IJARSCT
ISSN (Online) 2581-9429
ISSN (Print) 2581-XXXX
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 11, Issue 1, November 2020
Impact Factor: 4.819

Cloud Computing Review, Research and Challenges: A Technical Aspect

Sushama Pawar[1], Chetashri Bhusari[2] and Yogita Jore[3]
Lecturer, Information Technology, Vidyalankar Polytechnic, Mumbai, India[1,2]
HOD, Information Technology, Vidyalankar Polytechnic, Mumbai, India[3]

Abstract: *Cloud computing is the latest technology in delivering computing resources as a service. Cloud computing is architecture for providing computing service via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data center of a cloud provider like Google, Amazon, Salesforce.som and Microsoft etc. This research paper outlines what cloud computing is, the various cloud models and the main security risks and issues that are currently present within the cloud computing industry. This research paper also analyses the key research and challenges that presents in cloud computing and offers best practices to service providers*

Keywords: Cloud Computing, architecture, PaaS, SaaS, IaaS

I. INTRODUCTION

Computing is a model that allows universal, on-demand and easy network access to a common pool of configurable computing resources (e.g. networks , servers , storage, software , and services) that can be easily supplied and released with minimal management effort or interaction between service providers. [1]

Cloud computing can be seen as network-enabled platforms that offer flexible, on-demand services guaranteed by QoS that can be accessed over the Internet [2]. Cloud Computing is a distributed architecture that centralises server resources in order to provide computing resources and services on demand on a scalable platform. Cloud service providers (CSPs) provide their users with cloud systems to use to build their web services, just as internet service providers provide high-speed broadband Internet connectivity to customers. Both CSPs and ISPs provide services (Internet Service Providers). Three kinds of services are usually offered by the cloud, i.e. Software as a service (SaaS), Infrastructure as a service (IaaS) and Application as a Service (PaaS). There are numerous reasons for companies to shift towards cloud computing IT solutions, as they are only expected to pay for consumption-based services. Moreover, companies should easily meet the needs of rapidly evolving markets and ensure that their customers are still on the leading edge [3]. Users can access heavy applications through lightweight portable devices such as cell phones, PCs and PDAs by leveraging this technology.

II. SERVICE MODELS OF CLOUD COMPUTING [2]

There are usually three types of cloud services: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

A) Software as a Service (SaaS): This is where users simply use a web browser to access software created and provided by others as a web service. Users have no power or access at the SaaS level to the underlying infrastructure that is used to host the applications. Customer Relationship Management tools and Google Docs from Salesforce are common examples that use the cloud computing SaaS model.

B) Platform as a Service (PaaS): This is where a collection of programming languages and software provided by a PaaS provider are used to build applications. PaaS offers a high degree of abstraction for users that allows them to concentrate on designing their applications and not think about the technology underlying them. Users do not have

IJARSCT
ISSN (Online) 2581-9429
ISSN (Print) 2581-XXXX
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 11, Issue 1, November 2020
Impact Factor: 4.819

control or access to the underlying infrastructure used to host their applications at the PaaS level, much like the SaaS model. Engine5 from Google App and Mic

C) Infrastructure as a Service (IaaS): This is where users receive computer resources from an IaaS provider, such as computing power, memory and storage, and use the resources to instal and run their applications. The IaaS model is a low level of abstraction that enables users to access the underlying infrastructure by using virtual machines, as opposed to the PaaS model. IaaS provides users with greater versatility than PaaS because it enables the user to instal any software stack on top of the operating system. Flexibility, however, comes at a cost and users are liable at the IaaS level for upgrading and patching the operating system. EC2 and S3 from Amazon Web Services are common examples of IaaS.

"Erdogmus[4], described Software as a Service as the central principle behind cloud computing, indicating that" it's all software in the end" does not matter if the software being distributed is infrastructure, network or application. Although this is valid to some degree, as they have different abstraction levels, it nevertheless helps to differentiate between the types of service being offered. The service models mentioned in the description of NIST are deployed in clouds, but depending on who owns and uses them, different types of clouds exist. In the NIST concept, this is referred to as a cloud deployment model and the four common models are:

Private Server: a cloud primarily used by one company. The company itself or a third party can run the cloud. Examples of companies providing private clouds are the St Andrews Cloud Computing Co-laboratory and Concur Technologies[5].

