A Novel Cloud Hybrid Access Mechanism for Highly Sensitive Data Exchange

Elhadj Benkhelifa
Faculty of Computing, Eng and Sciences
University of Staffordshire
Staffordshire, UK
e-mail: e.benkhelifa@staffs.ac.uk

Dayan Abishek Fernando
Faculty of Computing, Eng and Sciences
University of Staffordshire
Staffordshire, UK
e-mail: d.fernando@staffs.ac.uk

***Abstract*— This paper presents a research contribution from a significant Business-University collaborative Project. The aim of the project is to develop a new disruptive approach for Digital Forensics service provision to enable the creation of new value chains via the Cloud technology. The project is highly complex and multidimensional. The project is concerned with the manipulation and service provision for highly sensitive data via a secure Cloud Service Delivery Platform. This paper reports on one aspect of a long running research program, concerned with Security. The paper presents a relatively novel solution adopted in the project for enhanced security to be implemented as part of the intended Cloud Service Delivery Platform. This solution is a hybrid approach between a Single-Sign-On and Multi-Factor Authentication in Federated Settings. Consideration of implementing this solution in the presence of Multi-Tenancy is also discussed in this paper, An aspect which has not been attempted yet, to the best of the authors' knowledge.**

Keywords- Cloud Computing, Single-Sign-on; Multi-Factor Authentication; Cloud Federation; Cloud Security, Multi-Tenancy

I. INTRODUCTION

Cloud computing is fast becoming a mainstream technology replacing the current practices in IT resource provisioning. The Cloud technology is a disruptive model as it represents a major change to the IT services landscape. Cloud Computing describes a new way of delivering IT services based on Internet protocols, and it typically involves provisioning of dynamically scalable and often virtualized resources [1]. Cloud services offer great benefit to organizations by eliminating complexity of service designing, deploying and configuring. Cloud Computing enables the delivery of services through the on-demand service-provisioning model to end users on a pay as you go basis over a network such as the Internet [1, 2].

Using the Cloud, companies can drive a more efficient, effective, and consumer led commercial that helps them continually reinvent and transform the way they do business, focusing on what makes sense from a business delivery, consumer satisfaction and growth model [1]. Enabling the underlying IT allows businesses to rapidly deliver services, integrate across technological divides, and increase efficiencies; where cost reduction and increased efficiency is a major feature; along with the ability to affect reach, reliability and availability no matter where you are or what time it is. In short, Cloud technology offers a wide spectrum of new digital value chains. However, security is often cited as one of the major concerns in adopting the technology.

Cloud services are mainly delivered through three main delivery models Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [1, 2, 3]. Table 1 summarises the main security concerns for each of the delivery models.

TABLE I. MAIN SECURITY CONCERNS ON CLOUD DELIVERY MODELS

Delivery Models	Security Concerns	Examples
SaaS	Data Security App Security Identity Authentication	Google Apps, Oracle SaaS, NetSuite Salesforce
PaaS	Data & Computing Availability Data Security Disaster Recovery	Google App Engine, RedHat, Microsoft Azure Heroku
IaaS	Data center construction Physical Security Network Security Transmission Security System Security	Amazon EC2, Verizon, IBM, Rackspace, Nimbus

As defined by the American National Institute of Standards and Technology (NIST), Cloud can be deployed in four models: Public and Private Clouds together with less commonly used models, Community and Hybrid Clouds; private Cloud; community Cloud; and hybrid Cloud; [3, 4].

This paper presents a relatively novel solution adopted in a real business case project; funded by a UK research Council to develop a complex Cloud Service Delivery Platform for Digital Forensics [15]. This solution is a hybrid approach between a Single-Sign-On and Multi-Factor Authentication in Federated Settings.

 ISBN: 978-1-61208-271-4

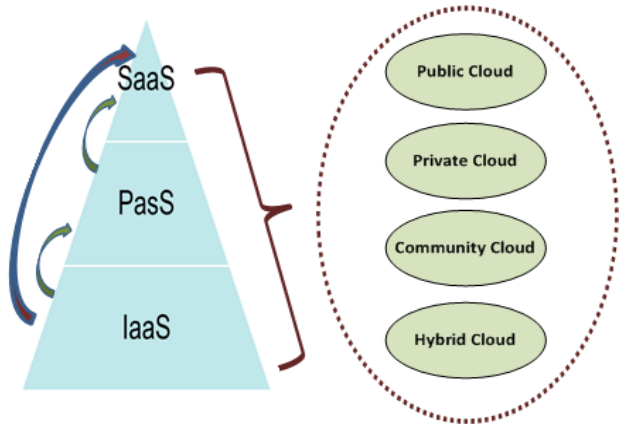

Figure 1. Delivery models vs. Deployment models.

