

An Analysis of Resilience of a Cloud Based Incident Notification Process

Paul de Vrieze and Lai Xu

{pdvrieze, lxu}@bournemouth.ac.uk
Faculty of Science & Technology
Bournemouth University, Poole House, Talbot Campus,
Fern Barrow, Poole, BH12 5BB, UK

Abstract. Cloud based Business Process Management (BPM) systems have provided SMEs with BPM in a pay-per-use manner. Previous work has focused on looking at cloud based BPM from the perspectives of distribution of data, activity or/and process engine and related issues, such as scalability of system, security of data, distribution of data and activities. To achieve business agility, business process collaboration needs to seamlessly connect local BPM systems and cloud based BPM systems. In this paper we look at BPM in the cloud from a user perspective: how can they support the fast pace of change of business collaborations and how to determine a resilience of a cloud based BPM solution. The paper proposes a distribution solution in which the shared process model can be discovered at the design time from a process repository, and adapted to local needs. At run-time the selected collaborative process model provides a global view, but is executed by multiple mashup engines of the participating parties. A real world case is used to explain our design. Collaborative processes for incident notifications are built to work across different organizations. Resilience of the solution are analysed accordingly.

Keywords: Business Process as a Service, Incident Management, Business Process Mashup, Resilience of Cloud based Processes.

1 Introduction

Cloud based Business Process Management (BPM) provides the distributed infrastructure as well as computing power to connect different partners towards a common goal. Cloud based BPM is therefore an ideal solution for collaborative BPM. In this paper, we look at the resilience of cloud based business process incident notification processes.

The Internet is a conduit for information exchange. In this role it has fundamentally changed how business is conducted. Cloud computing has enabled users to use computing resources in a pay-per-use manner and to treat these resources as unlimited [1]. In the cloud computing age, business process management systems have also adapted themselves to cloud environments. Business Processes as a Service (BPaaS) as a relative new concept can be any type of business process that is delivered based

on a cloud provisioning model. BPaaS can be seen as a new trend for Business Process Management [2, 3].

Incident notification processes normally are collaborative processes because industrial incident management most of time involves multiple parties. This kind of ad-hoc notification process is not supported by traditional BPM systems.

Looking at the incident notification process exposes the limitations of existing cloud-based business process service patterns. Executable business process models represent how the common business goals are achieved in a computer understandable way. Business process models thus are important assets for many organisations [4, 5]. Business processes encapsulate business drivers and policies. Therefore, business process models should be seen as an important component BPaaS. Traditionally, process models are created and deployed on a process engine by IT specialists. Today organisations face fast changes of their business environment. They need to be able to rapidly react to the changes. As such it is often desirable for Non-IT people to be able to select and modify process models to adapt to business needs.

In materials science, resilience represents the ability of a material to recover its original shape following a deformation [6]. In the corporate world, resilience refers to the ability of a company to bounce back from, or even resist, a large disruption – this includes, for instance the speed with which it returns to normal performance level (production, services, fill rate, etc.) [7]. Within cloud computing, the characteristic of resiliency can refer to redundant IT resources within the same cloud (but in different physical locations) or across multiple clouds [8]. In this paper, we analyse the resilience of a cloud based BPM solution for incident notification.

This paper is organized as follows: Section 2 presents related work; Section 3 briefly introduces our motivating case; Section 4 presents overview of analysis of resilience of the proposed solution; Section 5, data dependence of the case is presented; Section 6 address the proposed architecture; Section 7 presents an analysis of the resilience of our incident notification solution. Finally, the paper reviews related works and concludes with a future research direction.

2 Related Work

In recent years a good amount of work on providing BPM capabilities in the cloud has appeared. It specially attracts SME's (Small and Medium Enterprise), as they now can use scalable BPM services in a pay-per-use manner without incurring large maintenance costs [9]. Major IT vendors have begun to provide cloud based BPM services, such as Salesforce's Sales cloud, Market cloud [10], IBM's Blue Works [11], Vitria's M3O [12], and a solution based upon Amazon EC2 cloud [13]. These services are at different cloud levels.

Helo et. al. [14] have proposal and implement a prototype, NetMES system for distributed manufacturing. The cloud-based solution runs on a PaaS layer in the cloud architecture. NetMES builds a manufacturing execution system on Web services and provides a standard for information sharing/transferring environment. Cloud technology is adopted in order to support monitoring, information exchange and also other real-time interactions. Our proposed BPaaS solution goes further, which does

not only treat the cloud as a platform, but also allows a collaborative business process model shared, data, and activities running among participating parties in cloud environment.