- **Public Cloud:** A cloud which the general public can use (for a fee). Public clouds need considerable investment and are traditionally owned by major companies such as Microsoft, Google or Amazon.
- **Public Platform:** a cloud owned by many entities and typically designed to suit their particular requirements. The Open Cirrus cloud testbed could be regarded as a cloud for the community that aims to support cloud computing research[6].
- **Hybrid Cloud:** a cloud that is set up using a combination of the three deployment models described above. Each cloud in a hybrid cloud could be operated separately, but it would be possible to transfer software and data through the hybrid cloud. Hybrid clouds allow cloud bursting to take place, which is where, when more resources are needed, a private cloud will burst out into a public cloud.

Figure 1 provides an overview of the common deployment and service models in cloud computing, where the three service models could be deployed on top of any of the four deployment models.

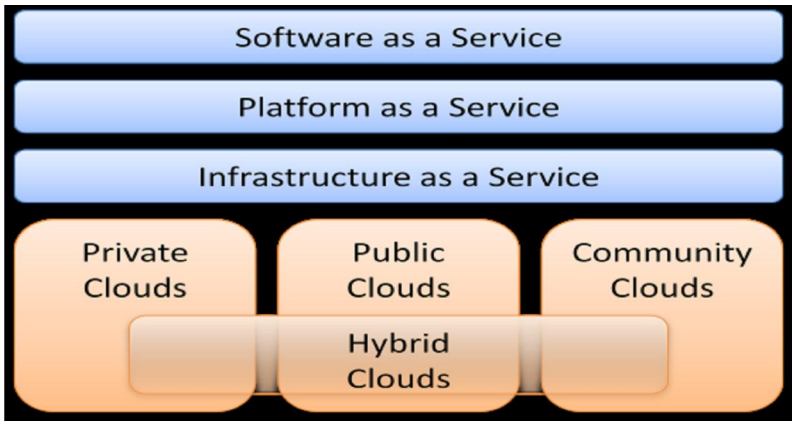

Figure 1: Cloud Computing Deployment and Service Models

IJARSCT
ISSN (Online) 2581-9429
ISSN (Print) 2581-XXXX
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 11, Issue 1, November 2020
Impact Factor: 4.819

III. Cloud Computing Entities

The two key entities in the business sector are cloud providers and customers. But, the two more emerging service level companies in the Cloud world are service brokers and resellers. As follows, these are discussed.

- **Cloud Providers:** Includes Internet service providers, telecommunications firms and major outsourcers of business processes that supply either the media (Internet connexions) or the infrastructure (hosted data centres) that enables cloud services to be accessed by customers. Service providers can also include systems integrators that build and maintain private cloud hosting data centres and provide various services to clients, service brokers or resellers (e.g. SaaS, PaaS, IaaS, etc.)[7]
- **Cloud Service Brokers:** Involves technology experts, technical service associations for companies, licenced brokers and agents and influencers to direct customers in the choice of solutions for cloud computing. Service brokers focus on negotiating consumer-provider partnerships without controlling or maintaining the entire cloud infrastructure. In addition, on top of the infrastructure of a cloud provider, they add extra services to make up the cloud ecosystem of the customer.
- **Cloud Resellers:** As cloud providers grow their business across continents, resellers may become an important force in the cloud industry. Local IT consultancies or resellers of their established products may be chosen by cloud providers to serve as "resellers" for their cloud-based products in a specific region. Cloud Consumers: End users belong to the Cloud Consumers group. However, as soon as you are a client of another cloud provider, broker or reseller, cloud service brokers and resellers may also belong to this group. Key benefits and potential threats and risks to Cloud Computing are described in the next section [8].

