Interface Design, and the types of evaluation approaches they would use to measure the usability of the security aspects of the user interface.

Regarding the technical component of the system, to attempt to make the case study authentic, students along with tutors develop and manage their groups own cloud-based learning environment. The cloud-based learning environment includes a small commercial system of a retail organisation. The students are tasked with reviewing this system and make recommendations for its usability.

In addition to students and tutors working together, for the socio-technical is to be effective, tutors are expected to work with cloud-based security specialist, and through student experts (who have studied a cybersecurity course) to implement technical aspects of the cloud-based security VLE. The mission for each student team involves the implementation of a user interface in the form of a low-fidelity prototype. Students are required to consider different ways to prevent social engineering and improve usability security. Students who have previously studied cybersecurity are expected to lead the practical sessions, helping the security specialist to share knowledge and expertise throughout the entail learning community.

A key aspect of the exercise involved tutors leaving students to drive agenda and facilitate the addressing of issues. Where possible consider the use of CSCW as opposed to independent standalone and individual practices. This includes each student team incorporating an ethical hacking approach by recruiting testers to attack their small commercial system, and conducting their own evaluation of the system. Students will have been given access to key components of the technical system such as the web server and database management system, but not the dedicated server. This server will be restricted to students but not tutors and the security specialist. Students will be introduced to ethical hacking and encouraged to test the usability and effectiveness of each teams solution. They will not be aware of the dedicated system.

Throughout the course tutors will assess the progress of the students and evaluate the performance of each teams security system. Tutors seek to address the following key questions based on students progress.

- How usability forms part of security; how it is integral to useable security.
- How technical strategies are realised within pilot.
- How social strategies are realised within pilot.
- How inclusive strategies realised within pilot.

Throughout, students are not made aware of the inclusive strategies taking centre stage. Tutors will be seeking evidence to what extent such strategies are present and being applied. Future work will seek to develop this aspect based upon findings.

In the course of the Pilot Study, students are asked to address the human weak link in security, and to explore ways of managing risks and threats within the provided cloud-based secure learning environment.

We outline below the main components of the Pilot Case Study to be implemented:

- Pilot Case Study to be implemented within HE;
- Aims and objectives of pilot case study:
  - To address the human weak link in security;
  - To enhance an inclusive security learning community, culture and environment;
  - To explore ways of managing risks and threats within a cloud-based secure learning environment.
- Targets MSc IT students studying the programme full time on campus:
  - September starts will have studied the first term of the programme;

    - January starts will have just started the programme.
- Rationale for target sample:
    - Students have various levels of knowledge and understanding of Information Security (IS);
    - Some students received course on IS;
    - Some students will not have received a course on IS.
- Cloud-based learning environment:
    - MyAberdeen / MyTimetable / MyCurriculum;
    - Email / Virtual Desktop Infrastructure (VDI) / Zend / PHPMYADMIN;
    - Bring Your Own Devices (BYOD)s — mobiles, tablets, laptops, PCs;
    - Personal storage space — University, external;
    - Social media — linkedin, facebook, twitter, youtube;
    - Integrated Development Environment (IDE)s — cloud9, Codio, Git/Github, SPM;
    - Other — Dropbox, milkthecow.
- How inclusive strategies are realised within pilot case study;
- How technical strategies are realised within pilot case study;
- Pilot case study forms part of a course on HCI; how to develop usable security.

Tutors and students develop and manage their own cloud-based learning environment as part of practical sessions. Practical sessions require students to apply content covered in HCI lectures and then consider its relevance to cloud-based security systems within HE. Additional two-hour voluntary weekly sessions introduced to provide space in the schedule for reflection and planning.

Tutors work with cloud-based experts, and through student experts (who have studied on the IS course) to implement technical aspects of the cloud-based security Virtual Learning Environment (VLE). The mission for each student group is to implement a course wiki in the form of a MySQL database with independent logging. Students are required to consider different ways to prevent social engineering and improve usability of security.