Duipmans et. al. [15, 16] present a cloud-based solution for a television broadcast organization. The organization allows users to submit their program ideas, which include users' personal information as well as text description and a short video of their ideas. The activities of the video conversion and analysis are computation-intensive activities which are assigned to the cloud. As well as video storages are allocated to the cloud. The original business processes within the organization have thus transformed into collaborating business processes. The main benefit of stockholders in choosing a cloud-based solution is that organization can utilise the flexibility of cloud resources dynamically to meet peak demand without investing in in-house resources. Their solution includes only distributed activities and related data of a process involved in a single organization. The significant difference from their work, our solution is supporting multi-partners involved collaborative business processes in cloud. Therefore, not only certainly activities and related data within an organization are running in cloud, but also each individual organisation is running a shared process collaboratively in cloud.

Chen and Hsu [17] implemented a decentralized collaborative process management system. Although collaborative process execution is based on business process model which is same as our solution, the design of an inter-enterprise collaborative business process management integrates E-Carry with E-Speak, which leads to lack of supporting of handling ad-hoc collaborative business processes in cloud. Our solution supports to support distributed collaborative processes in a flexible way, i.e. it means that the collaboration among partners are not hard code in a framework, but potential collaboration can be formed using service-oriented principles.

Our research includes the design and implementation of a business process mashup engine [18] and lightweight business process modelling language [19, 20]. Special attention is paid to the end-user aspect which is orthogonal to extending our designs for cloud based BPM. In [21] we look at data as a service in a cloud environment. The paper includes a data central solution for the same case. In our previous research, we have designed and implemented business process mashup for incident notification in a cloud environment. Further work in [22] presents a BPaaS solution for the same case. In this research, we extend a BPaaS pattern for collaborative business processes; provide more analysis of our solution; and a detailed performance evaluation.

3 Motivating Case

The Spanish electricity system is generally formed of a high-voltage electric power transmission network and grid connecting power stations and substations to transport electricity from where it is generated to where it is needed.

There are a number of stakeholders in the Spanish electricity system, each fulfilling various roles in the overall process of electricity generation and delivery. Many of the well-established, former government, parties play many of the roles in the system. The unavoidably monopolistic and critical roles of market operator

(OMEL) and system operator (REE) remain in government hands. There are three main energy producers, one market operator, three main distributors, eighteen substations, and 32 marketers [23].

The process of delivering electricity to a single customer involves the entire chain of roles (and therefore actors). The delivery of electricity to a single geographic group (for example, a street) of customers likely involves many more marketers. Given that most distributors are also active as marketers on a national level these distributors generally act both as each other's collaborators/customers and competitors.

Incidents in the electricity system can occur anywhere and anytime. These incidents, ranging from signal errors, cabling problems to serious substation overloads, will affect energy supply, lead to power cuts or even generate a further huge impact to the community and economy.

Large industrial customers directly connected to the 132kV network are generally on interruptible contracts. As their electricity demands can have significant impact on the network there is frequent and well-established contact with these customers that could be used for incident notification. Domestic customers and smaller business users however are often only known by name to marketers. The distributors and market operator generally only have knowledge of the address. As a result, domestic and small business users are currently not notified of incidents directly (for larger disruptions they may be informed indirectly through the local press).

To improve customer satisfaction, it becomes clear that effective incident management includes effective and timely informing of customers without relying on suddenly overloaded call-centers. The information provided should not only acknowledge the existence of an issue but also provide information on progress and estimated resolution timelines. When appropriate, follow-up notifications should be sent to all or interested customers.

4 Resilience

The resilience of the incident notification case is a multi-faceted problem. Resilience is required to handle normal problems, as well as abnormal problems. Normal problems are when the systems themselves continue to function properly (but need to handle external incidents and may be stretched beyond their ability to handle). Abnormal problems are when the systems to handle incidents themselves are compromised.

