STRATUS: Towards Returning Data Control to Cloud Users

Ryan K. L. Ko[1(✉)], Giovanni Russello[2], Richard Nelson[1], Shaoning Pang[3], Aloysius Cheang[4], Gill Dobbie[2], Abdolhossein Sarrafzadeh[3], Sivadon Chaisiri[1], Muhammad Rizwan Asghar[2], and Geoffrey Holmes[1]

[1] University of Waikato, Hamilton 3240, New Zealand,
[2] University of Auckland, Auckland 1142, New Zealand
[3] Unitec Institute of Technology, Auckland 1025, New Zealand
[4] Cloud Security Alliance (Asia Pacific), Singapore, 247672
Contact Email: ryan@waikato.ac.nz
Project home page: https://stratus.org.nz

Abstract. When we upload or create data into the cloud or the web, we immediately lose control of our data. Most of the time, we will not know where the data will be stored, or how many copies of our files are there. Worse, we are unable to know and stop malicious insiders from accessing the possibly sensitive data. Despite being transferred across and within clouds over encrypted channels, data often has to be decrypted within the database for it to be processed. Exposing the data at some point in the cloud to a few privileged users is undoubtedly a vendor-centric approach, and hinges on the trust relationships data owners have with their cloud service providers. A recent example of the abuse of the trust relationship is the high-profile Edward Snowden case. In this paper, we propose a user-centric approach which returns data control to the data owners – empowering users with data provenance, transparency and auditability, homomorphic encryption, situation awareness, revocation, attribution and data resilience. We also cover key elements of the concept of user data control. Finally, we introduce how we attempt to address these issues via the New Zealand Ministry of Business Innovation and Employment (MBIE)-funded STRATUS (Security Technologies Returning Accountability, Trust and User-centric Services in the Cloud) research project.

Keywords: Cloud Security; Cloud Computing; User Data Control; User-centric Security; Data Provenance; Homomorphic Encryption; Situation Awareness; Data Resiliency

1 Rising Cyber Security Incidents: The Case for User Data Control

From the Apple iCloud celebrity nude photo leaks [1], to the abuse of children's photographs on social networking services (e.g. Flickr and Facebook) for use of explicit sites [2], to the recent adultery website Ashley Madison user information

leak [3], we are regularly witnessing a serious problem: *the inability for data owners to help themselves in cyber security breeches situations.*

Underlying this problem, is a serious deficiency we are observing with the current state of the cyber security industry: *the inability for data owners to control their data.* When one gets compromised in a cyber security situation, one usually has no idea how to proceed to understand the situation, analyse the evidence and perhaps solve the situation (e.g. attribute and present compelling evidence against the perpetuator of the attack).

1.1 Lack of Ability Stemming From Lack of Data Control

Looking deeper into the gap of 'inability to help themselves', we notice the root of the issue is in the lack of control over the data they own, especially in the cloud or simply over the web. Sometimes, users do not even realise that their photographs taken from their mobile phone's camera are uploaded instantly onto public cloud storage, even though they may not have wanted those specific photos to go onto the cloud (despite agreeing to the terms and conditions of the application installation).

When we survey the landscape of cyber security tools, from the commonly known ones such as anti-malware and firewalls, to the sophisticated vulnerability scanners and penetration testing tools, none of them are built with the purpose of empowering the users to comprehensively help themselves in controlling their data's whereabouts and privacy in hacking incidents. There is no reversal or recourse.

1.2 Everyday Scenarios Demonstrating Users' Lack of Data Control

In 2010, a 27-year-old Google site reliability engineer was caught spying on teenagers on the GTalk service [4]. He abused his privileged administrator rights and was only found out after the parents of a teenager reported him. According to the Google, the extend of the damage or possible abuse is unknown, as there is no technology tracking the evolution of data from a data-centric point of view. There was also no technology which could alert the affected teenagers about the unauthorised access from the backend of the cloud service.

With no real accountability of administrators' rights over the access of clients' data, many more situations like these potentially happen on a daily basis in (both public and private) clouds utilised by businesses around the world. The sole reliance on the trust and reputation of a cloud service provider and their employees is neither a strong nor sustainable way forward for the cloud computing industry.

2 Elements of User Data Control and Related Work

Returning control of data to users is a 'holy grail' of cloud security research as it addresses trust tensions and accountability issues inherent in storing and processing of proprietary data in cloud environments.

