Enterprise Security and Privacy: Why Adding IoT and Big Data Makes It So Much More Difficult

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

Mark Whittington
Business School
University of Aberdeen
Aberdeen, UK
Email: mark.whittington@abdn.ac.uk

Victor Chang
International Business School Suzhou
Xian Jiaotong-Liverpool University
PR China
Email: ic.victor.chang@gmail.com

***Abstract*—Achieving enterprise security is a huge challenge, which becomes much more challenging when cloud is added to the mix, due to the multi-tenancy nature of cloud ecosystems. Once we add the dimensions of the Internet of Things (IoT) and Big Data, this problem becomes exponentially more complex. We consider why this is so and highlight a number of key research questions which have yet to be resolved. We seek to address the problem by combining a number of emerging research techniques which we and our collaborators have developed, in such a way as to improve the chance of achieving a better level of security and privacy for enterprises.**

***Index Terms*—Enterprise security; Enterprise privacy; Cloud security; Internet of Things; Big Data**

I. Introduction

In previous work [1], we questioned why we keep making enterprise security such a difficult challenge to achieve, and concluded that there were a number of contributing factors. We indicated that not enough attention was being paid to the ever increasing complexity of enterprise systems and that this led to unwarranted complacency developing in many enterprises. Added to this, a considerable number of well known flaws in the public face of enterprises — web services — continued to be ignored, yet the simple steps to protect against these weaknesses can often be very straightforward to address. The constant quest for ever more sophisticated and capable software, leads to ever more complex software, which opens up the possibility of inadvertently introducing ever more vulnerabilities into enterprise systems.

One might consider that these circumstances might induce a pause for thought, an attempt to catch up with the need to secure enterprise systems properly. However, this thought is little more than wishful thinking: instead, we must now also consider the addition of IoT and Big Data to this already vulnerable mix. Some may perceive these as limited extensions of already complex enterprise; we seek to raise the level of concern and awareness of the significant implications of expanding into these new zones.

While it is true to say they are extensions, such advances are far from simple. They are additional complexities being layered on top of already highly complex systems. This makes the job of proper enterprise security and privacy considerably more difficult. While this, in itself, should be sufficient to gain management attention, there is the unavoidable challenge of ensuring enterprises meet legislative and regulatory requirements. Indeed, it may well be the privacy requirements of the impending EU General Data Protection Regulation (GDPR) that will focus the minds of any enterprise operating within the EU, even with the smallest division, indeed especially with the smallest division.

Our contribution from this paper is to help enterprises become more aware of the pitfalls they face to security and privacy from the the combination of cloud, IoT and Big Data. We improve previous work in this area by combining the strength of this work through the use of immutable database technology with the work of collaborators to improve the efficiency and effectiveness of the resulting solution, thus improving the resilience to attack. The next stage in this work is to combine these solutions into a comprehensive framework to eliminate any possible weaknesses remaining. There is no doubt this presents a significant further challenge and forms part of our future work. The other contribution, which aligns this work to the DAES 2017 workshop is to highlight the huge potential threat from data breaches to enterprises in the light of the forthcoming EU GDPR, which comes into effect in May 2017. It will affect all enterprises who trade in the EU, even to a small extend, and fines for breaches are potentially catastrophic since they are based on the global turnover of the enterprise from the previous financial year, not the EU turnover only.

Thus we need to consider how the evolution of the business environment constantly drives the change in enterprise computing and we look at this in Section II. Once we have covered how the evolution of the business environment is the driving factor for technological change, we must look at the specifics of IoT and Big Data to better understand the impact on enterprise security and privacy. We address the IoT in Section III, and Big Data in Section IV. Of course, we must consider the cloud, and current weaknesses and unresolved issues, which we carry out in Section V.

The rest of the paper is laid out as follows: in Section VI, we ask why this matters. In Section VII, we consider how we might approach resolving these issues, and in Section VIII, we draw our conclusions and consider future research.

