A Management View of Security and Cloud Computing

Conference Paper · February 2018

CITATIONS
0

READS
47

4 authors, including:

Bob Duncan
University of Aberdeen
40 PUBLICATIONS **201** CITATIONS
SEE PROFILE

John D. Lamb
University of Aberdeen
33 PUBLICATIONS **142** CITATIONS
SEE PROFILE

A Management View of Security and Cloud Computing

Ndubuisi Anomelechi*, William Cooper†, Bob Duncan‡ John D. Lamb§
Business School, University of Aberdeen, UK
Emails: *n.anomelechi@abdn.ac.uk, †william.cooper@abdn.ac.uk, ‡robert.duncan@abdn.ac.uk, §j.d.lamb@abdn.ac.uk

***Abstract*—Cloud security is often seen as a technical problem. We argue that its solution needs both technical and management input. We find that cloud computing offers reliability and flexibility and its low cost makes it attractive, particularly to small and medium sized enterprises. We note that security technology must be adopted universally and often promptly. It requires both an organisational commitment and an individual commitment, which is most readily obtained if the technology places a low knowledge burden on users: that is, it is transparent or adds only a few, often-repeated, tasks. We note that providers have already achieved this in many cloud services. Organisations need clarity of what security is provided and who is responsible for breaches. They also need cloud providers to help them identify and recover from breaches. We consider why breaches have now become a hot topic, and provide a suggestion of how to mitigate the impact of these whilst meeting our management objectives and complying with the forthcoming EU General Data Protection Regulation.**

Keywords–Management goals; cloud security; EU GDPR.

I. Introduction

It is generally considered good practice for business organisations to embrace innovation, which may include disruptive technologies where appropriate [1], thereby doing things in what might be argued to be smarter ways. Such approaches may be adopted by sole trader start-up businesses to large scale multi-national corporations. While this all sounds entirely laudable and appears to make good business sense, there are some issues that may not be getting the level of attention they merit. The pressures on businesses to be efficient and effective, aligned with the adoption of innovative technology, raises issues that previously may not have been considered problematic. The potential for conflicting interests and flawed reasoning [2], is clearly demonstrated when it comes to the arena of cyber security and the way in which the importance of such may be viewed by businesses. This may be argued to be particularly relevant to the Small and Medium sized Enterprises (SME) sector and to the adoption and use of cloud computing.

The central element of concern is that too little attention may be paid to ensuring an adequate level of security is in place when businesses make use of cloud computing. Even where security elements have been made available, these may be compromised by the behaviour of individuals accessing the systems concerned. It has long been recognised that elements of interface design and ease of use are important when it comes to people effectively using computing provision. Human behaviour has been recognised as requiring ease of use more generally, for example by Drucker [3], who advised that removing difficulties would increase the likelihood of desired behaviour. The central message here would be that, if we wish cloud computing facilities to be accessed securely, we also need to consider issues of human behaviour and ensure we facilitate ease of use by removing potential difficulties that might detract from successful implementation of security elements.

In Section II, we consider how cloud is used and how it will impact on SMEs, and in Section III, we consider cloud security weaknesses. In Section IV, we address adoption and diffusion of innovations, and in Section V, we discuss the limitations of our management goals. In Section VI, we ask whether that is it, and discover some major issues that must be addressed. In Section VII, we consider how we might find a quick solution to this problem, and in Section VIII, we consider whether our ideas can meet the management goals we have set ourselves. Finally, in Section IX, we discuss our conclusions and future work.

II. Cloud computing

Cloud services and environments are variously defined. We note here the distinctions between Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [4] [5]. SaaS includes cloud file systems, web servers and database management. Any business user of cloud services is likely to use at least some of these. And businesses that use PaaS and IaaS may still use these separately for both convenience and security. We focus on these, because they are where cloud services must minimally provide security.

We note immediately that using a cloud system creates security issues that cannot be fully resolved by the enterprises served. When attackers breach a cloud system, there is nothing to stop them deleting the forensic trail. This means the enterprises cannot tell a regulator which files have been accessed, modified, deleted or exfiltrated. Secure encryption can mitigate this problem but still gives the enterprise no means to preserve data integrity other than keeping private backups of data. But this contradicts reasons for an SME choosing a Cloud Service Provider (CSP): to improve reliability without excessive cost.