Consideration of implementing this solution in the presence of Multi-Tenancy is also discussed in this paper; an aspect which has not been attempted yet, to the best of the Authors' Knowledge (Section IV). The paper also was an opportunity to review the area of Cloud service provision and reflect on the current practices for Cloud access management (Section III) and classifies Security challenges (Section II). Conclusions and direction for future research are summarised in Section V.

II. CLOUD SECURITY AND PRIVACY CHALLENGES

This section provides a concise summary of the current security and privacy challenges in a Cloud environment based on state of the art classification under five main categories, as illustrated in Figure 2.

There are number of security and privacy concerns for today's cloud computing landscape as it incorporates with various technologies including virtualization (i.e. virtual servers, virtual networks), on demand service provisioning, shared resource pools (i.e. data, memory), concurrent access, load balancing and distributed data are some examples [5]. Also big data in cloud has always been a security and privacy challenge due to the velocity, volume and variety of data. As shown in Figure 2, cloud security and privacy challenges can classified in to five main categories.

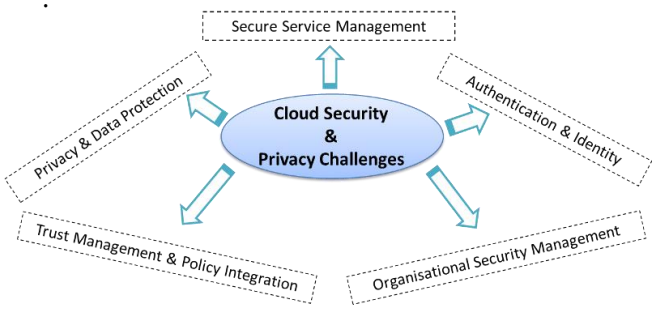

Figure 2. Cloud Security and Privacy Challenges.

Authentication and Identity Management

- Interoperability challenges in between service providers
- Inherent limitations in passwords
- Lack of clarification of multi-tenancy
- Multi-jurisdiction issues

Trust Management and Policy Integration

- Semantic heterogeneity
- Jurisdiction issues
- Trust and interaction/sharing requirements
- Composition of multiple services to enable bigger application services

Secure Service Management

- Issues such as price, QOS, and SLAs
- Automatic and systematic service provisioning; and a composition framework that considers security and privacy issues

Privacy and Data Protection

- Storing data and applications on systems that reside outside of on-premise datacentres
- Shared infrastructure, risk of potential unauthorized access and exposure.
- Privacy-protection mechanisms must be embedded in all security solutions.
- Balancing between data provenance and privacy

Organizational Security Management

- Shared governance
- Dependence on external entities
- Insider threat is significantly extended when outsourcing data and processes to Clouds.

III. CLOUD ACCESS MANAGEMENT

The Cloud Data Management Interface (CDMI) defines the functional interface: to implement strong access controls; provide data encryption; and storage media for secure multi-tenant Cloud environments; [6] CDMI supports most of standard protocols like File Transfer Protocol (FTP), Storage Area Network (SAN), Network Attached Storage (NAS) and Web Distributed Authoring and Versioning (WebDAV) [7].

Preventing un-lawful access to data resources in the Cloud is a key challenging deliberation. The most significant issue is that the digital identification and framework may not naturally extend into a Cloud environment, thus re-engineering the existing framework to support Cloud services may prove to be difficult [8]. Employing two different authentication protocols, one for the internal systems and another for external Cloud-based systems, leads to technical difficulty that can become unusable over time. Identity federation, supported by the introduction of Service Oriented Architectures (SOA), is one solution. Identity federation allows both Cloud service provider and service organisation to trust and exchange digital identities and

 ISBN: 978-1-61208-271-4

attributes across both domains. As shown in Figure 3, for federation to succeed, identity and access management transactions must be interpreted carefully and unambiguously, and protected against attacks [8, 9]. Federation is enabled by an Authorisation Exchange Standard [10].