While the next sections focus on resilience in normal cases, this section will briefly discuss the resilience in abnormal cases. In discussing the resilience an important consideration is the degradation behaviour of the solution. Catastrophic failure as such can be defined as a failure that completely prevents the system from notifying customers. Partial degradation is when either a subset of customers cannot be notified, the notifications cannot be as detailed as required, or when a superset of affected customers is notified even if they are not affected. The incident notification systems are passive, as such worse-than-catastrophic failure with the systems actively countermanding out of bounds notification does not need to be considered.

Considering catastrophic failure, a significant driver of this would be single points of failure. Primary candidates would be either OMEL or the incident sources (such as substations). In case of substation failure, this would be rapidly noticed, not the least due to customers contacting their suppliers, but also through a sudden reduced energy usage within the network. OMEL has a unique responsibility however, and could potentially fail. Within its marketer role OMEL however already has a high-resilience infrastructure for the management of the power supply. The incident notification processes could be linked to this infrastructure. In addition, as notification by OMEL is not directly to end-users notification could be performed through human intervention by directly contacting the relevant parties (such as the distributors) based upon pre-prepared contact protocols (eg. a phone-list printed out for these cases).

For the other parties involved complete failure is less significant, with the largest impact on critical failure of marketer systems. Whereas substation information is available in multiple parts of the system (and not commercially sensitive), customer information could be only available at the marketers. The customer systems can however be split into two parts, where one part is the raw contact information (address, contact details) and the other is the marketers related systems. Given the raw contact information an alternative, cloud based, notification system can easily be used as fallback with reduced functionality (for example not taking customer contact preferences into account). As the customer details are of significant commercial value to the marketers it should be expected that regular provision of this data in escrow is feasible, if not directly in the interest of the marketers.

As to the cloud systems it is clear that these are resilient to localised failures. Unfortunately, systematic failure (eg. software errors that affect all instances) can not be excluded. The loosely coupled nature of the architecture does however mitigate this to the extent that many cases can be treated as failure of a single node in the system.

Missing parties can in general be handled through bypassing the affected parties. This does degrade the experience of incident notification but not catastrophically so. The head of the chain (OMEL) and tail (the marketers) can be handled through an existing high-resilience system (and manual intervention) in the case of OMEL and escrow of customer details in the case of the marketers. With these measures, which need to be taken into account in the detailed design and implementation of the system, the notification system can be resilient against abnormal failure.

5 Data Dependence

In terms of normal failure, it is necessary that the systems can meet their requirements even in case of an abnormally large amount of failures. A possible disruption of the energy supply, that could be caused by varying circumstances, creates the need to inform to the customers affected. According to Gas Natural Fenosa, the information sent to customers affected is not immediate. The energy-distribution area has two distinct data bases named SGC and BDI. The SGC is an operational system and contains a list of Transformers Centers (CT in Spanish) and the customers are associated with one CT. This database also contains the name of the marketer that

provides the billing service to the consumer. Therefore, a CT has several consumers and a consumer is charged by one marketer. This information allows Gas Natural Fenosa (Distributor) to charge the marketer directly for the energy consumption of this consumer. Consequently, the marketer will charge its customers using this information.

The other information system, named BDI, has information about distribution substations and contains the list of positions inside the substation. For each position, it has a CT list. Therefore, a distribution substation has several positions or lines, and each line/position has several CTs. By aggregating this information from those two sources and the list of substations affected, a list of affected customers and streets can be created. Fig. 1 shows the data dependencies involved.

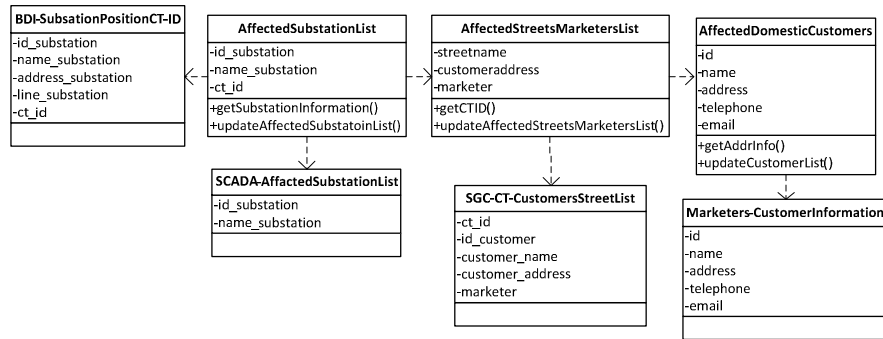


Fig. 1: Data Dependence between Distributors

The CRM stores all the information considered important in relation to the customers, offers, marketing campaigns, etc. However, the information that is needed for customer notification is just basic information about the customer such as, address, name, telephone number, etc. The list of affected customers and streets can then be combined with customer data from the CRM and used for notification.