We note that there may be further security responsibilities for both business users and CSPs. We focus on SMEs because they are most likely to choose cloud services without having the technical knowledge to deal with all the security issues that either a large entreprise or a CSP can.

A. Cloud Use: Advantages for SMEs

The potential gains for SMEs who choose to adopt cloud computing may be considered to include improvements in capacity, reliability and flexibility, reduced costs and faster time to market [6] [7]. The central benefits of the cloud approach may be considered to include low-cost availability, innovation power, expandability and environmental protection. Cloud computing enables the use of computing resources without the need to own them, which reduces the overhead costs for the businesses involved. This offers SMEs the potential for international capability, which would be likely to be more expensive using alternative means [8]. Cloud

use would potentially allow SMEs to compete at levels that previously would have been considered the domain of larger businesses. Research indicates that adoption of cloud services by SMEs relates to the potential advantage offered and that cloud computing may be of particular benefit to entrepreneurial ventures within developing nations [9].

B. Cloud Use: Adoption by SMEs

The adoption of cloud computing by SMEs is an area that has been highlighted as requiring further research. Entrepreneurial factors have been identified as likely to influence adoption of innovative technology, such as cloud computing. On a commercial basis, such innovative technology may be regarded as risky [10]. While cloud technologies may facilitate the development of SMEs, it may also open them to increased threats [11]. The cloud option may be considered to offer personalised and inexpensive computing facility on-demand [12] and to offer scalable capabilities [13], which is likely to be attractive to many within the SME sector. The scalability and mobility offered by the cloud option may offer greater levels of control over costs.

It is hardly surprising that such an option would be considered as a business asset and that those businesses for whom the minimisation of overhead costs, whilst maintaining cutting edge capability, is particularly valuable, would seek to utilise this facility. This is likely to be of particular relevance to SMEs, as their available budgets are likely to be lower than those of larger businesses. Supplier support may also be considered to be influential in the decision to adopt, with small businesses being more likely to rely on such external support [14]. Business concerns regarding the use of cloud computing may be considered to include lock-in, privacy and security, each of which may have a negative impact on the adoption of cloud computing by SMEs. The ease of use aspect of cloud computing is considered likely to impact the adoption level in SMEs, as has competitive pressure and the importance of relative advantage [11]. Cloud vendor lock-in may be exacerbated by the likely effort involved in moving to alternate providers. SMEs may be argued to be particularly vulnerable in this regard as they are less likely to have bargaining power [15]. The importance of the privacy element and the related issues of security and trust have been highlighted as important in the adoption process, with early adopters and prospectors emerging as more inclined to trust service providers. Security and privacy fears relate to the potential for public disclosure of sensitive information [16].

C. Security Issues

A major potential risk with cloud computing is that of security, with such elements as protocols, authentication processes and specific security standards requiring to be addressed. Thus, factors of concern for CSPs implementing security may be more technical.

Factors of concern to business entities when (rather than if) breaches occur include loss of productivity, (intellectual) property and business share, besides impact on customer experience/relationship and cost of recovery from an attack. Of utmost concern however will be business continuity. SMEs are more vulnerable to these as they are arguably less able to absorb the impacts of them than larger organisations. Whilst we argue that the CSP should assume responsibility for data integrity and recovery from breaches, obligations relating to the business continuity costs above remain the responsibility of the enterprises.

Partly owing to vendors' and developers' marketing strategies, new technology is often adopted on the assumption of complete sufficiency and security. Very little consideration tends to be given to what might happen in the event of a failure or breach. This gives rise to numerous risks related to the factors of concern. Such risks cannnot be mitigated without the adoption by each user organisation, including SMEs, of a robust system security and disaster recovery strategy.