IV. Cloud Computing Security Architecture

Since the computers used to deliver services do not belong to the users themselves, protection in cloud computing is a particularly troubling problem. Users have no power over what could happen to their results, nor any knowledge of it. In situations where customers have sensitive and personal information stored in a cloud computing service, this is a great concern. Users would not risk their privacy, so providers of cloud storage services must ensure that information is protected for consumers. This, though, is becoming increasingly difficult because there always seems to be someone to find out a way to disable the protection and take advantage of user information as security developments is made. SLA Track, Metering, Billing, Resource Provisioning, Scheduler & Dispatcher, Load Balancer, Advance Resource Reservation Monitor, and Policy Management are some of the essential components of the service provider layer. Some of the Service Provider Layer-related security concerns are Identity, Infrastructure, Privacy, Data transmission, People and Identity, Audit and Compliance, Cloud integrity and Binding Issues.

Any of the main components of the Virtual Machine Layer produce and control the number of virtual machines and the number of operating systems. VM Sprawl, VM Escape, Infrastructure, Customer Isolation, Cloud Legal and Regularity Problems, Identity and Access Management Some of the important components of the Data Center (Infrastructure) Layer include the servers, CPUs, memory, and storage, and are now commonly referred to as Infrastructure-as-a-Service (IaaS). Some of the main components of the Data Center (Infrastructure) Layer Safe data at rest, Physical Protection: Network and Server are some of the Data Center Layer based security concerns. To understand the risks associated with services in a business context, risk assessment controls are critical. Activities have been undertaken by the National Institute of Standard and Technology (NIST), USA (http:/www.nist.gov/) to support cloud computing standards[9]

Several standards groups and industry consortia are creating requirements and test beds in order to overcome the challenges and to facilitate cloud computing. Cloud Protection Alliance (CSA), Internet Engineering Task Force (IETF), Storage Networking Industry Association (SNIA) etc., are some of the current standards and test bed organisations. A cloud API, on the other hand, offers either a functional interface or a management interface (or both). There are several facets of cloud management that can be standardised for interoperability.

Federated protection (e.g. identity) across clouds, metadata and data exchanges between clouds, structured tracking, auditing, billing, reporting and notification outputs for cloud applications and services, cloud-independent

IJARSCT
ISSN (Online) 2581-9429
ISSN (Print) 2581-XXXX
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 11, Issue 1, November 2020
Impact Factor: 4.819

representation for policies and governance, etc., are some potential standards. Figure 2 shows the high-level view of the security architecture of cloud computing.

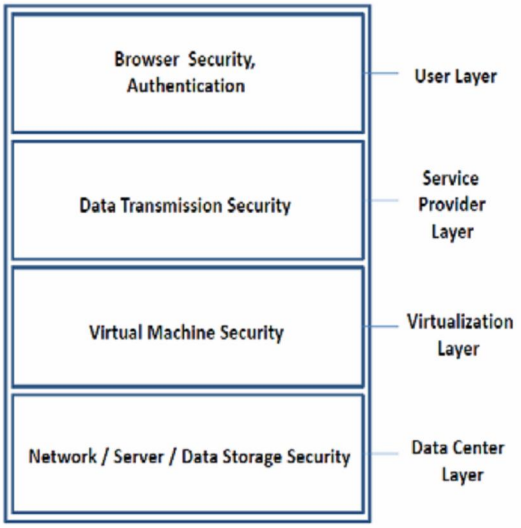

Figure 2: High Level Security Architecture of Cloud Computing

V. KEY SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing is made up of parts of software, systems and networks. Each section conducts various activities and provides companies and individuals around the world with various items. Software as a Service (SaaS), Utility Computing, Online Applications, Platform as a Service (PaaS), Managed Service Providers (MSP), Service Commerce and Internet Convergence are all included in the business application. Cloud computing has various security concerns, including networks, databases , operating systems, virtualization, resource scheduling, transaction management, load balancing, market control and memory management, as it encompasses several technologies. Security problems are also applicable to cloud computing with all of these systems and technologies. The network that links the systems in a cloud, for instance, must be safe and it must be secure to map the virtual machines to the physical machines. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. The given below are the various security concerns in a cloud computing environment.