Solving this 'holy grail' will also carve out a niche in security technologies around user control over their data through four proposed elements:

- **Element 1** – Transparency and auditability of data,
- **Element 2** – Privacy of data during processing and storing,
- **Element 3** – Detection and revocation of malicious actions, and
- **Element 4** – Resiliency and rapid recovery from untoward events.

Without all elements, the user cannot gain full control over their data, thus both technical and compliance aspects around these four elements will need to be addressed. We propose STRATUS (short for 'Security Technologies Returning Accountability, Trust and User-centric Services in the Cloud'), which will address the four elements, i.e. Research Aims (RAs), each focusing on one of these dimensions of user control of data. More details of STRATUS will be covered in Section 3 – Proposed Methodology. Before we delve into the STRATUS approach, we will need to understand in-depth, the elements of user data control in cloud environments. We will now provide a brief overview of the four main elements.

2.1 Element 1: Transparency and Auditability of Data Activities

Element 1 enables cloud users to trace and reconstruct data provenance, i.e. "what's happened to their data" behind the scenes. Technologies enabling cloud stakeholders to keep track of the provenance (i.e. derivation history) of their data will be built – enabling them to know if malicious insiders have accessed their data, or whether the users have leaked their important data to foreign systems.

Element 1 also covers the crucial governance aspects of cloud data and links technical implementations with auditing and compliance guidelines, standards, or regulations (e.g. CSA CCM [5], ISO27001 [6], PCI DSS [7]). From the global security perspective, Moreover, Element 1 addresses the difficulty in tracking criminals who use evasion and encryption techniques to mask their digital trails and activities.

2.2 Element 2: Protection of Privacy of Data During Processing and Storing

This Element addresses the issue of how users can ensure their data privacy in clouds, without compromising search, functionality or analytical capability. Currently, encrypted data cannot be processed or utilised meaningfully by computing systems. Element 2 aims to overcome this by enabling encrypted data to be utilised by cloud servers without revealing private data to the cloud system administrators – thereby preserving privacy of data without compromising the data utility.

2.3 Element 3: Immediate Detection and Revocation of Malicious Actions

This Element has three objectives:

1. Providing 'situational awareness' tools enabling cloud stakeholders to have real-time awareness of their data status.
2. New techniques that instantly reveal cloud software vulnerabilities and remedy them 'on the fly'. Current cloud technologies are protected by traditional but unsustainable methods (i.e. malware scanning using rule-based techniques).
3. Capabilities to attribute threat sources and revoke anomalous actions, i.e. achieving true control of one's data.

2.4 Element 4: Resiliency and Rapid Recovery from Untoward Events

Element 4's main objective is to enable rapid recovery from untoward incidents, malicious attacks and acts of nature. Due to a lack of work [8, 9] devoted to defending business data from malicious attacks and from large scale disasters, the following techniques will be developed: (1) techniques building resiliency into services; (2) decentralised cloud storage, and (3) multi-cloud based disaster recovery techniques. Tools that can be used in clouds to protect the availability of data through a decentralised solution must be developed. The solution should enable back-ups to be automatically replicated at multiple independent sites in near real-time.

3 Proposed Methodology

As mentioned, the proposed STRATUS approach will be based on addressing the above four key elements of user data control in clouds. STRATUS will create a platform of novel user-centric cloud security technologies that can be used by New Zealand companies to differentiate their products and services in global markets.

Our over-arching research goal therefore is to create first-in-the-world to export cloud security technologies that enable users to be aware of, assess and manage security events themselves. The research programme to deliver this comprises four 'Research Aims' (RAs), which are listed below. Each RA comprises one to three projects, which represent more specific technology developments as follows:

3.1 RA1: Transparency and Auditability of Data Activities in Clouds

Project 1: Tracking and Reconstruction of Data Provenance

Aims – This project enables cloud users to know data provenance, or "what has happened to their data" behind the scenes. Project 1 builds on Ko's research in cloud data provenance [10–14]. We will develop provenance tracking and reconstruction techniques to support data incident investigations. We will also build technologies that automate data-centric evidence acquisition and data forensics tasks required in RA3.

Gaps & Scientific Principles Addressed – The project addresses cloud data provenance and transparency of data activities. There is currently no elegant solution to this problem [10] due to the following challenging scientific problems. First, current cloud monitoring tools [15–17] (e.g. HyTrust [17]) only monitor utilisation and performance, and overlook data flow in clouds. Second, while most clouds adopt file-integrity checking systems (FICS) (e.g. TripWire [18]) to detect file intrusions, they do not track the history of changes and only report the last change [19]. Third, existing data provenance techniques [10–12] are not user-centric but vendor-centric [20]. There is also an absence of real-time provenance and timeline reconstruction techniques to piece back data activities and threat sources.