II. The Evolution of the Business Environment

It is usual to assume that the primary goal of an enterprise is to maximise the return on shareholders' investment. This results in a continuous drive to improve the efficiency of the organisation. Computing systems can play an ever increasing part in achieving these objectives, but only if they are properly developed, deployed and maintained. Many enterprises start out as small businesses, often family owned, which grow over time, until they can no longer be run by individuals, or families, which then, following many others before them in the development of the modern corporation, lead to professional managers being appointed to run the business on behalf of the owners (shareholders). These managers then seek to grow the companies, and achieve this by a combination of continuing re-investment and takeovers. Thus companies continue to expand and the logical consequence is that computing systems also need to evolve rapidly to keep up. Other things being equal, companies with the best, biggest and fastest computing systems may be expected to gain a competitive advantage over their competition over time.

The fast evolving environment leads to continuous change, and it is this change that drives the requirement for technological change. As technology advances and systems become more complex, control systems need to also develop to keep pace with developments and changing risk. In previous work [2], [3], we addressed the weaknesses in maintaining a proper audit trail in a cloud environment, proposing an emerging solution to this problem. Ensuring proper cloud forensics is also a major unresolved challenge, although a number of our collaborators [4], [5], have addressed this and proposed some solutions. This area will doubtless require further work, and as we will see in the following chapters, will impact on the further introduction of IoT and Big Data.

III. The Impact of IoT on Enterprise Security and Privacy

The IoT took some time to really get started. After Tim Berners-Lee proposed the World Wide Web in 1989, various developments started to give more traction to the possibility of the IoT. Kevin Ashton proposed the use of RFID technology, [6], would lead to the development of a global RFID-based item identification system called the Electronic Product Code or EPC, which was intended to replace the universal product code (UPC) bar code. Very little happened until 2007, when Gantz et al., [7] forecast that the total of all global electronic data collected would double every 18 months. 2008 saw the EU establish an international conference on the IoT, and Cisco suggested that the IoT had now been born, as there were now more connected devices to the internet than people.

Internet protocol version 4 (IPv4) had been projected to run out of numbers some time around the end of the century, which was one of the reasons that Kevin Ashton had been so keen on the RFID approach. But, internet protocol version 6 (IPv6) had been developed to address this issue, so there would no longer be any practical limitation to the number of "things" that could be connected to the internet, and this is why the use of IP became the preferred route for IoT connection. By this time, cloud computing was well evolved, and this helped to provide even more traction for the development of the IoT.

Given the usual motivation for the development of computer systems, where functional requirements often take precedence over security and privacy concerns, it is not a surprise when little thought is then given to the introduction of vulnerabilities caused by using cheaply built "things" with little or no security. Many of the "things" in use will often communicate using Bluetooth, or wifi to pass on information to the main data servers of the enterprise, often using cloud services to facilitate this process. Little account is taken of the weaknesses present in these systems, which leave the components open to hacking by malicious outsiders.

These are not the only weaknesses. Any component of a system which is connected via the internet is susceptible to potential hacking attempts by malicious outside parties. Sometimes the components are of low quality, with low levels of system memory, often with well known vulnerabilities and "back doors".

The IoT also causes considerable potential growth in another technology — Big Data: thus we also consider the impact of big data on enterprise security and privacy in the next section.

IV. The Impact of Big Data on Enterprise Security and Privacy

Big Data too, has been around a long time. Enterprises have been collecting data at an ever increasing rate for decades. For much of that time, the data has lain dormant due to enterprises having no means of understanding or analysing what it contains. With huge volumes of data increasing beyond the storage capacity of individual computers, doing anything with this amount of data was all but impossible.

Back in 2001, Doug Laney of Gartner [8], was first to classify Big Data problems as the 3 Vs — namely Variety, Velocity and Volume. He observed that data came in all shapes and sizes, meaning storage and classification of all these different data types would present an exceptionally difficult challenge. The velocity at which enterprises produced and accumulated data would also present a difficult challenge, due to the continuously increasing rate at which data was being collected. This would then compound the third issue — volume. This ever expanding rate of creation of new data would ultimately require to be stored somewhere. With data volumes reaching the stage where no single computer could contain them, this turned into a significant challenge.