- Access to server and application
- Data Transmission
- Virtual Machine Security
- Network Security
- Data Security
- Data Privacy
- Data Integrity
- Data Location
- Data Availability
- Data Segregation
- Security Policy and Compliance
- Patch management

IJARSCT
ISSN (Online) 2581-9429
ISSN (Print) 2581-XXXX
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 11, Issue 1, November 2020
Impact Factor: 4.819

VI. Research Challenges In Cloud Computing

Cloud Computing research addresses the challenges of meeting the needs of private, public and hybrid cloud computing systems of the next decade, as well as the challenges of enabling the advantages of cloud computing to be taken advantage of by applications and development platforms. Cloud computing research is also at an early stage. Many current problems have not been completely solved, although new issues continue to arise from applications in the industry. Some of the challenging cloud computing research problems are given below.

- Service Level Agreements (SLA's)
- Cloud Data Management & Security
- Data Encryption
- Migration of virtual Machines
- Interoperability
- Access Controls
- Multitenancy
- Server Consolidation
- Reliability & Availability of Service
- Common Cloud Standards
- Platform Management

Service Level Agreements (SLA's): The cloud is operated by service level agreements that enable several instances of one application to be replicated on multiple servers if necessary; the cloud will reduce or shut down a lower-level application depending on a priority scheme. The assessment of cloud vendors' SLAs is a major challenge for cloud customers. Most suppliers create SLAs to create a protective shield against legal action, while giving customers limited guarantees. Thus, there are some important concerns that need to be taken into account by consumers before signing a contract with a supplier, such as data security, outages, and price structures. If they resolve the necessary issues at the right time, the specification of SLAs will better represent the needs of the clients.

Cloud Data Management: Cloud data Cloud data management is an important research topic in cloud computing and can be very broad (e.g. text-based or science applications), unstructured or semi-structured, and usually append-only with rare changes. As service providers usually do not have access to the data centre physical protection system, in order to achieve maximum data security, they must rely on the infrastructure provider. Also for a virtual private cloud, only remotely can the service provider specify the security setting, without knowing whether it is completely enforced. In this sense, the infrastructure provider has to achieve goals such as confidentiality and auditability. These file systems are distinct in their storage structure, access pattern and application programming interface from conventional distributed file systems. They do not implement the standard POSIX interface, in particular, and thus introduce compatibility problems with legacy file systems and applications. This topic has been explored in many research efforts [10].

Data Encryption: Encryption is a crucial data protection technique. Understanding data in motion and encryption of data at rest. Note, security can range from simple (easy to handle, low cost and, quite frankly, not very safe) to highly secure (very difficult, costly to manage, and access-limiting). It is decrypted and processed until the object enters the cloud. Is there an option to encrypt it until it is saved? Before you upload the file for cloud computing, do you want to think about encryption or do you prefer the cloud computing service to do it for you automatically? There are ways to understand the cloud computing solution and make your choices based on the desired security levels.

Virtual Machine Migration: applications are not exclusive to hardware; multiple programmes can use virtualization to run on one machine, or several machines can run one programme. By allowing virtual machine migration to balance the load across the data centre, virtualization can provide major advantages in cloud computing. Furthermore, virtual machine migration in data centres allows robust and highly responsive provisioning. From process migration techniques, virtual machine migration has evolved. More recently, "live" migration of VMs was introduced by Xen and VMWare, involving extremely short downtimes ranging from tens of milliseconds to a second. Avoiding hotspots is the biggest advantage of VM migration, but this is not straightforward. At present, the identification of workload hotspots

IJARSCT
ISSN (Online) 2581-9429
ISSN (Print) 2581-XXXX
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 11, Issue 1, November 2020
Impact Factor: 4.819

and the initiation of a migration lack the agility to respond to sudden changes in workload. Moreover, the in memory state should be transferred consistently and efficiently, with integrated consideration of resources for applications and physical servers [11].