The nature of cloud computing is such that the users data is stored in a relational data base using fixed schemata. This raises the likelihood of stability and security issues for users. These may relate to traditional security, availability and third party data control. Risks may be due to the cloud providers, law restrictions, hackers, or the equipment in use. Such issues may be addressed in a range of ways, including information-centric security, transparency regarding data transfer and disposal, and the use of encryption [8]. The concept of cloud security may be considered to encapsulate ways in which the infrastructure and the applications and data within it are protected. As with most situations interrelated elements are put at risk by the weakest link in their chain. With the use of cloud computing it may be argued that the cloud itself may be the weakest link, given that once this is penetrated the assailant may erase any traces of entry and proceed to access areas within the cloud at will. One of the central issues in relation to cloud security might be argued to be that of user behaviour. Perceived usefulness and perceived ease of use [17] may be considered important in relation to the use of technology and this may impact approaches taken to security provision and the effective use of such.

III. Cloud Security Weaknesses

From a technical and legal perspective, there are several aspects of security that businesses have to comply with. For much data there is a legal requirement to ensure privacy and confidentiality. From a business perspective availability, integrity and authenticity are important and corruption or misuse may create legal or professional problems, for example, with accounting systems. In addition there is an increasing requirement for businesses to be able to (i) detect and (ii) recover from breaches of security, in both cases as fast as possible.

We may note three features that are likely to be true of most ICT security technologies. First, to work, the technologies often need to be adopted by everyone within an organisation. Second, many of the people adopting the technology may see little reward from using it. Third, both managers and users may have limited understanding of the reasons for using it or even of what the technology does. This can be particularly problematic for SMEs who, in choosing to outsource security to a CSP, may employ no one with this understanding.

When enterprises, especially SMEs, use cloud computing we show that both enterprise and CSP will have to implement some aspects of security. Since no one security model will work in all cases, it is vital to pin down who is responsible for which aspects of security in the service level agreements.

A. Secure cloud computing

Arguably it is even more important to develop technologies for security that are also as transparent as possible. For example, where encryption or data integrity are required, ideally the implementation should be at the level of the file system (whether local, remote or cloud) and handled within the operating systems so that users can be minimally aware. For example, the file manager and applications should be able to open, close, modify and copy files without the user being aware, except perhaps if there is an opportunity to copy data from a secure system to an insecure one.

The first requirement, then, that we identify for secure cloud computing for enterprises is that what it provides must place as low a knowledge burden as possible on end users. In practice this usually means that CSPs need to offer security as part of the cloud service. Possibly a business could provide encryption before storing data on an insecure cloud service. But this is likely to be difficult without increasing the knowledge burden on users and so increasing risk. Better is if the CSP provides encryption software as part of the service. Better still is to provide both encryption software and encryption standard so that the business requires only keys and knowldge to decrypt its data, but is relieved of the knowledge burden by using the CSP. Maintaining data integrity, detecting breaches and recovering from them should be the responsibility of the CSP managing the data.

The second requirement is that CSPs should provide clarity on what security is being provided, why it is being provided and who is responsible for what aspects of security. We have found that enterprises, especially SMEs, often lack the technical knowledge to identify this for themselves. It is important, however, to identify whether the security provided includes each of encryption (and how secure), authentication and data integrity. It is important also to identify who is responsible for any security failure. It may be clear that a CSP is responsible for implementing encryption standards, providing software and maintaining data integrity. But it is important also to make sure enterprises, who seek a low knowledge burden, are aware of their responsibilities, for example in choosing passwords, preventing unauthorised use of secure keys and preventing release of information through, for example, email or usb memory devices. It is also important to identify who is legally and financially responsible for security breaches that are the fault of the CSP.

A third requirement is that enterprises need means of rapid recovery from security breaches. That is, they need to recognise that there is always a risk of security failure and they need (i) means to detect failure rapidly, (ii) methods to prevent further damage and (iii) means to recovery rapidly from failures. Typically, this requirement places burdens on both enterprise and CSP. The enterprise needs to have means to deal rapidly with problems arising because it failed in its responsibilities. CSPs need means such as those suggested in [5] of detecting, reporting and recovering from breaches in security or failures in data integrity in the CSP.