Many years later, in 2012, IBM [9], added another issue to the Gartner 3Vs — Veracity. They were concerned that this collection of data would be worthless if veracity of the data could not be maintained. Just when we thought there were no more issues to contend with, Experian [10], added another

two issues — Vulnerability and Value. They realised that such large collections of data would provide attractive targets for attackers, as they realised that such data collections have massive potential value to companies if they can unlock their secrets. Obviously, the loss or compromise of such valuable data collections would have a potentially catastrophic negative impact on profits.

Both of these important technologies were very slow to gain traction, and it was not until the development of Cloud Computing that they really took off.

V. The Impact of Cloud on Enterprise Security and Privacy

Once cloud computing took off from around 2007 onwards, cloud provided greater traction for both IoT and Big Data. The nature of IoT is such that data may not be streamed at a constant rate, thus leading to a need for on demand resources, which cloud is perfectly placed to provision. Likewise, for Big Data, there may be a huge amount of data being generated which may exceed the capacity of in-house machines. Cloud can be very quickly expanded to cope with any volume and velocity of demand sought — a situation that cannot be matched with in-house resources.

However, a decade ago, cloud itself was anything but secure for enterprises, nor did it offer a satisfactory level of privacy. Early research was targeted towards showing how efficient and cost effective the technology was [11]–[13], although some [14], were questioning if cloud computing was ready for the mainstream yet. However, by 2010, there was a serious interest developing in recognising, and dealing with, the security and privacy implications of cloud [15]–[25], and this has continued apace in the years since.

Ko et al., [26], suggest there needs to be more accountability and audit-ability in cloud, with Almorsy et al., adding concern about collaboration [27], and further improvements in cloud architecture to improve security. Ruan et al., [28], highlight a problem for cloud forensics due to the ever increasing amounts of data being processed through cloud. The growing concern for security was further highlighted by Grobauer et al., [29], suggesting that companies need to be fully aware of the vulnerabilities of cloud computing, and to deal with them appropriately; Subashini and Kavitha [30], carrying out a survey on known security issues; and Winkler [31], suggesting we should take steps to make cloud architecture more secure.

The range of important security questions to be researched and addressed seems almost endless. The list below seeks to highlight some of the wide-ranging issues that require awareness, monitoring or solutions:

- Chen and Zhao [32], consider data security and privacy protection issues in cloud computing.
- Pearson et al., [33], express the need for cloud service providers (CSP)s to provide better stewardship and accountability for their services.
- Catteddu et al., [34], develop an accountability model for cloud computing.
- Chang, Walters and Wills [35], develop a cloud computing business framework.
- Doelitzscher et al., [36], propose a neural network approach for detecting anomalous behaviour in cloud.
- Duncan, Pym and Whittington [37], develop a conceptual framework for cloud security assurance.
- Pasquier, Shand and Bacon [38], propose information flow control to improve security and privacy in cloud situations.
- Pearson [39], proposes further work on privacy, security and trust in cloud services.
- Prufer [40], considers how the cloud should be governed.
- Bacon et al., [41], propose information flow control for secure cloud computing.
- Duncan and Whittington [42], consider whether management approach can have an impact on cloud security and suggest the adoption of stewardship theory can improve security results.
- Rebollo et al., [43], carry out an empirical test on a case study using their cloud computing information security governance framework and find it to be useful in helping organisations meet their security governance objectives.
- Singh et al., [44], suggest that as legal and regulatory issues associated with the cloud become more pronounced, it becomes more important to provide a means of identifying data control through cloud systems.
- Chang, Kuo and Ramachandran [45], propose a multi-layered security framework for business organisations.
- Duncan and Whittington [2], address the challenge of maintaining a solid audit trail in cloud systems.
- Singh et al., [46], provide 20 suggestions to improve cloud-supported IoT.
- Duncan and Whittington [3], propose the use of an immutable database to ensure proper capture of a full audit trail for cloud systems.
- Neovius and Duncan [47], propose an anomaly detection process to provide soft security in cloud based accounting systems.
- Tobin et al., [5], propose a one-time pad generator for personalising cloud security.
- Weir and Amuth [4], propose new forensic strategies using system calls to ensure a proper forensic trail may be maintained.

