Security of Cloud Computing: Seeing Through the Fog

M.T. Dlamini[1,2], H.S. Venter[1], J.H.P. Eloff[1,2] and M.M. Eloff[3]
Department of Computer Science
University of Pretoria[1], Pretoria, 0002, South Africa
Tel: +27 12 420 3654, Fax: +27 12 362
and SAP Research IA&S/Meraka UTD[2]
and School of Computing
University of South Africa[3], Pretoria, South Africa
email: {mdlamini, hsventer, eloff}@cs.up.ac.za[1]; {moses.dlamini, jan.eloff}@sap.com[2];
eloffmm@unisa.ac.za[3]

Abstract- Cloud computing is a new computing paradigm for the provisioning, delivery and consumption of IT resources and services on the Internet. This computing paradigm comes with huge benefits such as cost savings, increased resilience and service availability, improved IT operations efficiency and flexibility. However, most research cites security concerns as one of the biggest challenges for most of these organizations. This has led to fallacy or misconception about security challenges of the 'cloud' which needs to be clarified. This is a call for more research to separate reality from the hype. Hence, this paper aims to separate justified security concerns from the hype, fear of the unknown and confusion that currently prevails within cloud computing. This paper aims to advance the current discussions on cloud computing security in order to clear the 'foggy cloud' hovering over such a promising technology development. It seeks to inform and make decision makers aware of the real pertinent and justified security issues within cloud computing.

Index Terms—cloud computing, security challenges, hype.

I. INTRODUCTION

Today's business environment is characterized by the ever increasing business competition and rapidly changing ICT landscape. If organizations are to cope with today's fast paced technologically driven business environment, they must embrace the rapid technological changes and be ready to transform their business models accordingly. Cloud computing is one technological change that organizations are required to embrace if they are to respond to the ever increasing business competition. Its true potential lies in its capacity to radically transform business models and help organizations respond to the fast moving world.

Cloud computing offers a new model for provisioning and obtaining computing resources as a service. Cloud computing creates a highly dynamic environment, where everything is delivered, provisioned and consumed as a service and a service is everything in the cloud [4]. This model offers an on-demand and dynamic access to computing resources such as storage, applications, platforms and computing power as a service over the Internet. Cloud computing has compelling benefits such as significant cost savings, high resilience and service availability. However, cloud computing has not yet reached the expected adoption rates, just like an antique light bulb; it still generates more heat than light [12].

The weak adoption of cloud computing amongst most organizations are due to the fact that they are still spectators watching the early adopters from the sidelines; an indication that cloud computing has not been fully exploited by the majority of its potential customers. This could be attributed to quite a number of problems.

One such problem is related to the misconceptions regarding cloud computing security issues which must be clarified to improve its adoption rates. There is a surging need to separate justified security concerns from possible over-reaction, hype and fear of the unknown that currently prevails within cloud computing. Over-reaction, hype and the fear of the unknown has led to a generalization that '*security concerns are the biggest challenges of cloud computing*' [2,3].

Hence, this paper advances the current discussions beyond the over-reaction, hype and fear of the unknown for cloud computing in order to clear the fog hovering over such a promising computing paradigm. Its gravity is centered on separating justified from unjustified security concerns of cloud computing. The goal, however in not just to help potential cloud customers see beyond the fog that surrounds cloud computing security, but also inform and make potential cloud computing customers aware of the real pertinent and justified security issues.

The rest of the paper is structured as follows: Section II discusses some background to set the scene. Section III discusses related work. Section IV builds on related work to separate hype from reality and clear the general misconception of surrounding cloud computing. Section V provides a proposal for approaching security on cloud computing. Section VI concludes the paper.

II. BACKGROUND

This section discusses the definition of cloud computing and its benefits to set the scene for the remainder of the paper.

A. Cloud Computing Definition

Cloud computing can be loosely defined as a new computing paradigm that makes possible the utilization of computing infrastructure at a level of abstraction as an on-demand service, which is made available over the Internet

[2]. However, the most comprehensive definition of cloud computing is found in the recent draft definition from the NIST [1]. This definition is well accepted and widely used by most researchers and experts in the cloud computing arena [1,2,3,4,5, 14].