6 Architecture of the Case

The incident notification process used as our case is based upon the use of business process oriented mashup engines. These business process oriented mashup engines are deployed for all distributors and marketers. This insures that all involved stakeholders can flexibly deal with appeared incidents (the engines can also be used for other situational applications).

Fig. 2 shows the architecture of the Cloud-based Incident Notification Process Solution (CINPS). Within the CINPS, user management provides access control for all stakeholders. The process management subsystem handles process uploading, process editing, process ranking and selection, as well as service discovery. The

service runtime management subsystems handle monitoring, reporting and service invocation at the run-time. Furthermore the CINPS also has two repositories which enumerate collaborative processes and services related to incident notification.

Business process oriented mashup engines are deployed for all stakeholders. The business process model repository contains collaborative business process models. This repository is managed by the overall system owner OMEL and enables sharing and reusing of existing collaborative process models. The business process editor allows modifying, verifying, and ranking process models. Each stakeholder has access to the process editor and is able to make changes to its processes as long as that does not compromise the integrity of the overall system. The collaborative process models can be downloaded or uploaded to the business process model repository as desired. Process models are instantiated into process instances after all data sources and invoked services are (semi-) automatically identified.

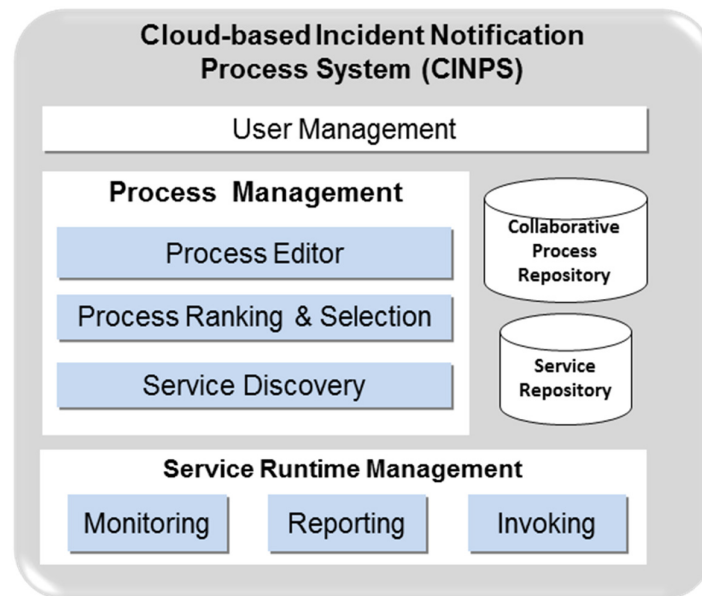


Fig. 2: Architecture of Cloud-based Incident Notification Processes

The decentralised execution of process instances is a core aspect of the incident notification system in the Spanish electricity system case. While the information needed from both distributors and marketers is not large in terms of data size (so transfer would not be a technical challenge), there are data sensitivity issues. While the information from the distributors is not commercially sensitive, the data from the marketers is. For the purpose of incident notification, marketers could download a common process model from the process model repository on the cloud. Starting with the downloaded process model, the marketers can make modifications; for example to adopt different notification channels, such as sending Facebook messages as well as

SMS messages. The marketers can use a local process editor to allocate the data (affected customers' mobile phone number, Facebook ID, or Twitter ID) and run the business process on a private process-oriented mashup engine. For the distributors, incidents or interruptions can be caused or observed in different parts of the organization. Therefore a sample process model can be modified according to the situation. The process can keep monitoring the process of the repair and ensure information is consistently published on the Web using the private process engine. Fig. 3 presents such a process model.