A key aspect of the exercise involved tutors leaving students to drive the agenda and facilitate the addressing of issues. Where possible, we considered the use of Computer Supported Co-operative Work (CSCW) as opposed to independent standalone and individual practices. This includes each student team incorporating an ethical hacking approach by recruiting testers to attack their small commercial system, and conducting their own evaluation of the system. Students will have been given access to key components of the technical system such as the web server and database management system, but not the dedicated server. This server will be restricted to students but not tutors and the security specialist. Students will be introduced to ethical hacking and encouraged to test the usability and effectiveness of each teams solution. They will not be aware of the dedicated system.

Throughout the course tutors will assess the progress of the students and evaluate the performance of each teams security system.

Tutors seek to address the following key questions based on students' progress:

- How usability forms part of security; how it is integral to use-able security;
- How technical strategies are realised within pilot;
- How social strategies are realised within pilot;
- How inclusive strategies realised within pilot.

Throughout, students are not made aware of the inclusive strategies taking centre stage. Tutors will be seeking evidence as to what extent such strategies are present and being applied. Future work will seek to develop this aspect based upon the findings. In the next section, we address some limitations of this work.

VII. Limitations and Discussion

There are a number of limitations in this work, which we will now discuss. Whilst the initial intentions are proving positive, this pilot case study involves small numbers of students who have had time to develop relationships as peers with fellow students and tutors. A key factor lacking is the heterogeneous nature of teams in learning environments. However, we plan to address this once the pilot case study concludes. Once the findings are fully analysed, we will incorporate the findings and implement the full case study starting from September, which will give us access to the impact of the full heterogeneous nature of teams in learning environments.

We hope to get the message across to all students that there needs to be serious consideration given to taking into account the potential impact of new legislation and regulation as it comes in to effect. Further education institutions need to be at the cutting edge so that once students leave with their qualifications, they will be ideally placed to ensure their future employers will be better able to improve policies, procedures and good working practices, to ensure they achieve adequate compliance with legislative and regulatory bodies. We also hope that students will achieve a better understanding of how to approach achieving a high level of usable security in their future employment.

VIII. Conclusion

This pilot case study forms part of a proof of concept for a longer term case study, which we hope to use to be able to ensure all students gain a better understanding of all the issues of security and privacy that must now be taken into account for all organisations who handle any form of PII. We anticipate being able to present the results of this pilot case study at the conference.

We believe the concept will help ensure that all students will be able to work in a secure and private environment, while learning how to safeguard themselves, their peers and their future employers. The proposed framework will be able to ensure that organisations can achieve compliance with the forthcoming EU GDPR, as well as achieving compliance with existing legislation on security and privacy. By ensuring that the framework can be resistant to the effects of the cloud forensic problem, this will ensure a robust capability to provide a high level of security and privacy.

Naturally, we accept that there will be a need for a more thorough and substantial investigation, and we will endeavour to achieve this with the next phase of the project, where we will be applying the framework to a full cohort of students, which will allow us to understand how those with different levels of experience can work together to ensure the safety of the whole educational environment.

REFERENCES

[1] Crown, "Data Protection Act 1998," 1998. [Online]. Available: http://www.legislation.gov.uk/ukpga/1998/29/contents [Retrieved: December 2017]

[2] EU, "EU General Data Protection Regulation (GDPR)," 2017. [Online]. Available: http://www.eugdpr.org/ [Retrieved: December 2017]

[3] N. Beacham and B. Duncan, "Development of a Secure Cloud Based Learning Environment for Inclusive Practice in Mainstream Education," in Cloud Comput. 2017 Eighth Int. Conf. Cloud Comput. GRIDs, Virtualization, Athens, 2017, pp. 1–4.

[4] J. M. Blythe, L. Coventry, and L. Little, "Unpacking security policy compliance : The motivators and barriers of employees ' security behaviors," Proceedings of the Eleventh Symposium On Usable Privacy and Security (SOUPS 2015), Ottawa, Canada, 2015, pp. 103–122.

[5] S. L. Pfleeger and D. D. Caputo, "Leveraging behavioral science to mitigate cyber security risk," Computers and Security, vol. 31, no. 4, 2012, pp. 597–611.