It defines cloud computing as “a model for enabling convenient and on-demand access to a shared pool of configurable computing resources and services that can be rapidly provisioned and released with minimal management effort or service provider interaction”. This model promotes and facilitates resource and service availability. It is based on **eight common characteristics** (i.e. massive scale, homogeneity, virtualization, low cost software, resilient computing, geographic distribution, service oriented and advanced security) and **five essential characteristics** (i.e. on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service). It also has **three service models** (software as a service, platform as a service and infrastructure as a service), and **four deployment models** (private, community, public and hybrid cloud) as depicted in figure 1 below**.**

The focal point of this paper is on the security concerns in cloud computing environments, hence, the reader is directed to the work of [1], [2] and [4] for more information on the cloud computing definition framework. The next subsection briefly highlights the benefits of cloud computing.

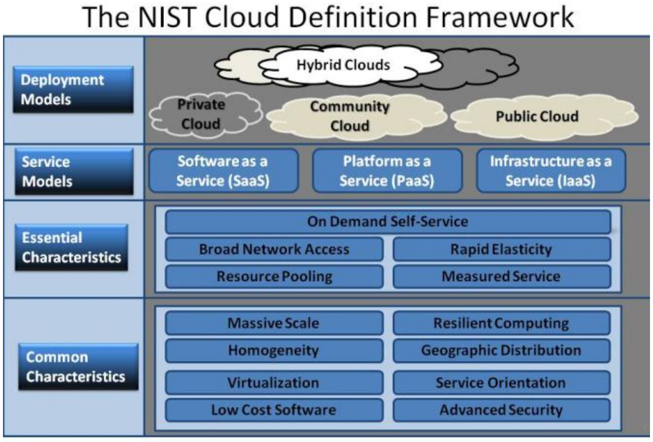

Fig.1: NIST Cloud Computing Definition Framework [2, 3]

B. Benefits of Cloud Computing

Cloud computing present a number of significant benefits that can greatly improve the efficiency of ICT operations to help organizations gain the competitive edge necessary to survive in today’s challenging business environment.

The most cited benefit of cloud computing is the significant cost saving [3, 4, 5, 6, 13]. This is also reflected in figure 2 below. According to [13], reduced costs stand out as the main benefit of the cloud, followed by increased IT efficiency, faster deployment rates and, improved security among others.

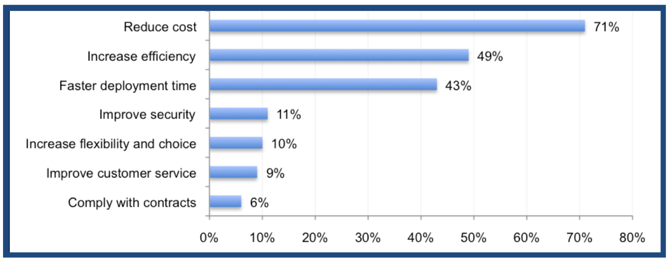

Fig. 2: The Primary Benefits for Cloud Computing [13]

In terms of reduced cost, cloud computing lowers or removes intensive capital IT costs and transform them into operational expenses to run core business operations. Cloud computing greatly reduces the time to get businesses up and running. It also reduces or removes upfront costs of acquiring ICT infrastructure and offers instant access to flexible computing resources [7, 13]. The main beneficiary of cloud computing is most likely to be small businesses with the lack economies of scale [5].

The other benefit of cloud computing is its high degree of redundancy that provides a high degree of service availability [10]. The level of redundancy provided in cloud computing makes the cloud infrastructure more resilient to security threats, failures and natural disasters.

Cloud computing also provides on-demand, elastic and scalable access to computing resources [1]. On-demand means that each service on the cloud is requested as the need arise on a need-to-use (demand) basis and paid for on pay-as-you-use basis using a utility pricing model to pay for only what you have used or consumed. For instance, a customer pays for storage per gigabytes/terabyte per hour that their data is stored by the cloud storage service provider. Scalability and elasticity means that the provisioned computing resources can be either increased or decreased depending on the customer demands. To cloud computing customers, the computing resources appear as if they are unlimited. In support, [6] agrees that cloud computing provide infinitely (unlimited) flexible computing resources.