The human issue with cloud security, and the use of such by those in SMEs, may be argued to parallel the issues raised regarding the design of software and the design of the human-computer interface. There may be some conflict of interest in the design of software, which is attributable to the fact that those who build it are also those who design it. When this is related to customer expectations with regard to functionality, ease of use and the like we may find a noticeable mismatch. The way in which people interact with software may be argued to lie within the specialist domain of usability and if we look slightly deeper into the human-computer interaction, the domain of psychology Cooper ([18], p. 94) reminds us, "Successful interfaces are those that focus on the users goals ldots." If we consider the cloud security element from such a perspective we may conclude that the end user may in many instances be SMEs, for whom the primary motivation to use the cloud is that it offers business advantage at low cost. The likely expectation of such users might be considered to be that all security issues are taken care of for them within the package provided.

Essentially, the SME users may be considered in a similar way to most of those who drive cars. They wish to benefit from the independence and enhanced capability offered, but they are unlikely to wish to do all the required maintenance of the safety elements within the machine. However, while variations in capability and performance range may be considered acceptable, relative to the cost of purchase or lease, it is unlikely to be considered acceptable that safety should be compromised. The expectation is likely to be that those providing the artefact, which offers the enhanced capability, should take whatever steps are necessary to ensure safety is ensured on a fail-safe basis. For SMEs accessing cloud facilities this might be applied to security and the responsibility for dealing with any breaches of such in a fail-safe manner. For CSPs, the challenge might be to inform SME users that, like car drivers, they must take some responsibility.

IV. Adoption and diffusion of innovations

Getting users to adopt cloud services or to comply with security needs usually means persuading them to adopt some technology that implements these things. This is a management problem. There is management research going back 40 years or so on how technology gets adopted. None that we know of is on security; a little is on cloud adoption; much may be helpful.

Rogers [19] summarises much of the recent research on how technology diffusion occurs. The research identifies innovation as a process over a period of time. Usually it divides it into stages. For example, [20] identifies knowledge, persuasion, decision, implementation and confirmation stages while [21] identifies initiation, adoption, acceptance, routinisation and infusion. What matters here is not the particular stage model but that adoption takes place, usually individually, over time and various factors influence the speed and likelihood of transition between stages.

Davis et al [17] summarise two models that identify influencing factors. The first is a general theory of reasoned action model, which helps us identify intended behaviours. The second, the technology acceptance model adds the perceived usefulness and perceived ease of use. They find that perceived usefulness is the primary, and ease of use secondary the secondary, determinant in people's intention to use technology. Gallivan [21] looks at influencing factors when adoption is not voluntary and finds that strong and clear communication, high resource commitment and centralised planning and control contribute to better adoption, but, as usual, finds many individual factors also influence.

Walley and Amin [22] study customers rather than users and discuss their adoption of customer processing technology such as ATMs, petrol pumps and vending machines. They identify factors affecting customer choice to use the technology or not. The ones of interest are these. Customers adopt better if they repeat the use of the technology often. They prefer technology that presents a low variety of tasks. They are more likely to choose the technology if they value what it provides. They also discuss the extent to which customers find using the technology rewarding. The study is of interest because it identifies the factors likely to make voluntary adoption work.

In a review of organisational adoption of technology, Fichman [23] classifies types of technology by two dimensions. The first combines the extent of interdependency between users and the burden of knowledge required for adoption. The second looks at the locus: individual or organisational adoption. The examples of [22] are adopted individually and work best when knowledge burden is low. Most customer-processing technologies do not have interdependency between customers.

Security technology requires both the organisational locus of adoption and an individual locus: one user not adopting is enough for failure. So, we need at the same time high resource commitment and clear communication from management, and a choice of technology that users are very likely to adopt. Often the adoption is needed quickly and so factors slowing individual adoption are undesirable. It may be difficult, however, to make the technology rewarding to the user and many may fail to perceive its usefulness. That is, while the adoption is essentially organisational, it makes sense to regard users as like the customers of ATMs and petrol pumps. That is, organisations should prefer technology that requires little new knowledge and changes as little as possible, or even reduces, the tasks that the users must perform.

The ideal, then, is for managers to choose technologies that are transparent or nearly so. Applying this, we can see some of the reasons for the success and growth of cloud services. Not only do they meet organisational requirements for outsourced computing at a reasonable cost, but user adoption is ensured by making the services simple enough that users can be unaware they are using them. For example, when a CSP provides file storage, programs or database servers that are set up so that users cannot easily distinguish them from software on their computer, then adoption is easy and managing the process is largely limited to managers committing the resources to ensure staff computers are set up correctly.