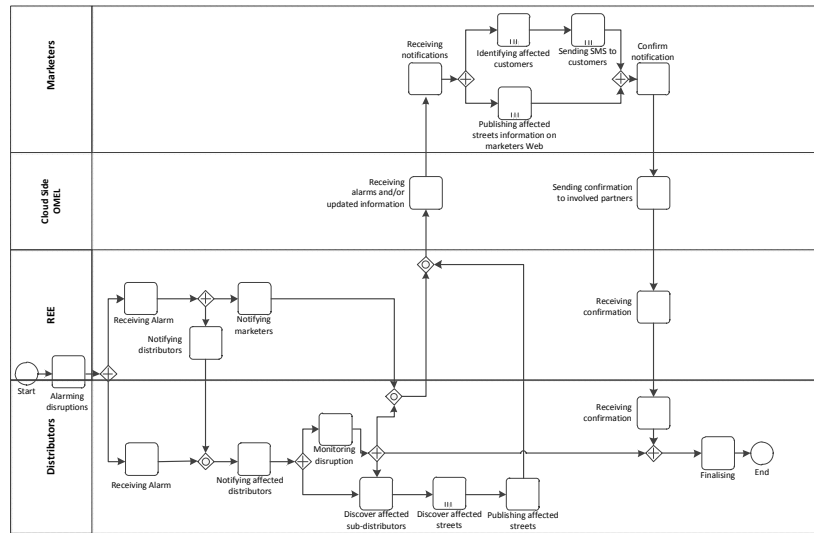


Fig. 3: Cloud-based Incident Notification Process Model for SES

The solution owner (in this case OMEL) mainly concentrates on maintaining the process model repository and on providing some common Web services. OMEL also provides a process editor and a process engine for users testing the process model. The other users are certainly able to upload their data for running their processes in case the private process engine is out of order. A collaborative process which runs in the cloud can be supported for special cases, e.g. monitoring the collaborative process.

7 Resilience of Incident Notification Solution

Marcon et al [8] deal with an on-going authorization model UCN_{ABC} , which provides resilience to the re-evaluation of usage policies of individual users. The meaning of resilience is providing the model with the ability to deal with some individual user authorization attributes exceeding, while the SLA for the respective consumption

service is under the contracted amount. Our proposed resilience model is adapted from that paper.

Let R be the resilience of the solution. SLA is a service level agreement of the maximum time to notify domestic customers. $T(i)$ represents the process notification time of each partner. The resilience of the incident notification solution is defined only if SLA minus the sum of time cost of each partner for processing the incident is greater than t . The constant is a spare quota freely defined by the consumer for the notification services.

$$R: \exists \left[\left(SLA - \left(\sum_{i=1}^n T(i) \right) \right) > t \right]$$

In this solution, all involved partners have process engines installed, creating redundancies throughout. The solution could hold extra computing power in case of certain failure. In CINPS, notification or maintenance processes can be triggered by REE, distributors, substations, or OMEL.

For the Spanish Electricity System, there are three main energy producers, one OMEL, three main distributors, eighteen substations, and 32 marketers. We assume that it takes 10 minutes for distributors, substations, and REE and takes 5 minutes to process incident notification activities respectively. These are worst-case estimates, where the 10 minutes involves human action, and the 5 minutes is the time required to send all text messages.

There are three main distributors. If all of them are in danger, i.e. $a=3$, it takes in total $10 \sum_{i=1}^a i$ minutes. It can also apply to all substations. If all of them are in danger, i.e. $b=18$, it takes in total $10 \sum_{j=1}^b j$ minutes. Notifying OMEL, REE and markets needs 10+10+5 minutes and sending all messages to customer needs 5 minutes. Therefore, the resilience model for the worse case of incidents is presented as follow,

$$R: \exists \left[\left(SLA - \left(20 + 10 \sum_{i=1}^a i + 10 \sum_{j=1}^b j \right) \right) > t \right], (0 < a \leq 3, 0 < b \leq 18)$$

Table 1 shows total time of processing incident notification, i.e. $20 + 10 \sum_{i=1}^a i + 10 \sum_{j=1}^b j$. The row represents how many substations have trouble. The column indicates how many main distributors are in trouble. This table can be used to determine SLA.

Table 1: Total Time Cost of Different Incident Sizes

(b,a)	0	1	2	3	4	5	6	7	8	9
0	0	10	30	60	100	150	210	280	360	450
1	10	20	40	70	110	160	220	290	370	460
2	30	40	60	90	130	180	240	310	390	480
3	60	70	90	120	160	210	270	340	420	510

(b,a)	10	11	12	13	14	15	16	17	18
0	550	660	780	910	1050	1200	1360	1530	1710
1	560	670	790	920	1060	1210	1370	1540	1720
2	580	690	810	940	1080	1230	1390	1560	1740
3	610	720	840	970	1110	1260	1420	1590	1770

The x-axis of Fig. 4 presents the numbers of substations in danger; y-axis of Fig. 4 notes the number of main distributors in dangers; and z-axis of Fig. 4 presents total time of processing incident notification in minutes.