With cloud computing, businesses need not worry about having expertise to run and maintain computing resources in-house. This responsibility is transferred to the cloud service providers. The aim is to reduce operating overheads for cloud customers to allow them to focus on their core competences. For example, with the Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) cloud model applications and software running on the cloud infrastructure is maintained and managed by the cloud service provider [4]. This facilitates timely updates and patches to quickly eliminate vulnerabilities before they could be exploited.

However, this is by no means an exhaustive list of the benefits of cloud computing. It is clear that cloud computing has a revolutionary potential to radically change the way business is conducted and most organizations are well aware of its compelling benefits and potential.

III. RELATED WORK

Numerous research efforts concur that cloud computing has considerable benefits for today’s organizations [2, 3, 4, 5, 6, 7, 8, 9, 10]. However, security concerns are cited as one of the biggest stumbling blocks for most organizations that are considering moving their critical applications and sensitive data to the cloud. Skeptics are using security concerns as an excuse not move to the cloud. This has been exacerbated by the fact that cloud computing is still to prove its worth to its end users. The fear of the unknown has also contributed to the slow adoption of cloud computing. Therefore, much has been reported on security concerns of cloud computing and it has become difficult to separate justified security concerns from hype, fear and confusion. To clear the air, the remainder of this section discusses some of the work that has already been carried out on the security of cloud computing.

Cloud computing is a game-changing paradigm that has significantly changed the threat landscape with regards to service resilience, availability and the protection of sensitive data and applications [4]. Firstly [4] asserts that cloud computing depends on multiple independent cloud service providers (i.e. applications, data, infrastructure and platform) which creates multiple points of failure.

The shared nature of cloud services (multi-tenancy) is cited as the key factor that contributes to serious security concerns on the cloud. Segregation of co-located data, computing resources, storage etc relies on software controls which raise concerns about unintentional data leakage.

[4] reports that data access controls and identity management are other security concerns that turn out more complex within cloud computing environments. Cloud customers are heavily dependent on cloud service providers (CSPs) to manage most of their business services. Cloud customers lose control of their data to the cloud service providers. This limits cloud customers' situational awareness of the looming security threat that could possibly affect their data [4].

An interesting view raised in [4], is that of audit logs and forensic data in case of a reported security breach. Cloud service providers have legal obligations to protect and preserve the privacy of its customers, yet on the other hand they must provide audit logs and forensic data.

The issue of data life-cycle management is also raised in [4]. Cloud computing requires security measures that can securely create, process and destroy client data residing on the cloud. Most of the issues raised in [4] are justified security concerns that are specific to a cloud computing environment.

A special publication [5] by NIST provides an overview of the security challenges (related to system complexity, shared multi-tenancy, Internet-enabled services and loss of control) that are pertinent to cloud computing. Of note, this publication raises one of the most overlooked points in cloud computing: it has grown out of the combination of already existing technologies or paradigms such as distributed systems, service oriented architecture and pervasive computing, with already known security issues being cast in a new environment [4, 5]. In addition [4] and [10] also agrees that cloud computing might be a new way of delivering computing resources, but it is definitely not a new technology. This reflects that there is nothing more to fear as most security threats are already known and already have effective security measures already in place. This could mean that cloud computing security issues are more of a hype and over-reaction from sceptics aimed at stifling the adoption of cloud computing.

In [5], the complexity of the cloud computing environment is acknowledged as one of the factors that exacerbate cloud computing security issues. The complexity is due to the combination of existing technologies and many components such as virtual machines, databases, supporting middleware, resource metering and billing, data replication, etc that combine to make cloud computing a reality. Most of these technologies and components already have known security issues with known mitigation strategies. However, complexity comes with their interactions which raise new security concerns. Security is argued to be inversely proportional to complexity, i.e. more complexity exponentially increases vulnerabilities [5]. This work [5] ends with some recommendations for organisations that are planning to move their data, applications or infrastructure to the cloud. Most of the cloud computing security issues raised in [5] are justified concerns related to applicable characteristics of cloud computing such as system complexity, multi-tenancy, Internet–enabled services and loss of control.