By 2014, this academic concern was matched by over 30 organisations working on cloud security and privacy standards. Yet there is still no comprehensive standard in operation in 2017 [48]. The EU is one of many regulatory organisations concerned about cloud security and privacy issues. The EUs Article 29 data protection working party [49], carried out a thorough analysis of cloud computing, from a data protection perspective, with particular emphasis on security and privacy issues in the cloud. Hon, Hornle and Millard [50], address the jurisdiction of EU data privacy concerns. The implications of regulatory behaviour are also addressed by academics with, for example, Bernsmed et al., [51], considering accountability obligations when deploying medical sensor networks in EU

jurisdictions and Hon et al., [52], addressing the likely impact of proposed EU data protection regulation on cloud computing. With a broader perspective Hon et al, [53], address the policy, legal and regulatory implications of an EU-only cloud.

There has been such a plethora of security and privacy research carried out, especially based on technical solutions, that there is a consensus that there has been such an improvement in cloud security and privacy, that there is likely to be a greater danger from people-based attacks rather than from technical weaknesses. While there is a great deal of truth in tat thought, there is no doubt that attackers continue to probe cloud systems for technical weaknesses, which means there is little scope to breath easy on this front. It is also the case that the ease with which full forensic trails can be attacked, and destroyed, in cloud systems remains a worrying concern.

VI. Why Does This Matter?

By looking at the previous sections, we can start to get an idea of the magnitude of the challenge. Cyber security is not a trivial exercise. In the cloud, the challenge increases exponentially. IoT and Bid Data simply add additional layers of complexity to this already highly complex challenge. When we consider that a great many enterprises are already heavily committed to the use of cloud-based IoT systems and Big Data, we can start to get a sense of the enormity of the challenge.

Then, there is the forthcoming EU GDPR legislation, which will come into force in May 2018. Why would this matter? There is a very good reason why this would matter. Every company that trades in the EU will be subject to the privacy provisions of this legislation, or rather the resulting punitive fines for breach of these privacy provisions. One of the most challenging aspects of this legislation will be the requirement to report any privacy breach within 72 hours of its occurrence. In 2012, Trustwave [54], were reporting an industry average of 6 months between breach and discovery, with most discoveries made by external parties. The latest report from Infocyte [55], suggests that the global average is 146 days. The Verizon 2017 [56], report confirms the gap between breach and discovery.

But why does this matter? Remember the EU GDPR? With a requirement to report a breach within 72 hours, this means the average enterprise will be breaking the law without even trying. Fines for a first offence can be as high as 10 million Euros or 2% of global turnover. Since few enterprises will be in a position to catch a security breach within 72 hours, let alone report it in time, there are likely to be a lot of fines levied. Latest estimates suggest over 5 billion Euros for the big UK banks alone within the first year.

VII. How Do We Address This Problem?

Enterprises need to recognise a number of points. First, cloud computing is not yet guaranteed secure, nor can it guarantee privacy. Second, the IoT is riddled with insecurities and there are also weaknesses in communication which need to be addressed. Third, Big Data can be considered inherently insecure due the fact that it is database-based, and is therefore subject to all the existing security vulnerabilities of conventional enterprise database systems. Added to this, these database systems are hosted on cloud systems which cannot be guaranteed to provide adequate security and privacy.

One of the major obstacles yet to be fully resolved for cloud is the ease with which an attacker can delete any forensic evidence contained in cloud systems. This also pertains to audit trail data. Due to the multi-tenancy nature of cloud, there are far more people who can access enterprise data than most enterprises would care to believe, with many of these coming from within the cloud ecosystem itself. The high complexity of cloud systems, especially when linked with IoT and Big Data, means that configuring these systems securely is a far greater challenge than ever before.

Performing cloud encryption properly also represents another significant challenge. Some enterprises are still in the habit of leaving encryption keys on cloud servers “to make it easier to identify and query cloud data”, which completely undermines the point of encryption. There are plenty of solutions to this problem which are readily available to allow this major risk to be eliminated.