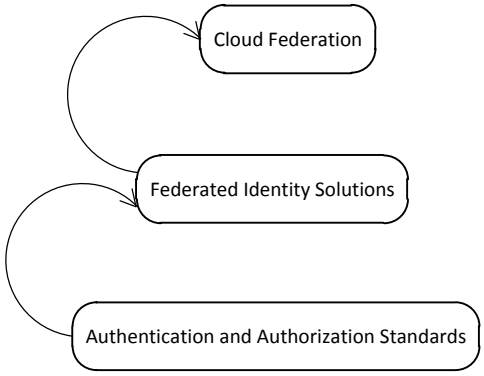

Figure 3. Single Sign-on based Cloud federation framework.

A. *Authentication /Authorisation Standards*

The Authentication and Authorisation Standard for Cloud computing defines a set of principles for exchanging authentication and authorisation between security domains. There are a number of protocols like OpenID, UMA, Radius and SAML which provide support to build the authentication and Authentication frameworks [10]. The Security Assertion Markup Language (SAML) is the most widespread standard that integrates digital security tokens containing assertions which pass information about a user, protocols and profiles so as to implement authentication and authorisation scenarios which allow secure data exchange between domains [11].

B. *Single Sign-On (SSO)*

As shown in Figure 4, Single Sign-On (SSO) is a process that enables a user to have single user credentials to gain access to multiple applications and resources which have been assigned for the user. SSO allows users to switch between different applications more effectively without any additional authentication requests [11].

Numerous researches have shown the prompt impact of SSO within Cloud industry. Shibboleth IDP, oxAuh OP, UMA PDP and LDAP cache are some of the architectures that refer to frameworks to build SSO environments [10, 11].

According to JANET, Shibboleth is the most widely adopted open source federated identity solution developed by the Internet2 middleware group [12]. The latest Shibboleth (V 2.0) builds on top of the SAML 2.0 authentication and authorization standards.

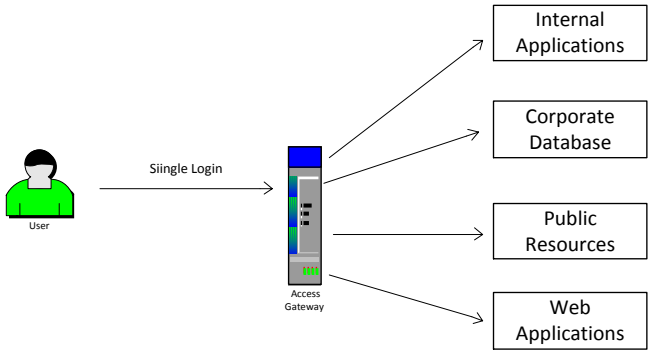

Figure 4. Single Login – Multiple Applications.

C. *Multi-Factor Authentication*

The multi-factor authentication is an authentication method, which requires two or more authentication factors to allow access to the IT resources [13]. As shown in Figure 5, there are three factors involved in establishing the multi-factor authentication framework.

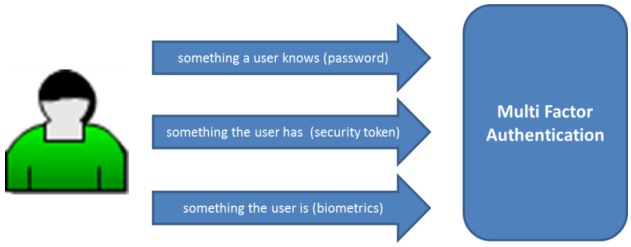

Figure 5. Multi-Factor Authentication.

Research studies have shown that a traditional username and password based Single-factor authentication is no longer strong/scalable enough to support the present security demands of the cloud. This is because compromise of a single factor results in a breach; whereas multi-factor authentication decreases the chance of subversion by having an increase in likelihood of correct identification with every additional factor. The current and widely used trend is two-factor authentication; it is widely spread amongst large financial institutions in Europe [8]. Two-factor authentication can also be found in a number of user-facing applications, such as social networks (Facebook) and Google Applications. Although the two-factor is currently considered the most efficient and very secure scheme, research continues to explore other more effective solutions as Two-factor authentication is already seen being breached. Therefore, an increased factor authentication (eg. three-factor) or hybrid approaches [9, 10], are currently being tested and researched.