[6] claims that security concerns are the final barrier for most organizations looking to adopt cloud computing. According to [6] organizations have understandable concerns about security issues. The reason cited therein is that cloud computing is still considered a vague and intangible paradigm whereby clients cannot be certain about the whereabouts of their data or how it is handled, stored or transmitted. This raises reasonable and understandable doubts about the safety of their data. Therefore, [6] argues that before most organizations could adopt cloud computing they need assurance that;

- cloud computing won't compromise their security;
- their sensitive data and intellectual property will be protected
- they can easily retrieve their data should a need arise to change service providers
- they can still maintain their standards and competitive performance

This work [6] further examines and assesses the perceived security concerns of cloud computing, in order to determine whether they are justified or not. It concludes by recommending controls with the potential to make cloud computing security a reality.

[7] raises ten security concerns for cloud computing. These include geographical location of data on the cloud, regulatory requirements, access controls, classification and separation of data from different multi-tenants, handling security breaches, service level agreements, auditing, long-term viability of the cloud service provider, training and disaster recovery/business continuity plans. Most of these security concerns in [7] are not necessarily specific to cloud computing and some have already been addressed in other environments. All that needs to be done now is to tailor them into the cloud computing environment.

[8] discusses the problem of resource metering as one of the security issues on the cloud. This issue is discussed with regards to the services rendered by cloud service providers to their customers. This work [8] proposes a solution that seeks to ensure that cloud customers are billed in accordance with the service rendered by the cloud service provider.

Metering and billing has been successfully implemented in pay-as-you-go and pre-paid models for telecommunication and utility companies e.g. Cisco VoIP Prepaid billing solution. With a few tweaks the same principles could also be used in cloud computing resource metering.

The work of [10] agrees that security is a top priority for cloud computing customers. Therein it is argued that cloud customers make buying choices on the basis confidentiality, integrity, availability and resilience of the security services offered by a cloud service provider. Furthermore, [10] make recommendations on priority research areas that could help improve security of cloud computing technologies.

In summary, most of the covered related work is in agreement that cloud computing has attractive and compelling benefits for those organizations that seek to embrace it. They all agree that security concerns remains a challenge for the adoption of cloud computing. However, most of the work, apart from [6] fails to acknowledge that some of the perceived security concerns of cloud computing could just be an over-reaction or be a result of the fear of the unknown for cloud computing. Failure to acknowledge and show that cloud computing security is an issue that has been blown out of proportion and failure to pin-point the justified security concerns of the cloud might just worsen the current situation and direct further research efforts to wrong and unjustified security concerns.

Most of the covered related work clearly identifies security concerns of cloud computing, but instead of providing specific solutions to the problem at hand, they either make recommendations or provide priority research areas that need to be covered to solve the problem. Surely, this is a good point of departure, but there is a need to at least propose specific solutions to the problems of security of the cloud.

It is in the wake of these and other issues that this paper attempts to separate hype from reality and focus on real pertinent and justified security concerns in cloud computing. This is an attempt to bring clarity to a complicated threat landscape which is quite often filled with more hype, fear of the unknown, incomplete and oversimplified information which has led to gross generalization that *'security remains the biggest challenge for cloud computing'*.

This paper furthermore, attempts to advance the current state-of-the-art and go beyond such generalization to deliver more insightful and targeted security proposals for cloud computing. It builds on the related work and as its point of departure, acknowledges that some of the raised concerns about security in the cloud are valid and some maybe overrated or hyped.

The next section tries to summarize the justified security concerns gleaned from the above related work.

IV. Justified Security concerns of the Cloud

Before we could delve into the justified security concerns of cloud computing, it is worth noting we acknowledge that some of the raised concerns are unjustified. Most of the issues raised such as resource metering, remote access, access controls and identity management, for instance, have already been discussed in some spheres and solutions (such as pay-as-you-go, pre-paid, VPN and remote attestation, IAM models). These solutions may not have been used in a cloud computing environment before, but they could be tweaked and re-packaged in a way to apply them successfully to also work in a cloud computing environment.

Table 1 outlines and categorize the justified security concerns of cloud computing gleaned from the above related work. The categorization is adopted from [14] i.e. data protection, security control, compliance, multi-tenancy and security governance.

V. Some Proposed Solutions for Cloud Computing Security

The cloud computing paradigm is made possible by integrating a number of already existing technologies. These technologies have already been deployed successfully in other computing environments and their security concerns are already known. Security solutions have already been proposed to solve some of security issues raised. This section briefly discusses Kerberos authentication protocol, single sign-on, transparency enhancing technologies, service level agreements and tamper-proof digital forensics audit logs and evidence to show how some of the existing technologies could be used in the cloud.