Social engineering remains a growing concern for enterprises. With cloud systems becoming more technically secure, attackers use alternative means of attack. Social engineering is a long used part of their armoury and they keep using it because it works! Enterprises would do well to recognise this fact of life and carry out regular training on this insidious, yet successful, practice.

An obvious conclusion to be drawn from the security breach reports into the long time gap between breach and discovery, would be that many enterprises are failing to monitor their systems properly. The security breach reports also indicate that there can be some time between compromise and effecting the ex-filtration of data. This would also provide some evidence to support the idea that many enterprises are failing to monitor their systems properly, as forensic evidence would be left at this stage. Clearly, the ease with which this evidence can be erased from cloud systems is a major concern, but failing to monitor systems properly is every bit as damaging as handing the keys to the attacker would be.

Cloud is a web-based resource. There are a great many known vulnerabilities in web systems, and in database systems in particular. The Open Web Application Security Project (OWASP) [57], is an online community producing reports and security recommendations for a variety of web-based architectures, including cloud, mobile computing and IoT. They regularly produce a Top Ten list of the most dangerous vulnerabilities in each category. They produce full lists of all vulnerabilities and also provide good advice on how to mitigate each vulnerability. In addition, they also offer free software tools to test for various vulnerabilities.

We would recommend any enterprise wishing to alleviate the risk of attack on their cloud/IoT/Big Data systems should consider our Top Ten recommendations as appropriate or required:

If you are not monitoring your systems, there is no way that

Step	Action
1	Set up a comprehensive live monitoring system
2	Test all current systems for vulnerabilities
3	Check all IoT systems for weaknesses
4	Install all necessary mitigation steps
5	Set up an audit trail immutable database
6	Set up a forensic trail monitoring system
7	Ensure encrypted systems are securely installed
8	Train all staff to be aware of social engineering
9	Train all staff to be aware of email weaknesses
10	Ensure security updates are installed on time

TABLE I: Our Top Ten Security Recommendations

you can pick up what is happening day by day. A regular test for potential vulnerabilities in all your systems is a good way to keep up with the changing threat environment. Your systems might be fine today, but next week, next month or next year, there may be new vulnerabilities which can cause your secure systems to become vulnerable again. There are many known weaknesses in IoT systems. Enterprises need to check every single component, embedded, mobile or otherwise to ensure they do not contain any known vulnerabilities.

Utilising the advice of an organisation like OWASP can be an inexpensive route to improved security. Much of their advice is common sense, although that is not always in abundance in enterprise systems. We seek to incorporate some emerging technology to address the issues of ensuring a proper audit trail is achieved through the use of an immutable database, as a good way to secure accounting systems in the cloud, but this approach can also be adapted to any other system using a database back end, including all system calls, see [3].

We also seek to include the work of our collaborators to ensure a proper forensic trail monitoring system [4], [5], can be achieved, especially in conjunction with an immutable database, which will provide the prospect of retaining a high level of forensic evidence in the event of a security breach.

When encrypted systems are used, it is vital that they are properly configured. Leaving the keys for all comers on cloud instances is an elementary error. It is essential that these systems are also protected for both audit trail and forensic record purposes.

Two of the most successful attacks on staff are social engineering and email exploits. These attacks are well known and have been successfully deployed for decades. No modern enterprise should allow themselves to be victims to these well worn attack vectors.

While it would appear to be a case of "stating the obvious", a great many security breaches have been made possible by the very action of failing to update security patches. Excuses like "Oh, I do them all together", or "I don't do them, because it always upsets the smooth running of our software", do not cut it. A great many attackers spend all their time prowling the internet just to find enterprises like that.

Covering all the bases is likely to be both expensive and time consuming. Financial audit has developed techniques that seek to balance risk and effort with some additional random checking. Such an approach is effectively playing for a deliberate mix of achieve-ability and risk reduction. Of course, this would always need to be confidential as it would otherwise be ineffective.

VIII. Conclusions

We make the point that there are currently no comprehensive solutions for cloud computing security and privacy, and especially where IoT and Big Data are included.

While the measures we suggest will help to provide a short term solution for an enterprise, it is clearly far from satisfactory. Most software systems can trace their ancestry back to the times of pre-internet early enterprise systems. Here, the focus was on usability, not on security nor privacy.