V. Limitations and discussion

These requirements presents challenges for managers. They must be able to identify competently what they need from cloud providers. And they must be willing to provide the resource for it.

The most challenging problems for enterprises will be those where users have to increase their burden of knowledge or where security is dependent on technology that has a high degree of interdependency among users, especially when the users are outside of the organisation.

Passwords are a good example of where there may be little choice but to increase the knowledge of users. Passwords should have high information entropy, but most users perceive little value in learning this. It is possible to remove some of the burden from the users by testing and reporting entropy at the time a password is set and by rejecting weak passwords. But it remains important to teach users good ways to remember strong passwords. It may be impossible to prevent users using a good password on a secure system and also using it on a less secure one, such as when they use their work password on their social-media account.

The most common applications where there is a high interdependency between users are email and web browsers. These technologies, like most computing applications, were developed long before security standards. What makes them difficult to replace is that all parties must implement more or less the same standards. Secure email requires the co-operation of both sender and recipient and is usually impractical between organisations. Secure email within an organisation is possible, though may be expensive to make transparent. It is possible to remove email attachments, but without incentive to coöperate, users can bypass this kind of transparent security measure, for example by using web-based email. Possibly a secure email standard, but it is likely to take decades to get enough users to use it.

Web browsers can be easier to manage, because the security threat is largely external. Here again, managers are best advised to try to use a web browser with security features that require little or no knowledge from the user. But, once again, they leave open the possibility of having an intruder undetected in the system. For SMEs in particular, this presents a challenge, because they are likely not to have the expertise to deal with this. PaaS, where the web browser is provided by the CSP can improve matters. But if it is not easier to use the cloud-based web browser users are likely to see little reward from it and so find it simpler to use a web browser on their own device, which is much harder to secure.

VI. Is That It?

Well, under normal circumstances, having made researchers aware of the management issues as we see them, we could perhaps relax and wait for researchers to deliver, were it not for two very pertinent dark clouds on the horizon. The first is the Cloud Forensic Problem and the second is the forthcoming EU General Data Protection Regulation (GDPR), which comes into effect on 25th May 2018.

The first dark cloud—the Cloud Forensic Problem, can be best described as the elephant in the room. Many are aware that it exists, but few are willing to talk about it. It concerns the fundamental weakness in cloud computing, namely, that although cloud cyber security research has progressed significantly during the past decade on strengthening cloud security, there is one major and important issue that has yet to be resolved, namely that once an attacker finally breaches cloud defences, and become embedded within the system, they become an intruder for as long or as little time as they wish. Their primary goal will be to escalate privileges until they can seek out the forensic trail and obliterate all evidence of their presence within the system and how they were able to get there. Their desire is often to obtain a permanent foothold within the system, so that they can return again and again in order to harvest whatever they can get their hands on. Worst of all, there is absolutely nothing that existing cloud systems can do to prevent this from happening.

The second dark cloud we need to consider is the question of why cloud cyber security is becoming such a hot topic?

While there are many other pieces of data protection around that need to be complied with, the real reason this is becoming such a hot topic is that once the forthcoming EU GDPR [24], comes into effect, any company that is breached will be required, on pain of potentially massive punitive fines, to report exactly which records were accessed, modified, deleted or ex-filtrated from the company system. By potentially massive, punitive fines, we consider the larger of €20 million or 4% of Global Turnover, for every breach, to be a serious amount for any company, whether large or small.

If the cloud forensic trails are purged, this will leave the breached company with a potentially impossible task for them to comply with the strict reporting requirements of the legislation, namely that they must report every breach within 72 hours of discovery of the breach. Without the existence of forensic log data, it is doubtful whether any such company would be able to meet even this simplified deadline. If we consider that five years ago, the global average time between breach and discovery was 6 months [25], and that by last year, this had only improved to three weeks [26], it is clear that no matter how quickly a breach is discovered, if the forensic trail has been completely wiped, then a company will likely be unable to understand which records may have been seen, modified, tampered with, deleted or ex-filtrated from the system.