Interoperability: This is the ability of two or more systems to work together to share information and to use the information that they exchange. Many public cloud networks are configured and not intended to communicate with each other as closed systems. The lack of collaboration between these networks makes it hard for companies to integrate their cloud IT systems and realise cost savings and productivity gains. Industry standards must be established to help cloud service providers build interoperable systems and enable data portability in order to address this challenge. Organizations need to deliver services automatically, handle VM instances, and use a single tool set to work with both cloud-based and enterprise-based applications that can work through existing programmes and multiple cloud providers. There is a need to provide cloud interoperability in this situation.

Access Controls: The management of authentication and identification is more critical than ever. And, it's not all that different either. What is the standard of password strength compliance and change frequency invoked by the service provider? What is the technique for password and account name recovery? How are passwords supplied to users after a change is made? What about logs and links to the right to audit? This is not all that different from how you secure your internal systems and data, and it works the same way that you can protect that access aspect if you use strong passwords, updated regularly, with typical IT protection processes.

Multi-tenancy: There are many types of cloud applications that can be accessed via the Internet by users, from small Internet-based widgets to large enterprise software applications that have enhanced security requirements based on the type of data stored on the infrastructure of the software provider. For several purposes, these application requests require multi-tenancy, with cost being the most significant. Reaction times and output for other customers can be influenced by many customers accessing the same hardware, application servers, and databases. Specifically, resources are shared at each infrastructure layer for application-layer multi-tenancy and have legitimate security and efficiency issues. Many service requests that access resources at the same time, for example, increase wait times but not inherently Processor time, or the number of connexions to an HTTP server has been depleted, and the service must wait before an available link can be used or, in the worst case scenario, the service drops [12]

Consolidation of servers: The increased usage of energy and the decrease in power and cooling requirements achieved by server consolidation are now being extended into the cloud. In a cloud computing system, server consolidation is an efficient approach to optimise resource usage while minimising energy consumption. In order to merge VMs residing on multiple under-used servers on a single server, Live VM migration technology is also used so that the remaining servers can be set to an energy-saving state. The topic of consolidating servers in a data centre optimally is also formulated as a variant of the problem of vector bin-packing, which is a problem of NP-hard optimization. Various heuristics for this topic have been proposed.

Reliability & Service Availability: When a cloud provider provides on-demand software as a service, the problem of reliability falls into the picture. In order for users to access it under any network conditions (such as during sluggish network connexions), the app needs to have a consistent quality factor. Owing to the unreliability of on-demand apps, there are a few cases found. The MobileMe cloud service from Apple, which stores and synchronises data across multiple devices, is one example. When several users were not able to access mail and synchronise data correctly, it started with an embarrassing start. Providers are turning to technology such as Google Gears, Adobe AIR, and Curl to prevent such issues, enabling cloud-based applications to run locally, some even allowing them to run in the absence of a network connexion. These tools provide access to the desktop's storage and processing resources for web applications, forming a connection between the cloud and the user's own computer. Considering the use of software such as 3D gaming applications and video conferencing systems, reliability is still a challenge to achieve for an IT solution that is based on cloud computing [13]

Popular Cloud Standards: Cloud Computing security-based accreditation will cover three main fields, which are technology, staff and operations. Organizations such as Jericho Forum1 are likely to be guided by technical requirements before being ratified by existing bodies, such as ISO2 (International Standard Organization). The Institute

IJARSCT
ISSN (Online) 2581-9429
ISSN (Print) 2581-XXXX
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 11, Issue 1, November 2020
Impact Factor: 4.819

for Information Security Professionals3 (IISP) also provides formal accreditation for security professionals on the personnel side. There are some workable solutions for the operational components, such as modifying ISO 27001 and using it as the default measurement standard within the SAS 704 system. One of the key issues at present is that there are many scattered activities going in the direction of Cloud accreditation, but there is a lack of a common body to organise those activities. It will also be a major challenge to create a single accreditation body to certify Cloud services [14].