When it comes to software implementations, enterprises would do well to learn the lessons of separation of duties, both for staff, process and technology, particularly in the case of audit trail logging.

The approach of the EU to fine breaches not reported within a very tight time frame might push companies and organisations to implement systems that are less about stopping invasive actions, but flash the equivalent of a blue light very soon after their occurrence. A nightly integrity routine might be one such measure.

As to the development of new software, there is a clear need to develop secure software systems from the ground up, rather than try to add security to an already complex piece of software as an afterthought. There is no doubt that there is a place for the development of an immutable database system, which would be particularly suitable for system logging and would be especially useful for deployment in accounting systems. And, of course, ensuring as full a forensic trail as can be retained is vital to establish who breached your systems and how they got in, so that you can ensure it does not happen again.

We strongly believe there is a pressing need to find a solution to this problem, and while our proposals present a pragmatic approach to improve matters at this time, further work needs to be done to enhance the resilience of this technology to serious attack.

References

[1] B. Duncan, M. Whittington, and V. Chang, "Enterprise Security: Why Do We Make It So Difficult?" in *33rd Euro-Asia Manag. Stud. Assoc. Annu. Conf.*, no. October, Suzhou, China, 2016, pp. 1–6.

[2] B. Duncan and M. Whittington, "Enhancing Cloud Security and Privacy: The Power and the Weakness of the Audit Trail," in *Cloud Comput. 2016 Seventh Int. Conf. Cloud Comput. GRIDs, Virtualization*, no. April. Rome: IEEE, 2016, pp. 125–130.

[3] 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: IARIA, ISBN: 978-1-61208-529-6, 2017, pp. 54–59.

[4] G. Weir and A. Aßmuth, "Strategies for Intrusion Monitoring in Cloud Services," in *Cloud Comput. 2017 Eighth Int. Conf. Cloud Comput. GRIDs, Virtualization*, Athens, 2017, pp. 1–5.

[5] P. Tobin, L. Tobin, M. McKeever, and J. Blackledge, "On the Development of a One-Time Pad Generator for Personalising Cloud Security," in *Cloud Comput. 2017 Eighth Int. Conf. Cloud Comput. GRIDs, Virtualization*, Athens, Greece, 2017, pp. 1–6.

[6] K. Ashton, "That 'Internet of Things' Thing," *RFiD J.*, vol. 22, no. 7, pp. 97–114, 2009.

[7] J. F. Gantz, D. Reinsel, C. Chute, W. Schlichting, J. McArthur, S. Minton, I. Xheneti, A. Toncheva, and A. Manfrediz, "The Expanding Digital Universe: A Forecast of Worldwide Information Growth Through 2010," in *Extern. Publ. IDC (Analyse Futur. Inf. Data*. IDC, 2007, pp. 1–21.

[8] D. Laney, "META Delta," *Appl. Deliv. Strateg.*, vol. 949, no. February 2001, p. 4, 2001.

[9] IBM, "IBM Four V's of Big Data," 2012. [Online]. Available: http://www.ibmbigdatahub.com/infographic/four-vs-big-data

[10] Experian, "Experian 6Vs of Big Data," 2017. [Online]. Available: http://www.experian.co.uk/blogs/latest-thinking/the-evolution-of-big-data-the-6vs/

[11] TSB, "Our strategy for 'Digital Britain'," *Technology*, no. June, pp. 1–16, 2009.

[12] E. N. Agency and I. Security, "Cloud Computing: Benefits, Risks and Recommendations for Information Security - Google Search," *Computing*, vol. 72, no. 1, pp. 2009–2013, 2009.

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

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

[15] M. Almorsy, J. Grundy, and I. Müller, "An analysis of the cloud computing security problem," *17th Asia-Pacific Softw. Eng. Conf. (APSEC 2010) Cloud Work. Aust.*, no. December, p. 7, 2010.

[16] E. Brynjolfsson, P. Hofmann, and J. Jordan, "Cloud Computing and Electricity: Beyond the Utility Model," *Commun. ACM*, vol. 53, no. 5, p. 32, may 2010.