Methodology – We will focus on investigating research questions and developing proofs-of-concept using continuous hypothesis testing [21] within the University of Waikato (UoW)'s Cloud8 (large-scale cloud test-bed): (1) redesigning cloud systems to embed provenance records in their metadata (2) design, patent and implement cloud data access protocols (3) building data-centric logging, provenance mining, and reconstruction mechanisms that collect provenance not only within, but also outside clouds. The inventions will be verified against our commercial collaborators. Then, they will be validated against real-life scenarios and infrastructures provided by commercial collaborators. Finally, we will create export advantages by building export-ready cloud data provenance services.

Project 2: Data Governance and Accountability in Clouds

Aims – This project complements Projects 1 and 7, as it covers the cloud data governance and links technical implementations with auditing guidelines and compliance regulations. This builds on the experience of two existing CSA New Zealand Chapters research: (1) NZISM controls-mapping with unified security and governance controls (e.g. ISO 27001/2, COBIT, PCI-DSS, NIST800-53, BITS) (2) privacy requirements for data governance in New Zealand.

Gaps & Scientific Principles Addressed – This project primarily addresses the cross-border policy alignment and technology-to-policy alignment for innovations invented in the four RAs. The governance controls of cloud service providers do not support data sovereignty rights of cloud users [22–24]. Existing standards (ISO 27001, COBIT, ISO 38500, NIST 800-53, NZISM, PCI-DSS) do not offer controls that can accredit and audit cloud user cloud architecture for data governance. Governments have highlighted this pressing need in various documents [25, 26].

Methodology – Comparative analyses of standards, legal controls and best practices will be conducted. Controls from our analysis will be documented according to the Deming (Plan-Do-Check-Act: PDCA) Cycle [27] as a first draft. Next, we will have two consultation rounds with industry (e.g. NZICT) and New Zealand Government (i.e. DIA, NZTE, ATEED). The unified framework draft will be accomplished. This draft will be sent to ISO committees, government and industry for review. The controls' validity will be tested by integration with software created by all RAs. Then, we will focus on publishing recommendations into international standardisation bodies (e.g. ISO, ITU-T). Finally, Cloud Security Alliance (CSA) (which is one of STRATUS research collaborators) will link up commercial collaborators to CSA corporate members, establishing a first-mover advantage and global market.

3.2 RA2: Protection of Privacy of Data During Processing and Storing

Project 3: Secure Information Retrieval / Encrypted Search

Aims – This project will first provide data centre owners with new storage tools that allows search operations on encrypted data and provide stakeholders tools for statistical analysis and testing of cloud data while preserving privacy at a granular level. This project builds on the University of Auckland's current work [28]. We will combine previous results on proxy-encryption for simple search operations in a multiuser setting [29–31] with our latest work [28, 32–38] supporting complex matching operations and indexing extensions.

Gaps & Scientific Principles Addressed – The main scientific principles addressed are cryptographic schemes which protect data confidentiality while supporting search operations on encrypted data. Current solutions either (1) support only simple queries based on equality matches (e.g. "Name=John") but not complex queries based on ranges (e.g. 18<Age<65), or (2) require users to share keys, complicating key management, i.e. requiring regular key regeneration. Related works have only partially solved these two issues. For example, single-user searchable encryption schemes [39–41] only work well for single users, while semi-fledged multi-user schemes [42–45] force other users to only perform 'read' operations if a user 'writes'. More recently, full-fledged multi-user schemes allow multiple users to 'write' and 'read' without sharing keys [29–31] but only support keyword-based searches. We aim to support both complex queries and do not require users to share keys.

Methodology – We will define security requirements, business cases, and create partial prototypes based on our previous research [28]. Next, we will deploy a fully working mechanism and study indexing techniques enabling lower latencies for data retrieval. Our commercial collaborators will provide requirements, business cases and access to dedicated hardware. Indexing will be integrated to the search mechanism; a tool which minimises data exposure while doing fast indexing will be implemented. Then, we will integrate and validate on thin-clients with constrained resources (e.g. battery), and implement client-side

crypto schemes. Finally, search optimisation and parallel execution extensions will be built.