Platform Management: Difficulties in the delivery of middleware capabilities in a multi-tenant, elastic and flexible environment to develop, deploy, integrate and manage applications. One of the most significant components of cloud systems provides developers with different types of platforms to write applications that run in the cloud or use cloud services, or both. Different names, including on-demand and platform as a service (PaaS), are used for this type of platform today. There is tremendous potential for this modern way of helping applications. Most of what the application requires already exists when a development team develops an on-site application (i.e. one that will operate within an organisation). The operating system provides fundamental support for programme execution, database interaction, and more, while other computers in the environment provide services such as remote storage.

VII. Conclusion and Feature Work

In the cloud computing model, one of the main security issues is the sharing of resources. Cloud service providers need to alert their customers of the degree of protection that their cloud provides. We first addressed different models of cloud computing, security problems and research challenges in cloud computing in this paper. In Cloud Computing, data protection is a big concern. There are some other security issues, including network and virtualization security components. All these cloud computing problems have been illustrated by this article. We think that it would be hard to achieve end-to - end protection due to the complexities of the cloud. It is important to create new security security techniques and to dramatically tweak older security techniques in order to be able to work with the cloud architecture.

References

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology," *Natl. Inst. Stand. Technol. Inf. Technol. Lab.*, vol. 145, p. 7, 2011.

[2] F. Hu *et al.*, "A review on cloud computing: Design challenges in architecture and security," *Journal of Computing and Information Technology*, vol. 19, no. 1. pp. 25–55, 2011.

[3] A. Kundu, C. D. Banerjee, P. Saha, "Introducing New Services in Cloud Computing Environment", International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.

[4] ERDOGMUS, H. 2009. Cloud Computing: Does Nirvana Hide behind the Nebula? *Software, IEEE* 26, 2, 4-6.

[5] LEMOS, R. 2009. Inside One Firm's Private Cloud Journey. Retrieved December 1, 2009, from http://www.cio.com/article/506114/Inside_One_Firm_s_Private_Cloud_Journey

[6] Open CirrusTM: the HP/Intel/Yahoo! Open Cloud Computing Research Testbed. Retrieved December 1, 2009, from https://opencirrus.org/

[7] Pring et al., "Forecast: Sizing the cloud; understanding the opportunities in cloud services," Gartner Inc., Tech. Rep. G00166525, March 2009.

[8] AmanBakshi, Yogesh B. Dujodwala, "Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine," ICCSN '10 Proceeding of the 2010 Second International Conference on Communication Software and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.

[9] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, "Intrusion detection techniques for Grid and Cloud Computing Environment," IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43, 2010.

[10] X. Zhang, N. Wuwong, H. Li, and X. J. Zhang, "Information Security Risk Management Framework for the Cloud Computing Environments", In Proceedings of 10th IEEE International Conference on Computer and Information Technology, pp. 1328- 1334, 2010.

IJARSCT
ISSN (Online) 2581-9429
ISSN (Print) 2581-XXXX
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 11, Issue 1, November 2020
Impact Factor: 4.819

[11] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing," 17th International workshop on Quality of Service, USA, pp.1-9, July 13-15, 2009, ISBN: 978-1-4244-3875-4

[12] S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing"; Journal of Network and Computer Applications, Vol. 34(1), pp 1–11, Academic Press Ltd., UK, 2011, ISSN: 1084-8045.

[13] V. Krishna Reddy, B. Thirumal Rao, Dr. L.S.S. Reddy, P.SaiKiran "Research Issues in Cloud Computing " Global Journal of Computer Science and Technology, Volume 11, Issue 11, July 2011.

[14] Harold C. Lin, ShivnathBabu, Jeffrey S. Chase, Sujay S. Parekh, "Automated Control in Cloud Computing: Opportunities and Challenges", Proc. of the 1st Workshop on Automated control for data centres and clouds, New York, NY, USA, pp. 13-18, 2009, ISBN: 978-1-60558-585-7.