This paper is an attempt to implement a hybrid authentication approach, using Single-Sign-On together with two-factor authentication whilst considering the multi-Tenancy Scenario (Section IV). This approach is proposed for direct application in a real business case.

 ISBN: 978-1-61208-271-4

IV. SECURE CREDENTIAL FEDERATION FOR HIGHLY SENSITIVE DATA EXCHANGE

Finding a balance between security and simplicity/accessibility is very important [13]. The proposed multi-level, hybrid authentication mechanism based on Single Sign-on (SSO) and two-factor authentication, enables not only Cloud federated access among multiple applications and organizations but also allowing sensitive data exchange between different domains (Figure 7).

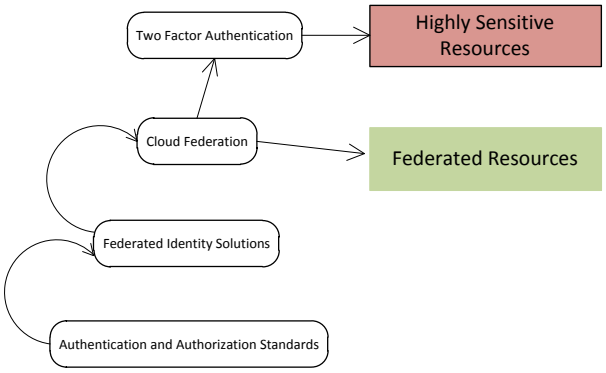

Figure 6. Proposed - Multi-Level Hybrid Authentication Mechanism

Single-Sign-On provides a unified mechanism to manage and monitor user interactions and business rules, determining user access to Cloud applications and data resources through the internet. Some industries require extra levels of security and identity protection over SSO settings in order to precede some specific secured tasks such as extremely sensitive application/data access, cross-border investigations, and remote data manipulation activities. Therefore, this paper is inspired to introduce a hybrid Cloud access framework by combining multifactor authentication with SSO in order to protect enterprise identities and thus enable a strong authentication method. Figure 6 and 7 illustrate the basic idea of the proposed solution.

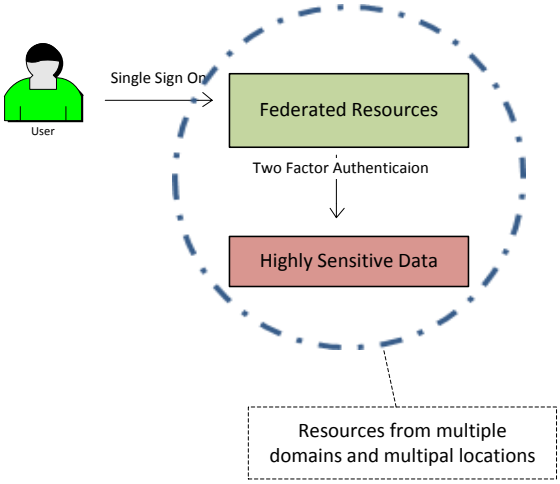

Figure 7. Resource Access through Multi-Level Hybrid Authentication.

The proposed hybrid solution comprises of two levels of security access layers providing access to federated resources and further sensitive resources within the federation agenda. The proposed solution defines federated resources as combined Cloud environments and applications for the purpose of resource sharing using single sign on to access multiple applications from multiple locations. Also, this solution allows access to highly sensitive resources within federation settings. Table 2 displays the access matrix vs. authentication of the proposed framework.

TABLE II. DIFFERENT RESOURCE ACCESS THROUGH MULTI-LEVEL HYBRID AUTHENTICATION

Data Access \ Authentication	Federated Resources	Highly Sensitive Resources
Single Sign-on	√	√
Two Factor Authentication	X	√

Figure 8 shows the high level access flow of the proposed hybrid access mechanism. The cloud access gateway acts as the doorman at the enterprise perimeter to cloud services and service users. The users can gain access to federated resources simply by providing SSO credentials. If the user need to access sensitive data within the federated settings, then they will be diverted to the two factor authentication for further credentials in order to gain access. Figure 9 illustrates the interaction between cloud components and users, showing how processes operate with one another and the direction in which federated resources are accessed. In a similar manner, Figure 10 displays the enhanced version of accessing sensitive data through two factor authentication.