Project 4: Efficient Privacy and Utility Preserving Encryption

Aims – This project attempts to achieve an efficient, practical method for a major scientific breakthrough: Gentry's fully homomorphic encryption (FHE) [46, 47]. FHE allows computers to process data without the need to decrypt them, thereby solving all cloud data privacy concerns. However, FHE is currently inefficient and impractical ($\sim$ 15 mins/1 kilobyte) [47]. Therefore, there are opportunities to introduce innovation that gives New Zealand cloud providers a competitive advantage. We will focus on implementing practical homomorphic cryptographic mechanisms for supporting meaningful computation on encrypted data, e.g. statistical functions.

Gaps & Scientific Principles Addressed – FHE's drawback is that it requires huge ciphertext and cryptographic material that is not practical with today's computational power. Recently, small optimisations have been proposed [48, 49]. Although these optimisations require smaller ciphertexts to work they are still far from being practical in a cloud environment serving large amount of users. Close to our approach is [47]. However, it is not ideal for corporates with numerous employees requiring access to the encrypted service. Pragmatically, our solutions will adopt partial homomorphic encryption (PHE), which supports a subset of well-defined operations. PHE is efficient in term of computation time. Furthermore, PHE can provide the same level of security as FHE. Our idea is that combining several PHE solutions supporting a range of operations can provide enough computation power to be used in several sectors including finance, healthcare and government. We will build from our previous work based on proxy encryption and Elgamal crypto blocks [29, 32, 33, 38].

Methodology – We will define security and functional requirements with business requirements and study related cryptographic schemes. A prototype with different functions will be implemented, tested and evaluated. Then, the prototypes will be optimised and delivered as SaaS products. Next, we will implement the support of thin-clients and provide a platform for integrating different providers' services.

3.3 RA3. Awareness and Response to Anomalous Data Activities

Project 5: Real-time Situational Awareness

Aims – This project will draw from UoW's decade of machine learning (ML) experience (i.e. Weka [50]) , and passive network measurement and anomaly detection expertise [51–54] to develop new techniques enabling cloud stakeholders with real-time situational awareness (SA) of their data. SA is a top priority in several defence organizations globally [55], as there is currently a lack of techniques for instant identification of trouble spots in the cloud [56]. We will apply ML techniques to develop actionable insights to improve SA.

Gaps & Scientific Principles Addressed – The ability to detect and report anomalous actions is the basis for notifying cloud stakeholders abnormal data provenance behaviour [57]. This permits active corrective actions rather than reactive. Cloud systems are also live and dynamic [10] – instances are live or shut down in ad hoc fashion. Therefore, accurately detecting and reporting abnormal behaviours from large-scale measurements with zero false positives is an open problem. SA needs to perform well with large data volumes, differentiate between harmless and malicious anomalies, and detect covert or stealthy information flows.

Methodology – Anomalous events will be identified and classified. Algorithms for effective detection over large datasets will also be developed. Next, the classifications and algorithms are combined to test against commercial collaborators and experimental findings from RA1. Finally, we will build export-ready cloud SA services integrated with the STRATUS platform.

Project 6: Effective Cloud Vulnerability Scanning

Aims – This project will develop new techniques to instantly reveal and remediate from cloud security vulnerabilities. Virtualization in clouds increase scale and utilization of infrastructures but brings about new complexities and vulnerabilities. Currently, clouds are protected by traditional methods designed for single machines (i.e. malware scanning using rule-based techniques, firewalls); these are not sustainable. Our work builds on Ko's existing research on Cloud failures [58] and his collaborative research with Bell Labs on cloud reliability.

Gaps & Scientific Principles Addressed – This project will create a cloud vulnerability scanning kit which will enable security consultants, cloud service provider and cloud user (e.g. SaaS companies) to identify and recommend remedies for both software [59, 60] and network vulnerabilities [61] efficiently. In the area of networks, work on addressing Internet Protocol version 6 (IPv6)-related vulnerabilties (e.g. firewalls deployed for IPv4 only, transiting from IPv4 to IPv6) are lacking . Existing work include the SecureCloud [62], RedShield [63], software fuzzers [59, 60] and the THC IPv6 vulnerability scanning toolkit [61]. However, they are not ready for clouds' live and dynamic nature [11]. The main challenges stem from the widespread usage of virtualisation and software defined networks in clouds.

Methodology – We will automate fast and efficient malware analysis that traces back and attributes sources to empower law enforcement and prevent future outbreaks. Next, we will focus on classifying vulnerability types, and develop a suite of proofs-of-concept for each vulnerability type. Then, we will focus on tool productisation. Finally, we will build cloud vulnerability scanning suites for commercial collaborators.