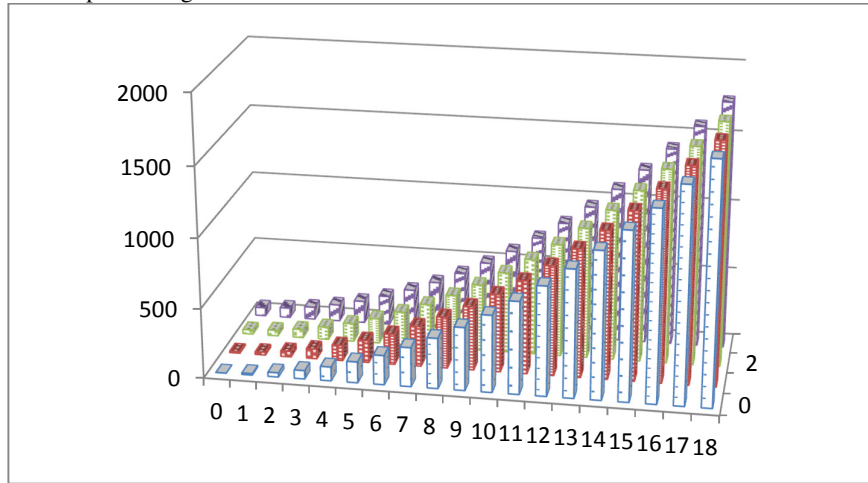


Fig. 4: Total Time Cost of Different Incident Effect

8 Conclusion

Cloud-based BPM systems bring many benefits to business users. They provide a good opportunity for organizations which seek scalable and flexible solutions. Cloud-based BPM systems are not likely to replace all local BPM systems. To achieve business agility business process collaboration needs to seamlessly connect local BPM systems and cloud-based BPM systems. Business process models as assets for many organizations are important to supporting business agility. The lightweight business process modeling technologies, lightweight business process mashup engines, and large collections of process models are providing possible solutions for end-user oriented BPM and BPaaS.

In this paper, we have provided an analysis of the resilience of a BPaaS solution to incident notification in the electricity supply market. Careful design with manual overrides allows for graceful degradation (in some cases only resulting in - short - additional delays due to manual processes). We have addressed both abnormal failures, where the system itself is compromised, as normal failures where the electricity supply is compromised, but not the notification system. It is clear that the system can be designed to be highly resilient, only to fail in extreme circumstances.

These circumstances however are likely to be such extreme that traditional broadcast solutions (radio cars, door-to-door leaflets) are acceptable.

The use of loosely coupled cloud solutions provides for resilience and fallback, effective cooperation while not limiting competition, innovation and variety in the usage by the parties involved.

Effective incident management can be considered as a more cost-effective solution to reduce the negative impact on the community and economy after an industrial incident occurs. From the end-user perspective, this relies on instant situation awareness and response. The core concept of the architecture is that it uses verified incident notification process models and a business mashup engine to help organizations respond to emerging situations triggered by incidents more intuitively. The architecture also supports on-demand and flexible situational applications which are used to address timely and immediate customer needs. The case study has demonstrated how BPaaS for collaborative processes facilitate in solving a real world problem effectively. Further, we propose a resilience model to show how to determine resilience of our cloud based BPM solution.

Acknowledgments. This work is made possible by the support of the Natural Science Foundation of China (NSFC) under Grant No.61150110484, ESSENTIAL: Enterprise Service deSign based on ExistiNg software Architectural knowLedge, the National Basic Research Program of China under Gran No. 2014CB340404, and FIF Strengthening Service Computing Research in Bournemouth University, UK.