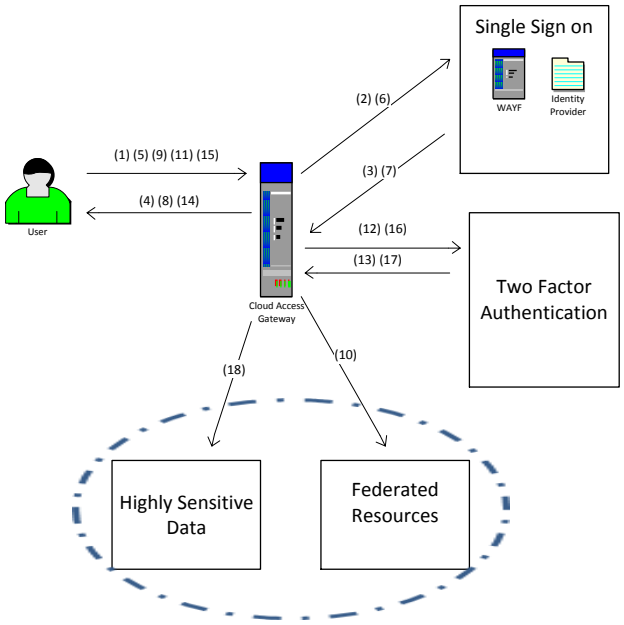

Figure 8. Hybrid SSO-Two-Factor Authentication Framework.

A. *Cloud Access Process flow*

1. Request to access federated resources
2. Redirected to the SSO WAFS (Where are you from)
3. IDP Request
4. Request User Credentials
5. Provide Credentials
6. Authentication
7. If success – Generate SSO User Session and pass into the Access Gateway
8. Prompt Authentication Status and redirect to federated resource pool
9. Access to Federated Resources
10. Federated Resources
11. User Request to access Highly Sensitive Data
12. Redirected to the Two Factor Authentication Service
13. Generate Security Token and pass into the Access Gateway
14. Send Security Token via SMS / Email
15. Enter Security Token
16. Pass token for verification
17. Update SSO session
18. Access to Highly Sensitive Data

B. *Considering Multi-Tenancy with the Proposed Solution*

Multi-tenancy is a method of sharing a single instance of data and applications among multiple customers (tenants) by allocating a unique profile for each tenant. Multi-tenancy presents a number of benefits such as: reduced operation cost by sharing resources (software/hardware); increased utilisation /optimisation rate in data centres and instant service provisioning for new clients [14]. However, despite the above-mentioned benefits, multi-tenancy is not widely deployed in the Cloud industry. The balance between resource sharing and security is very constrained and conflicting within a multi-tenancy framework. Also, the present multi-tenancy delivery models (Dedicated resource model, Metadata map model) are either less flexible or less secure (Table 3). The future developments of the proposed hybrid authentication solution will attempt to embed the multi-tenancy architecture where it is believed a mix of dedicated resources and metadata map architectures will deliver stronger security and greater flexibility. To the best of the authors' knowledge, this work is unprecedented, due to its complexity and limitations in the current Cloud Technology.

TABLE III. MULTI-TENANT DELIVERY MODELS

Dedicated resource model	**Metadata map model**
Increased Security	Increased Flexibility
Lower Flexibility	Lower Security

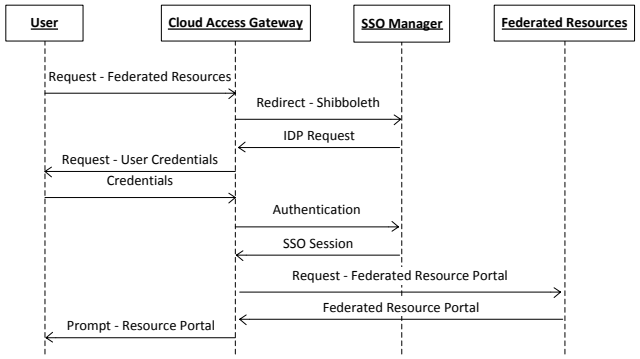

Figure 9. Sequence Diagram – Access to Federated Resources.