Project 7: Attribution and Revocation of Actions

Aims – This project builds on data from Projects 1, 2 and 5. Cloud stakeholders would have abilities to identify the actors or malware behind each cloud data anomaly, and revoke malicious actions, i.e. achieving true control of one's data. We will also develop the ability to cyber "fingerprint" attackers through identification and detection of their behaviours, and techniques. This automates repetitive tasks such as evidence collation, reducing workload of investigators.

Gaps & Scientific Principles Addressed – The principles addressed are identity management, access control [64–66], and revocation policies [67, 68]. Related work such as sticky policies, EnCoRe and revocation schemes often run into scale and latency problems [67, 69]. We aim to overcome these limitations to achieve near real-time control and policy implementation.

Methodology – We will focus on: (1) classification of identity types of all granularities within cloud systems, (2) development of access control policies which adhere to international auditing regulations identified by Project 2, and (3) building of proofs-of-concepts of attribution techniques. Our attribution techniques will be validated against our New Zealand commercial collaborators.

3.4 RA4. Resiliency and Recovery of Data

Project 8: Rapid Disaster Recovery (DR) Infrastructure

Aims – This project will develop capabilities for efficient data protection and rapid recovery from untoward incidents, malicious attacks and acts of nature. This project builds on prior work on decentralised network federation systems [70] at Unitec's Centre for Computational Intelligence for Cyber-Security.

Gaps & Scientific Principles Addressed – The project primarily addresses the challenge of business continuity via data resiliency and recovery mechanisms [8]. Applications must rapidly come back online after a failure occurs to minimise losses. Two existing mechanisms: (1) network reconfiguration [9, 71, 72], and (2) virtual machine migration or cloning [73] operate at service or platform layer but none connects DR to the infrastructure layer or consider geographic and network-topological locations. Citrix [73] and Pokharel et al. [74] considered secondary cloud infrastructures for disaster recovery but they require extra physical sites, i.e. higher costs. As such, we will (1) build resiliency into services (2) create decentralized cloud storage techniques and (3) create multi-cloud based disaster recovery techniques.

Methodology – We will build resilient services focusing on business continuity. Then, we will develop automated data distribution techniques that decentralises data storage and achieves cost reduction. Next, we will setup an industry-grade disaster recovery infrastructure, enable seamless integration of existing clouds as part of single wide-area resource leasing federation and a structured peer-to-peer routing method.

4 Opportunities for Cloud Security: A Technology Platform with Multiple Applications

STRATUS not only has the potential to achieve the elements of data control, but also establish, maintain and continually develop a wide portfolio of user-centric cloud security technologies.

Some examples include the development of user-centric data provenance tracking tools, which can inform the whereabouts of data to their owners. Other examples include a fully homomorphic range of cloud applications for the healthcare, banking and government sectors – reducing the reliance and risk trusting of cloud computing privileged system administrators.

The ability to know about users' data also empowers us with the potential ability to revocate and attribute malicious activities, giving full control of data to users.

This mix of user-centric cloud technologies, skills and resources will comprise the STRATUS platform. Our goal is for the combination of successful, real world 'proofs-of-concept' with supporting resources to ensure easy access for exporters and domestic users alike.

5 Concluding Remarks

In this position paper, we presented STRATUS, a New Zealand cyber security research project focusing on empowering users with control over their data in third party environments such as the cloud. We will create a platform of novel security tools, techniques and capabilities which return control of data to cloud computing users. Such innovations empowering users to have data control offer opportunities for companies across the cloud computing value system.

We proposed four elements of security technologies around user control over their data including (1) transparency and auditability of data, (2) privacy of data during processing and storing, (3) detection and revocation of malicious actions, and (4) resiliency and rapid recovery from untoward events. When all elements are addressed, we will return data control to users. It is our proposition that for the cloud to be a truly trustable service, cloud service providers must not be data owners but data processors.

Acknowledgements

This research is supported by STRATUS (Security Technologies Returning Accountability, Trust and User-Centric Services in the Cloud) (https://stratus.org.nz), a science investment project funded by the New Zealand Ministry of Business, Innovation and Employment (MBIE).