[6] D. Mitchell, " What really works in special and inclusive education: Using evidence-based teaching strategies." (2nd ed.). [Online] Available: http://ovidsp.ovid.com/ovidweb.cgi?T=JS&PAGE=reference&D=psyc11&NEWS=N&AN=2014-03315-000 [Retrieved December 2017]

[7] L. Dare and E. Nowicki, "Strategies for inclusion: Learning from students' perspectives on acceleration in inclusive education," Teaching and Teacher Education, vol. 69, 2018, pp. 243–252.

[8] H. Dong, "Strategies for teaching inclusive design," Journal of Engineering Design, vol. 21, no. 2-3, 2010, pp. 237–251.

[9] V. E. Mumford and J. P. Chandler, "Strategies for Supporting Inclusive Education for Students with Disabilities," Strategies, vol. 22, no. 5, 2009, pp. 10–15 Taylor & Francis Group.

[10] K. S. Young, "Institutional separation in schools of education: Understanding the functions of space in general and special education teacher preparation," Teaching and Teacher Education, vol. 27, no. 2, 2011, pp. 483–493

[11] L. Florian and J. Hegarty, ICT and Special Educational Needs: a tool for inclusion. McGraw-Hill Education (UK), 2004.

[12] A. Istenic Starcic and S. Bagon, "ICT-supported learning for inclusion of people with special needs: Review of seven educational technology journals, 1970-2011," British Journal of Educational Technology, vol. 45, no. 2, 2014, pp. 202–230.

[13] A. K. Yadav, "Supporting Inclusive Education Through ICT Implementation: An Intermediary Role," Educational Quest, vol. 5, no. 1, 2014, pp. 51–55.

[14] World Health Organisation, "Assistive Technology for Children with Disabilities: Creating Opportunities for Education, Inclusion and Participation A discussion paper," World Health Organization, 2015, p. 34.

[15] N. Beacham, "Developing NQTs e-pedagogies for inclusion," University of Aberdeen, Aberdeen, Tech. Rep. May, 2011. [Online]. Available: https://www.heacademy.ac.uk/system/files/8065_0.pdf [Retrieved: December 2017]

[16] N. Papanikolaou, S. Pearson, M. C. Mont, and R. Ko, "A Toolkit for Automating Compliance in Cloud Computing Services," Int. J. Cloud Comput., vol. x, no. x, 2014, pp. 45–68.

[17] J. Singh and J. M. Bacon, "On middleware for emerging health services," J. Internet Serv. Appl., vol. 5, no. 1, 2014, p. 6.

[18] J. Singh, J. Bacon, and D. Eyers, "Policy Enforcement Within Emerging Distributed, Event-based Systems," Proc. 8th ACM Int. Conf. Distrib. Event-Based Syst. - DEBS '14, 2014, pp. 246–255.

[19] J. Singh, J. Powles, T. Pasquier, and J. Bacon, "Seeing through the clouds: Management, control and compliance for cloud computing," Cloud Comput., 2015, pp. 1–12.

[20] B. Duncan and M. Whittington, "Creating and Configuring an Immutable Database for Secure Cloud Audit Trail and System Logging," Int. J. Adv. Secur., no. 3&4, 2017.

[21] R. K. L. Ko et al., "TrustCloud: A Framework for Accountability and Trust in Cloud Computing," Perspective, 2011, pp. 1–9.

[22] 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, 2011, pp. 432–444.

[23] N. Papanikolaou, S. Pearson, and M. C. Mont, "Towards Natural-Language Understanding and Automated Enforcement of Privacy Rules and Regulations in the Cloud: Survey and Bibliography," Analysis, 2011, pp. 1–9.

[24] S. Pearson, "Taking Account of Privacy when Designing Cloud Computing Services," Current, 2009, pp. 44–52.

[25] S. Pearson, "Toward accountability in the cloud," IEEE Internet Comput., vol. 15, no. 4, jul 2011, pp. 64–69.

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

[27] B. Duncan and M. Whittington, "Creating an Immutable Database for Secure Cloud Audit Trail and System Logging," in Cloud Comput. 2017 Eighth Int. Conf. Cloud Comput. GRIDs, Virtualization. Athens, Greece: IARIA, ISBN: 978-1-61208-529-6, 2017, pp. 54–59.