[17] Y. Chen, V. Paxson, and R. H. Katz, "Handbook of Cloud Computing," *Handb. Cloud Comput.*, vol. 20, no. 2010, pp. 493–516, 2010.

[18] M. Collinson, B. Monahan, and D. Pym, "Semantics for Structured Systems Modelling and Simulation Matthew," *Proc. 3rd Int. ICST Conf. Simul. Tools Tech.*, pp. 34–43, 2010.

[19] B. Grobauer and T. Schreck, "Towards Incident Handling in the Cloud: Challenges and Approaches," *ACM Work. Cloud Comput. Secur. Work.*, pp. 77–85, 2010.

[20] A. Haeberlen, "A Case for the Accountable Cloud," *ACM SIGOPS Oper. Syst. Rev.*, vol. 44, no. 2, p. 52, 2010.

[21] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," in *2010 IEEE Second Int. Conf. Cloud Comput. Technol. Sci.*, no. December. Ieee, nov 2010, pp. 693–702.

[22] D. Pym and M. Sadler, "Information Stewardship in Cloud Computing," *Int. J. Serv. Sci. Manag. Eng. Technol.*, vol. 1, no. 1, pp. 50–67, 2010.

[23] S. Ramgovind, M. M. Eloff, and E. Smith, "The management of security in cloud computing," in *Proc. 2010 Inf. Secur. South Africa Conf. ISSA 2010*, 2010, pp. 1–7.

[24] C. Soghoian, "Caught in the cloud: Privacy, encryption, and government back doors in the web 2.0 era," *J. Telecomm. High Tech. L.*, vol. 8, no. 2, pp. 359–424, 2010.

[25] P. C. Van Oorschot, "System Security, Platform Security and Usability," *Proc. fifth ACM Work. Scalable Trust. Comput.*, pp. 1–2, 2010.

[26] 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, pp. 432–444, 2011.

[27] M. Almorsy, J. Grundy, and A. S. Ibrahim, "Collaboration-Based Cloud Computing Security Management Framework," in *Proc. - 2011 IEEE 4th Int. Conf. Cloud Comput. CLOUD 2011*, 2011, pp. 364–371.

[28] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics," in *Adv. Digit. Forensics VII, IFIP Adv. Inf. Commun. Technol.*, vol. 361, no. 2009, 2011, pp. 35–46.

[29] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding Cloud Computing Vulnerabilities," *IEEE Secur. Priv.*, vol. 9, no. 2, pp. 50–57, 2011.

[30] S. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, 2011.

[31] V. J. Winkler, "Chapter 4 - Securing the Cloud: Architecture," in *Secur. Cloud*. Syngress Publishing, 2011, ch. 4, pp. 89–123.

[32] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," *2012 Int. Conf. Comput. Sci. Electron. Eng.*, vol. 1, no. 973, pp. 647–651, 2012.

[33] S. Pearson, V. Tountopoulos, D. Catteddu, M. Sudholt, R. Molva, C. Reich, S. Fischer-Hubner, C. Millard, V. Lotz, M. G. Jaatun, R. Leenes, C. Rong, and J. Lopez, "Accountability for Cloud and Other Future Internet Services," in *CloudCom 2012 - Proc. 2012 4th IEEE Int. Conf. Cloud Comput. Technol. Sci.*, 2012, pp. 629–632.

[34] D. Catteddu, M. Felici, G. Hogben, A. Holcroft, E. Kosta, R. Leened, C. Millard, M. Niezen, D. Nunez, N. Papanikolaou, S. Pearson, D. Pradelles, C. Reed, C. Rong, J.-C. Royer, D. Stefanatou, and T. W. Wlodarczyk, "Towards a Model of Accountability for Cloud Computing Services," in *Int. Work. Trust. Account. Forensics Cloud*, 2013, pp. 21–30.

[35] V. Chang, R. J. Walters, and G. Wills, "The development that leads to the Cloud Computing Business Framework," *Int. J. Inf. Manage.*, pp. 1–22, 2013.