A. Authentication, Authorization and Accounting (AAA) on the Cloud

Some of these solutions have already been tried and tested like the Kerberos authentication protocol, remote attestation, single sign-on (SSO) used to mutually authenticate and verify clients, software applications and CSPs. These could be repackaged and integrated to provide AAA in the cloud.

The Kerberos authentication protocol forms the backbone for SSO in terms of authentication and authorization on the cloud. It however lacks the accounting principle used to monitor resource usage for logging and billing purposes. The proposal we make is to enhance the Kerberos authentication protocol with an added functionality of an accounting protocol. Used in conjunction with an identity management system, this could solve the issues of AAA on the cloud and help enable cloud customers to keep track of all user access and usage of their data.

B. Transparency Enhancing Technologies (TETs)

Some of the major cloud computing challenges that raise security concerns are that quite often clients do not have an idea of exactly where their data sits, or who has access to it, or who process it and for what purposes. This is due to the fact that after the clients migrates their data and applications to the cloud, they pretty much lose control and entrust everything to the cloud service provider. Transparency Enhancing Technologies (TETs) have already been used in customer profiling [15]. This technology coupled with scalable access and usage controls can be effectively used by cloud computing clients to claim back the lost control from the CSPs. TETs can effective help cloud customers to locate where their data resides on the cloud, keep track of how it is handled and by whom?

Table 1: Justified Security Concerns for Cloud Computing

Data Protection	Security Control	Compliance	Multi-tenancy	Security Governance
Ensure that client data is available, its integrity and confidentiality are preserved.	The controls to be considered by both CSP and Client (what controls are to be implemented on both the CSP and client?)	Specific compliance requirements for both the CSP and Client	Safety of co-located client data on multi-tenant and shared cloud platforms.	Data ownership (who own the data including the replicated and redundant copies on the cloud? Who has the ownership of and rights to IP?)
Physical location of data (Is there a way of telling where data reside or how it is stored and handled? Is the sensitive data and intellectual property safe wherever it is stored?)	Control implementation (how are the controls implemented?)	Readily available tamper-proof logs and audit trails for timely forensic investigation (How to conduct effective incident handling and reporting, the gathering of forensic data, dispute resolution and rules of evidence?)	Data segregation and the shared nature of cloud services (How can we prevent unintentional data leakage in a multi-tenancy environment?)	Data replication (upto what extent can the client's data be replicated? How to ensure an almost real-time synchronization of the replicated data which might reside in different regions?)
Legal and compliance ramifications related to the data location (Does the clients have to comply with extra mandates in case of data residing in multiple locations e.g different countries.)	Assurance level (How are they managed and assessed? Can the CSP or client substantiate the sufficiency of the implemented controls?)	Extra compliance mandates arising from geographical location (How do you ensure compliance in multiple jurisdictions?)	Resource sharing (Ensuring that that malicious activities carried out by one tenant does not affect the reputation of another tenant)	Data lifecycle management (How can we ensure a secure creation, processing and complete deletion of customer data from the CSP?)
Data protection at storage, in transit within and across the Cloud (Is the data always in an encrypted format?)		Service Level Agreements (How can we monitor, measure and track performance?)		Data control and governance (How can you enforce policies for data access on the cloud and local device cache? Who has access to the client data?)

A. *Digital Forensics and SLA*

Cloud computing provides scalable storage for tamper-proof service level agreements (SLA) flags, audit logs and digital forensic evidence. Scalable storage services provided on an abstracted layer of cloud virtualization technologies can help create virtual machines with the images of the tamper-proof SLA flags, audit logs and digital forensic evidence. This can help reduce downtime as the systems holding such data would not be taken offline for analysis.

VI. Conclusion

Most organizations have cited security concerns as one of the biggest challenge preventing them from migrating their data and applications to the cloud. Surely, security is an important issue on the cloud, but this issue seems to have been blown out of proportion. This paper has shown that some of these concerns are not even justified to start off and are nothing but hype and fear of the unknown. It has also shown that even the justified security concerns can be solved by repackaging already existing security technologies and integrating them in an appropriate manner that would be applicable in the cloud environment.

Acknowledgements

The support of SAP Research IA&S/Meraka UTD and the University of Pretoria's ICSA research group towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at are solely those of the authors and should not necessarily be attributed to SAP Research IA&S/Meraka UTD or ICSA research group.