References

1. Goldman, D., Pagliery, J., Segall, L. How celebrities' nude photos get leaked. http://money.cnn.com/2014/09/01/technology/celebrity-nude-photos/index.html?iid=EL. CNN Money. Accessed 7 September 2015 (2014)
2. Quenqua, D. Guardians of Their Smiles. http://www.nytimes.com/2009/10/25/fashion/25facebook.html. The New York Times. Accessed 7 September 2015 (2009)
3. Isidore, C., Goldman, D. Ashley Madison hackers post millions of customer names. http://money.cnn.com/2015/08/18/technology/ashley-madison-data-dump/. CNN Money. Accessed 7 September 2015 (2015)
4. Chen, A. GCreep: Google Engineer Stalked Teens, Spied on Chats. http://gawker.com/5637234/gcreep-google-engineer-stalked-teens-spied-on-chats. GAWKER. Accessed 7 September 2015 (2010)
5. Cloud Controls Matrix v3.0 Info Sheet. https://downloads.cloudsecurityalliance.org/initiatives/ccm/CCM_v3_Info_Sheet.pdf Accessed 7 September 2015 (2013)
6. Calder, A.: Information Security Based on ISO 27001/ISO 1779: A Management Guide. Van Haren Publishing (2006)
7. Morse, E. A., Raval, V.: PCI DSS: Payment card industry data security standards in context. Computer Law & Security Review. 24(6), 540–554 (2008).
8. Alhazmi, O. H., Malaiya, Y. K.: Assessing Disaster Recovery Alternatives: On-Site, Colocation or Cloud. The IEEE 23rd International Symposium on Software Reliability Engineering Workshops (ISSREW). 19–20 (2012)
9. Wood, T., Cecchet, E., Ramakrishnan, K. K., Shenoy, P., Van der Merwe, J., Venkataramani, A.: Disaster recovery as a cloud service: economic benefits & deployment challenges. Proc. 2nd USENIX Conference on Hot Topics in Cloud Computing (HotCloud'10). Berkeley, CA, USA (2010)
10. Ko, R. K. L., Jagadpramana, P., Mowbray, M. *et al.*: TrustCloud - A Framework for Accountability and Trust in Cloud Computing. IEEE 2nd Cloud Forum for Practitioners (IEEE ICFP 2011). Washington DC, USA, 1–5 (2011)
11. Ko, R. K. L., Kirchberg, M., Lee, B. S.: From system-centric to data-centric logging-Accountability, trust & security in cloud computing. Defense Science Research Conference and Expo (DSR). 1–4 (2011)
12. Ko, R. K. L., Lee, B. S., Pearson, S.: Towards Achieving Accountability, Auditability and Trust in Cloud Computing. International workshop on Cloud Computing: Architecture, Algorithms and Applications (CloudComp2011). Kochi, India, 5–18 (2011)
13. Tan, Y. S., Ko, R. K. L., Jagadpramana, P., et al.: Tracking of Data Leaving the Cloud. Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE 11th International Conference on. 137–144 (2012)
14. Zhang, O. Q., Ko, R. K. L., Kirchberg, M., Suen, C. H., Jagadpramana, P., Lee, B. S.: How to Track Your Data: Rule-Based Data Provenance Tracing Algorithms. Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. 1429–1437 (2012)
15. RACKSPACE Cloud Monitoring. http://www.rackspace.com/cloud/monitoring/. Accessed 7 September 2015 (2015)
16. vRealize Hyperic. http://www.vmware.com/products/vrealize-hyperic/. Accessed 7 September 2015 (2015)