[36] F. Doelitzscher, M. Knahl, C. Reich, and N. Clarke, "Anomaly detection in IaaS Clouds," in *Proc. Int. Conf. Cloud Comput. Technol. Sci. CloudCom*, vol. 1, 2013, pp. 387–394.

[37] B. Duncan, D. J. Pym, and M. Whittington, "Developing a Conceptual Framework for Cloud Security Assurance," in *2013 IEEE 5th Int. Conf. Cloud Comput. Technol. Sci.* Bristol: IEEE, 2013, pp. 120–125.

[38] T. Pasquier, B. Shand, and J. Bacon, "Information Flow Control for a Medical Records Web Portal," *Cl.Cam.Ac.Uk*, pp. 1–8, 2013.

[39] S. Pearson, "Privacy and Security for Cloud Computing," in *Priv. Secur. Cloud Comput.* e: Springer, 2013, pp. 3–42.

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

[41] J. Bacon, D. Eyers, T. F. J.-M. Pasquier, J. Singh, I. Papagiannis, and P. Pietzuch, "Information Flow Control for Secure Cloud Computing," *IEEE Trans. Netw. Serv. Manag.*, vol. 11, no. 1, pp. 76–89, 2014.

[42] B. Duncan and M. Whittington, "Company Management Approaches Stewardship or Agency: Which Promotes Better Security in Cloud Ecosystems?" in *Cloud Comput. 2015*. Nice: IEEE, 2015, pp. 154–159.

[43] O. Rebollo, D. Mellado, E. Fernández-Medina, and H. Mouratidis, "Empirical evaluation of a cloud computing information security governance framework," *Inf. Softw. Technol.*, vol. 58, pp. 44–57, 2015.

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

[45] V. Chang, Y. H. Kuo, and M. Ramachandran, "Cloud computing adoption framework: A security framework for business clouds," *Futur. Gener. Comput. Syst.*, vol. 57, pp. 24–41, 2016.

[46] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, "Twenty Security Considerations for Cloud-Supported Internet of Things," *IEEE Internet Things J.*, vol. 3, no. 3, pp. 269–284, 2016.

[47] M. Neovius and B. Duncan, "Anomaly Detection for Soft Security in Cloud based Auditing of Accounting Systems," in *Closer 2017 - 7th Int. Conf. Cloud Comput. Serv. Sci.*, Porto, Portugal, 2017, pp. 1–8.

[48] B. Duncan and M. Whittington, "Compliance with standards, assurance and audit," in *Proc. 7th Int. Conf. Secur. Inf. Networks - SIN '14*. Glasgow: ACM, 2014, pp. 77–84.

[49] Data Protection Working Party, "Opinion 05/2012 on Cloud Computing," 2012. [Online]. Available: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196{_}en.pdf

[50] 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?" *Int. Rev. Law, Comput. Technol.*, vol. 26, no. 2-3, pp. 129–164, 2012.

[51] K. Bernsmed, W. K. Hon, and C. Millard, "Deploying Medical Sensor Networks in the Cloud Accountability Obligations from a European Perspective," in *Cloud Comput. (CLOUD), 2014 IEEE 7th Int. Conf.* IEEE Comput. Soc, 2014, pp. 898–905.

[52] W. K. Hon, E. Kosta, C. Millard, and D. Stefanatou, "Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation," *SSRN Electron. J.*, no. 172, pp. 1–54, 2014.

[53] W. K. Hon, C. Millard, J. Singh, I. Walden, and J. Crowcroft, "Policy, legal and regulatory implications of a Europe-only cloud," *Int. J. Law Inf. Technol.*, vol. 24, no. 3, pp. 251–278, 2016.

[54] Trustwave, "2012 Global Security Report," Tech. Rep., 2012.

[55] Infocyte, "Breach Detection by the Numbers: Days, Weeks or Years?" 2017. [Online]. Available: https://www.infocyte.com/blog/2016/7/26/how-many-days-does-it-take-to-discover-a-breach-the-answer-may-shock-you

[56] Verizon, "Verizon Security Breach Report 2017," Tech. Rep., 2017.

[57] OWASP, "OWASP home page," 2017. [Online]. Available: https://www.owasp.org/index.php/Main{_}Page