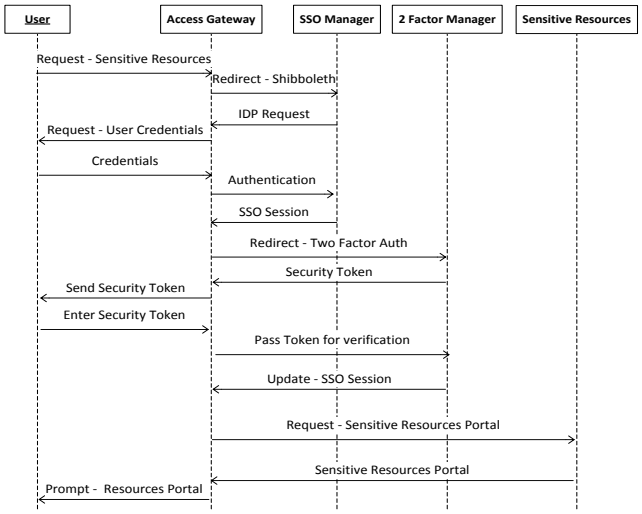

Figure 10. Sequence Diagram – Access to Sensitive Resources.

V. CONCLUSION

This paper proposes a novel hybrid solution for increased security to be implemented as part of a real business case project. The project is concerned with highly sensitive data, hence a more complex security approach is needed. The proposed hybrid solution, Single-Sign-On and two-factor authentication, is accepted by the project consortium and end-users to be a state-of-the-art and highly secure authentication approach. The proposed framework is currently being tested as part of the project deliverables, and results will be shared in future publications. Immediate future work will investigate the implementation of the proposed framework in the presence of Multi-tenancy, in federated Cloud settings. Another direction for future research is to evaluate the feasibility of implementing more than two factors for authentication. This evaluation will include the readiness of the current Cloud technologies for such enhancement in security and working out the balance under different constraints.

 ISBN: 978-1-61208-271-4

REFERENCES

[1] C. M. DaSilva, P. Trkman, K. C. Desouza, J. Lindic, Disruptive Technologies: A Business Model Perspective on Cloud Computing, 2013.

[2] C. Chapman, et al., Software architecture definition for ondemand cloud provisioning, Cluster Computing, 2011: pp. 1-21.

[3] P. Mell and T. Grance, The NIST Definition of Cloud Computing, 2011

[4] M. Armbrust, et al., A View of Cloud Computing, Communication of ACM, 2010

[5] A. Lenk., et al., What is Inside the Cloud? An Architectural Map of the Cloud Landscape, in Workshop on Software Engineering Challenges of Cloud Computing, Collocated with ICSE 2009, IEEE Computer Society: Vancouver, Canada , 2009.

[6] SNIA Cloud Data Management Interface (online). Available at URL: http://cdmi.sniaCloud.com [Retrieved: Feb 2013]

[7] JSON-RPC project (online). Available at URL: http://json-rpc.org [Retrieved: Feb 2013]

[8] P. A. Boampong, L. A. Wahsheh, Different facets of security, Proceedings of the 15th Communications and Networking Simulation Symposium, 2012.

[9] L. Peterson et al., Slice-based federation architecture, v2.0. http://groups.geni.net/geni/attachment/wiki/SliceFedArch/SFA2.0.pdf [Retrieved March 2013]

[10] K. D. Lewis, J. E. Lewis, "Web Single Sign-On Authentication using SAML," IJCSI- International Journal of Computer Science Issues, 2009.

[11] D. Raywood, Google adds two factor authenticationton Gmail via SMS one time passwords, 2010.

[12] L. M. Vaquero, L. Rodero-Merino, J. Caceres, M. A. Lindner, Break in the Clouds: towards a Cloud definition, 2009.

[13] M. Trojahn and F. Ortmeier, Biometric authentication through a virtual keyboard for smartphones, in International Journal of Computer Science & Information Technology (IJCSIT), 2012.

[14] S. Walraven, T. Monheim, E. Truyen, W.J. Sdsd, Towards performance isolation in multi-tenant SaaS applications, Proceedings of the 7th Workshop on Middleware for Next Generation Internet Computing, 2012.

[15] E. Benkhelifa and D. Fernando, Developing a Complex Cloud Service Delivery Platform: Practical Lessons From Real Business Case. International Conference of Cloud Computing and Services Science (ICCCSS'13), Dubai. 29-31 Jan 2013.

 ISBN: 978-1-61208-271-4