17. HyTrust Products. http://www.hytrust.com/products/. Accessed 7 September 2015 (2015)
18. Kim, G. H., Spafford, E. H..: Experiences with tripwire: Using integrity checkers for intrusion detection. Purdue University Technical Reports. (1994)
19. Ko, R. K. L., Jagadpramana, P., Lee, B. S.: Flogger: A file-centric logger for monitoring file access and transfers within cloud computing environments. Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on. 765–771 (2011)
20. Ko R. K. L., Goh G., Mather T., Jaini S., Lim R.: Cloud Consumer Advocacy Questionnaire and Information Survey Results (CCAQIS) v1.0. Cloud Security Alliance (2011)
21. Popper, K. R.: The logic of scientific discovery: Routledge. Taylor and Francis Group. (1959)
22. American Bar Association.: Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet. The Business Lawyer. 55, 1801–1946 (2000)
23. Bradshaw, S., Millard, C., Walden, I. : Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services. International Journal of Law & Information Technology. 19, 187–223 (2011)
24. Hon, W. K., Millard, C., Walden, I.: Negotiating Cloud Contracts - Looking at Clouds from Both Sides Now. Queen Mary School of Law Legal Studies Research Paper. (2012)
25. Regulation (EC) No 45/2001 of The European Parliament and of The Council. The European Parliament (2001)
26. Government of New Zealand. Summary Comparison with Overseas Jurisdictions. http://www.consumeraffairs.govt.nz/legislation-policy/policy-reports-and-papers/discussion-papers/international-comparison-discussion-paper/part-2-summary-comparison-with-overseas-jurisdictions/. Accessed 7 September 2015 (2010)
27. Susanto, H., Almunawar, M. N., Tuan, Y. C.: Information security management system standards: A comparative study of the big five. (2011)
28. Eyers, D., Russello, G.: Toward flexible and unified security policies enforceable within the Cloud. 13th International IFIP Conference on Distributed Applications and Interoperable Systems (DAIS 13). Florence, Italy (2013)
29. Dong, C., Russello, G., Dulay, N.: Shared and searchable encrypted data for untrusted servers. Journal of Computer Security, 19, 367–397 (2011)
30. Russello, G., Dong, C., Dulay, N., Chaudron, M. R. V., Steen, M. van: Encrypted Shared Data Spaces. COORDINATION (2008)
31. Russello, G., Dong, C., Dulay, N., Chaudron, M. R. V., Steen, M. van: Providing data confidentiality against malicious hosts in Shared Data Spaces, Sci. Comput. Program. 75, 426–439 (2010)
32. Asghar, M. R., Ion, M., Russello, G., Crispo, B.: ESPOON: Enforcing Encrypted Security Policies in Outsourced Environments. ARES. (2011)
33. Asghar, M. R., Ion, M., Russello, G., Crispo, B. Securing Data Provenance in the Cloud. iNetSeC. (2011)
34. Ion, M., Russello, G., Crispo, B.: An implementation of event and filter confidentiality in pub/sub systems and its application to e-health. the ACM Conference on Computer and Communications Security. (2010)
35. Ion, M., Russello, G., Crispo, B.: Providing Confidentiality in Content-based Publish/subscribe Systems. SECRYPT. (2010)

36. Ion, M., Russello, G., Crispo, B.: Supporting Publication and Subscription Confidentiality in Pub/Sub Networks. SecureComm. (2010)
37. Ion, M., Russello, G., Crispo, B.: Enforcing Multi-user Access Policies to Encrypted Cloud Databases. POLICY. (2011)
38. Ion, M., Russello, G., Crispo, B.: Design and implementation of a confidentiality and access control solution for publish/subscribe systems. Computer Networks. 56, 2014–2037, (2012)
39. Bösch, C., Brinkman, R., Hartel, P. H., Jonker, W.: Conjunctive Wildcard Search over Encrypted Data. Secure Data Management. (2011)
40. Popa, R. A., Redfield, C. M. S., Zeldovich N., Balakrishnan, H.: CryptDB: protecting confidentiality with encrypted query processing. SOSP. (2011)
41. Song, D. X., Wagner, D., Perrig, A.: Practical Techniques for Searches on Encrypted Data. IEEE Symposium on Security and Privacy. (2000)
42. Li, M., Yu, S., Cao, N., Lou, W.: Authorized Private Keyword Search over Encrypted Data in Cloud Computing. Distributed Computing Systems (ICDCS), 2011 31st International Conference on. (2011)
43. Rhee, H. S., Park, J. H., Susilo, W., Lee, D. H.: Trapdoor security in a searchable public-key encryption scheme with a designated tester,. Journal of Systems and Software. 83, 763–771 (2010)
44. Yang, Y., Lu, H., Weng, J.: Multi-User Private Keyword Search for Cloud Computing. 2011 IEEE Third International Conference on the Cloud Computing Technology and Science (CloudCom). (2011)
45. Zhu, B., Zhu, B., Ren, K.: PEKSrand: Providing Predicate Privacy in Public-Key Encryption with Keyword Search. ICC. (2011)
46. Gentry, C.: A fully homomorphic encryption scheme. Stanford University. (2009)
47. Naehrig M., Lauter K., Vaikuntanathan V.: Can homomorphic encryption be practical?. Proceedings of the 3rd ACM workshop on Cloud computing security workshop. 113–124 (2011)
48. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (Leveled) fully homomorphic encryption without bootstrapping. ITCS. (2012)
49. Gentry, C., Halevi, S., Smart, N. P.: Fully Homomorphic Encryption with Polylog Overhead. EUROCRYPT. (2012)
50. Witten, I. H., Frank, E., Trig, L. E., Hall, M. A., Holmes, G., Cunningham, S. J.: Weka: Practical machine learning tools and techniques with Java implementations (1999)
51. Nelson, R., Lawson, D., Lorier, P.: Analysis of long duration traces. ACM SIGCOMM Computer Communication Review. 35, 45–52 (2005)
52. Alcock, S., Nelson, R., Miles, D.: Investigating the impact of service provider NAT on residential broadband users. (2010)
53. Lof, A., Nelson, R.: Comparing anomaly detection methods in computer networks. Fifth International Conference on Internet Monitoring and Protection (ICIMP). 7–10 (2010)
54. Alcock, S., Lorier, P., Nelson, R.: Libtrace: a packet capture and analysis library. ACM SIGCOMM Computer Communication Review. 42, 42–48 (2012)
55. Cloud Security Alliance. The notorious nine: cloud computing top threats in 2013. `https://cloudsecurityalliance.org/group/top-threats/`. Accessed 7 September 2015 (2013)
56. Krautheim, F. J.: Private virtual infrastructure for cloud computing. Proceedings of the 2009 conference on Hot topics in cloud computing. (2009)
57. Dr Dobbs Journal. SIEM: A Market Snapshot. `http://www.drdobbs.com/siem-a-market-snapshot/197002909`. Accessed 7 September 2015 (2007)