VII. References

[1]. P Mell and T Grance, The NIST Definition of Cloud available: http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc, accessed 18 April 2011.

[2]. P. Mell and T. Grance, Effectively and Securely Using the Cloud Computing Paradigm, 22nd Annual Conference: "Awareness, Training and Education: The Catalyst for Organisational Change, Federal Information Systems Security Educator's Association (FISSEA 2009) ,NIST, IT Lab, March 24 – 26, 2009, available: csrc.nist.gov/.../fissea/.../fissea09-pmell-day3_cloud-computing.pdf, accessed 18 April 2011.

[3]. Cloud Security Alliance (CSA), Security Guidance for Critical Areas of Focus Cloud Computing Version 2.1, December 2009, available: www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf , accessed 18 April 2011.

[4]. S. Gornaik, D. Ikonomou, P. Saragiotis, I. Askoxylakis, P. Belimpasakis, M. Broda, L. Buttyan, G. Clemo, P. Kijewski, A. Merle, K. Mitrokotsa, A. Munro, O. Popov, C.W. Probst, L. Romano, C. Siaterlis, V. Siris, I. Verbauwhede and C. Vishik, Priorities for Research on Current and Emerging Network Technologies, European Network and Information Agency (ENISA) European Union Agency) Report, 20 April 2010, available: www.enisa.europa.eu/act/it/library/deliverables/procent, accessed: 08 April 2011.

[5]. W. Jansen and T. Grance, Guidelines on Security and Privacy in Public Cloud, NIST Draft Special Publication 800 – 144, January 2011, Department of Commerce, USA.

[6]. Cable & Wireless Worldwide, Ensuring Security: The Last Barrier to Cloud Adoption, Cable & Wireless Worldwide Whitepaper, March 2011.

[7]. M. Gregg, 10 Security Concerns for Cloud Computing, Global Knowledge, Expert Reference Series of White Papers, available: www.globalknowledge.com, accessed: 18 April 2011.

[8]. R. Dubey, M.A. Jamshed, X. Wang and R.K. Batala, Addressing Security Issues in Cloud Computing, Technical Report, Carnegie Mellon University. n.d.

[9]. S. Dokras, B. Hartman, T. Mathers, B. Fitzgerald, s. Curry, M. Nystrom, E. baize and N. Mehta, The Role of Security in Trustworthy Cloud Computing, RSA White Paper, RSA Security Inc., CLOUD 0209, 2009, available: www.rsa.com, accessed: 14 April 2011.

[10]. D. Catteddu and G. Hogben, Cloud Computing: Benefits, Risks and Recommendations for Information Security, European Network and Information Security Agency (ENISA), November 2009, available: www.enisa.europa.eu/act/it/library, accessed: 08 April 2011.

[11]. D. Catteddu, Security and Resilience in Governmental Clouds: Making an Informed Decision, European Network and Information Security Agency (ENISA), January 2011.

[12]. C. Baudoin, Cloud Computing: Fear, Hype, Reality and Pragmatics, Cutter Consortium, Summit 2010: Strategies for the Road Forward, Cambridge, MA, 25 – 27 October 2010, available: www.cutter.com/summit/2010.html, accessed: 08 April 2011.

[13]. Ponemon Institute, Flying Blind in the Cloud: The State of Information Governance, A Research Report, Ponemon institute LLC, sponsored by Symantec, April 2010, available: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-ponemon_institute_flying_blind_in_the_cloud_WP.en-us.pdf, accessed: 08 May 2011.

[14]. R. Ritchey, Cloud Computing Security: Five key Considerations, Presentation Slides, DOE IMC, March 2011, available: http://cio.energy.gov/documents/Tuesday_Marquis_4_1355_Ritchey.pdf, accessed: 08 May 2011.

[15]. S. Gutwirth, Y. Poullet and P. De Hert, Data Protection in a Profiled World, Springer Dordrecht Heidelberg, London, New York, 2010.

Moses Dlamini received his BSc from the University of Swaziland, BSc Honours and MSc from the University of Pretoria, where he has now enrolled for his doctorate. Moses works at SAP Research IA&S Africa. His research interest: security of cloud computing, collaborative networks, NGN, IoT, and economics of information security.