Once a breach is spotted, if due to the deletion of some or all of the forensic data by the intruder, the company will be unlikely to understand which records must be reported under the regulation. This will render them liable to a much higher range of possible penalties under the regulation.

The answer then, is a resounding no. The EU GDPR will kick in within the next few months time, and those companies who are not ready will have no excuse. This means that something must be done NOW, not months after the GDPR kicks in.

VII. How do we Find a Quick Solution to This Problem?

Given the fact that the Cloud Forensic Problem has not been solved, it is clear that the solution cannot be run on the existing cloud server, otherwise it will be exposed to the same problem as everything else. A simple approach would be to use the Duncan and Whittington approach [27]–[30], whereby the audit trail, the forensic trail and a log of all database commands made are safely stored in an immutable database held on a system external to the main cloud system. All existing logging would continue to be carried out on the existing cloud servers to encourage those attackers who succeed in becoming intruders might be lulled into a false sense of security.

Obviously, these covert logging systems will themselves become a target for attackers, but if they are configured as ultra high security servers with no direct web access, no other software running on them, and highly restricted access, together with a serious Intrusion Detection and Monitoring System, they will be a little more difficult to breach. These, it turn, can also be protected by another similar system, or indeed a chain of them, to provide a continuous self protecting loop, preferably with each system running on a different CSP offering.

VIII. Will this Meet the Criteria we have Identified as being Important from a Management Perspective?

We have prepared a list of the management goals we have identified in the paper, which we consider essential to meet in order to ensure a high level of take up of security systems within an organisation.

TABLE I. How our proposed Solution will Impact on Management Goals

	Management Goals Identified	Impact of our proposal
1.	Management need reliability at reasonable cost and possibly scalability	No adverse impact
2.	To avoid lock-in	No adverse impact
3.	Very low knowledge burden to use secure computing	No adverse impact
4.	Need to be able to protect data integrity, maintain privacy and detect breaches	Helps achieve goal
5.	Need clarity about who is responsible legally and financially for security and what is provided by CSPs	Ability to retain forensic trail helps with legal recourse
6.	Need to be able to recover rapidly from breaches of security or damage to data	Helps achieve goal
7.	Require security technology that is readily adopted by the whole organisation	Helps achieve goal
8.	Require a very low knowledge burden so that they get adoption by everyone individually	Helps achieve goal
9.	Need high resource commitment and clear communication from management	Not expensive to implement

As we can see, the proposed method of implementing this security approach is likely to have a minimum adverse impact on our management goals, and therefore is likely to stand a much higher chance of successful implementation.

IX. Conclusion and Future Work

From a management perspective, we consider it is very important that any security system meet our management goals in order to ensure a high level of uptake. We can see from TABLE I that we can implement the proposed methods to ensure a high level of security in cloud systems is achieved, which we can do while fulfilling our identified management goals. A useful bonus is that we can also comply with the EU GDPR and will have a useful means of ensuring rapid turnaround of our business continuity plans.

This means that there will be a higher likelihood that such an approach will be successfully implemented, especially by SMEs. This will also ensure that in the event of a systems breach, it will be possible to fully comply with the GDPR reporting requirements. Also, the ability to fully recover from such an attack will enhance any business continuity plan, ensuring a faster and more full recovery than would otherwise be possible.

In future work, we propose the development of a use case model to test how well a company might recover from an attack whilst still remaining compliant with the GDPR. We believe this can provide a useful means of ensuring many SMEs, who would otherwise fall foul of the new regulation.

References

[1] J. Tidd, J. Bessant, and K. Pavitt, Managing innovation. Hoboken. NJ: Wiley, 2013.

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

[3] P. Drucker, Management Challenges for the 21st Century, ser. Management Challenges for the 21st Century. HarperCollins, 1999, no. pt. 794.

[4] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST, Tech. Rep., 2011. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf [Last accessed: November 2017]

[5] G. Weir and A. Aßmuth, "Strategies for Intrusion Monitoring in Cloud Services," Cloud Computing 2017: The Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, 2017, pp. 1–5.

[6] M. Miller, Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online. Que Publishing, 2008.