58. Ko, R. K. L., Lee, S. S. G., Rajan V.: Understanding Cloud Failures. IEEE Spectrum. 49(12) 84 (2013)
59. Sutton, M., Greene, A., Amini, P.: Fuzzing: Brute force vulnerability discovery. Pearson Education. (2007)
60. Takanen, A., Demott, J. D., Miller, C.: Fuzzing for software security testing and quality assurance. Artech House.(2008)
61. THC.org. THC-IPV6. http://www.thc.org/thc-ipv6/. Accessed 7 September 2015 (2015)
62. Trend Micro. SecureCloud - Securing and Controlling Sensitive Data in the Cloud. SecureCloud. http://www.trendmicro.com/us/enterprise/cloud-solutions/secure-cloud/index.html. Accessed 7 September 2015 (2015)
63. Aura Information Security. (2012). Aura RedShield. https://auraredshield.com/. Accessed 7 September 2015 (2015)
64. Bertino, E., Paci, F., Ferrini, R., Shang, N.: Privacy-preserving digital identity management for cloud computing. IEEE Data Eng. Bull. 32, 21–27 (2009)
65. Gopalakrishnan, A.: Cloud computing identity management. SETLabs briefings. 7, 45–54 (2009)
66. Celesti, A., Tusa, F., Villari, M., Puliafito, A.: Security and cloud computing: intercloud identity management infrastructure. The 19th IEEE International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE). 263–265 (2010)
67. Agrafiotis, I., Creese, S., Goldsmith, M., Papanikolaou, N., Mont, M. C., Pearson, S.: Defining Consent and Revocation Policies. Proceedings of 2010 IFIP/PrimeLife Summer School. (2010)
68. Yu, S., Wang, C., Ren, K., Lou, W.: Attribute based data sharing with attribute revocation. Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. 261–270 (2010)
69. Mont, M. C., Sharma, V., Pearson, S.: EnCoRe: Dynamic Consent, Policy Enforcement and Accountable Information Sharing within and across Organisations. HP Laboratories. Technical Report HPL-2012-36 (2012)
70. Pang, S.: Research and development on decentralized analytical methods for network traffics with regional information. Unitec-NICT Research Center on Computational Intelligence for CyberSecurity (2012)
71. Pang,S., Ban, T., Kadobayashi, Y., Kasabov, N.: LDA Merging and Splitting with Applications to Multi-agent Cooperative Learning and System Alteration. The IEEE Transactions on System, Man, and Cybernetics-Part B. 42(2), 552–564 (2012)
72. Wood, T., Gerber, A., Ramakrishnan, K., Van der Merwe, J., Shenoy, P.: The case for enterprise ready virtual private clouds. Proceedings of the Usenix Workshop on Hot Topics in Cloud Computing (HotCloud). San Diego, CA, USA (2009)
73. Citrix Systems Inc. Business Continuity. https://www.citrix.com/solutions/business-continuity/overview.html.Accessed 7 September 2015 (2015)
74. Pokharel, M., Lee, S., Park, J. S.: Disaster Recovery for System Architecture Using Cloud Computing. The 10th IEEE/IPSJ International Symposium on Applications and the Internet (SAINT). 304–307 (2010)