[7] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud computing - The business perspective," Decision Support Systems, vol. 51, no. 1, 2011, pp. 176–189.

[8] K. Gai and S. Li, "Towards Cloud Computing: A Literature Review on Cloud Computing and Its Development Trends," 2012 Fourth International Conference on Multimedia Information Networking and Security, 2012, pp. 142–146.

[9] S. Greengard, "Cloud computing and developing nations," Communications of the ACM, vol. 53, no. 5, 2010, pp. 18–20.

[10] V. Ratten, "Entrepreneurial and ethical adoption behaviour of cloud computing," Journal of High Technology Management Research, vol. 23, no. 2, 2012, pp. 155–164.

[11] Y. Alshamaila, S. Papagiannidis, and F. Li, "Cloud computing adoption by SMEs in the north east of England," Journal of Enterprise Information Management, vol. 26, no. 3, 2013, pp. 250–275.

[12] L. Wang, G. Von Laszewski, A. Younge, X. He, M. Kunze, J. Tao, and C. Fu, "Cloud computing: A perspective study," New Generation Computing, vol. 28, no. 2, 2010, pp. 137–146.

[13] D. C. Plummer, T. J. Bittman, T. Austin, D. W. Cearley, and D. M. Smith, "Cloud Computing : Defining and Describing an Emerging Phenomenon," Gartner Research, vol. G00156220, no. June, 2008, pp. 1–9.

[14] W. DeLone, "Determinants of Success for Computer Usage in Small Business," MIS Quarterly, vol. 12, no. 1, 1988, pp. 51–61.

[15] P. K. Ross and M. Blumenstein, "Cloud computing as a facilitator of SME entrepreneurship," Technology Analysis \& Strategic Management, vol. 27, no. 1, 2015, pp. 87–101.

[16] M. Stern-Peltz and J. Armitage, "IT Firms Lose billions after NSA Scandal Exposed by Whistleblower Edward Snowden," 2013. [Online]. Available: http://www.independent.co.uk/life-style/gadgets-and-tech/news/it-firms-lose-billions-after-nsa-scandal-exposed-by-whistleblower-\\edward-snowden-9028599.html [Last accessed: November 2017]

[17] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models Author," Management Science, vol. 35, no. 8, 1989, pp. 982–1003.

[18] A. Cooper, About Face: The Essentials of User Interface Design. IDG Books Worldwide, Inc., 1995.

[19] E. M. Rogers, Diffusion of Innovations, 5th ed. New York: Free Press, 2003.

[20] E. M. Rogers, Diffusion of Innovations, 3rd ed. London: The Free Press, 1983.

[21] M. J. Gallivan, "Organizational adoption and assimilation of complex technological innovations," ACM SIGMIS Database, vol. 32, no. 3, 2001, p. 51.

[22] P. Walley and V. Amin, "Automation in a Customer Contact Environment," International Journal of Operations & Production Management, vol. 14, no. 5, 1994, pp. 86–100.

[23] R. G. Fichman, "Information Technology Diffusion: A Review of Empirical Research," Proceedings of the Thirteenth International Conference on Information Systems ({ICIS} '92), 1992, pp. 195–206.

[24] EU, "EU General Data Protection Regulation," 2017. [Online]. Available: http://www.eugdpr.org/ [Last accessed: November 2017]

[25] Verizon, "2012 Data Breach Investigations Report," Verizon, Tech. Rep., 2012.

[26] Verizon, "2016 Verizon Data Breach Report," Tech. Rep., 2016.

[27] B. Duncan and M. Whittington, "Enhancing Cloud Security and Privacy: The Power and the Weakness of the Audit Trail," in Cloud Computing 2016: The Seventh International Conference on Cloud Computing, GRIDs, and Virtualization, no. April. Rome: IEEE, 2016, pp. 125–130.

[28] B. Duncan and M. Whittington, "Cloud cyber-security: Empowering the audit trail," International Journal on Advances in Security, vol. 9, no. 3 & 4, 2016, pp. 169–183.

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

[30] B. Duncan and M. Whittington, "Creating and Configuring an Immutable Database for Secure Cloud Audit Trail and System Logging," International Journal On Advances in Security, no. 3&4, 2017.