References

1. Bouvry, Pascal. "Emerging Paradigms and Areas for Expansion." *Cloud Computing*, IEEE 1, no. 1 (2014): 58-61.
2. Sun, Yutian, Jianwen Su, and Jian Yang. "Separating Execution and Data Management: A Key to Business-Process-as-a-Service (BPaaS)." In *Business Process Management*, pp. 374-382. Springer International Publishing, 2014.
3. Zhang, Liang-Jie, and Qun Zhou. "CCOA: Cloud computing open architecture." In *Web Services, 2009. ICWS 2009. IEEE International Conference on*, pp. 607-616. Ieee, 2009.
4. Radulescu, Corina, Hui Min Tan, Malini Jayaganesh, Wasana Bandara, Michael zur Muehlen, and Sonia Lippe. "A framework of issues in large process modeling projects." In *ECIS*, pp. 1594-1605. 2006.
5. Dijkman, Remco M., Marcello La Rosa, and Hajo A. Reijers. "Managing large collections of business process models-current techniques and challenges." *Computers in Industry* 63, no. 2 (2012): 91-97.
6. Campbell, Flake C., ed. *Elements of metallurgy and engineering alloys*. ASM International, 2008.
7. Sheffi, Yossi. "Building a resilient supply chain." *Harvard Business Review* (2005): 1-4.
8. Marcon, Arlindo Luis, A. Olivo Santin, Maicon Stihler, and Juliana Bachtold. "A UCON_{ABC} Resilient Authorization Evaluation for Cloud Computing." *Parallel and Distributed Systems*, IEEE Transactions on 25, no. 2 (2014): 457-467.
9. Buyya, Rajkumar, Chee Shin Yeo, and Srikumar Venugopal. "Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities." In *High Performance Computing and Communications, 2008. HPCC'08. 10th IEEE International Conference on*, pp. 5-13. IEEE, 2008.

10. Salesforce, "Salesforce: Sales Cloud, Marketing Cloud", 2012.
11. IBM, "Blueworkslive", 2013.
12. VitriaCloud, "VitriacLOUD m3o in the cloud", 2013
13. Amazon, "Amazon elastic compute cloud (amazon ec2)", 2013
14. Helo, Petri, Mikko Suorsa, Yuqiuge Hao, and Pornthep Anussornnitisarn. "Toward a cloud-based manufacturing execution system for distributed manufacturing." *Computers in Industry* 65, no. 4 (2014): 646-656.
15. Duipmans, Evert F., Luis Ferreira Pires, and Luiz Olavo Bonino da Silva Santos. "Towards a BPM cloud architecture with data and activity distribution." In *Enterprise Distributed Object Computing Conference Workshops (EDOCW), 2012 IEEE 16th International*, pp. 165-171. IEEE, 2012.
16. Duipmans, Evert Ferdinand, Luis Ferreira Pires, and Luiz Olavo Bonino da Silva Santos. "A transformation-based approach to business process management in the cloud." *Journal of grid computing* 12, no. 2 (2014): 191-219.
17. Chen, Qiming, and Meichun Hsu. "Inter-enterprise collaborative business process management." In *Data Engineering, 2001. Proceedings. 17th International Conference on*, pp. 253-260. IEEE, 2001.
18. de Vrieze, Paul, Lai Xu, Athman Bouguettaya, Jian Yang, and Jinjun Chen. "Building enterprise mashups." *Future Generation Computer Systems* 27, no. 5 (2011): 637-642.
19. Xie, Li, Lai Xu, and Paul de Vrieze. "Lightweight business process modelling." In *E-Business and E-Government (ICEE), 2010 International Conference on*, pp. 183-186. IEEE, 2010.
20. Lai Xu, Paul de Vrieze, Keith Phalp, Sheridan Jeary, Peng Liang. "Lightweight Process Modeling for Virtual Enterprise Process Collaboration". In: *IFIP Advances in Information and Communication Technology Volume 336, 2010*, pp 501-508.
21. Jiang, Nan, Lai Xu, Paul de Vrieze, Mian-Guan Lim, and Oscar Jarabo. "A cloud based data integration framework." In *Collaborative Networks in the Internet of Services*, pp. 177-185. Springer Berlin Heidelberg, 2012.
22. Xu, Lai, Paul de Vrieze, and Nan Jiang. "Incident Notification Process as a Service for Electricity Supply Systems." In *2013 IEEE 6th International Conference on Cloud Computing (CLOUD)*, pp. 926-933. IEEE, 2013.
23. Bilbao, J. Bravo, E. Garcia, O. Varela, C. Rodriguez, M. Gonzalez, P. International *Journal on Technical and Physical Problems of Engineering*. 9(3), 2011, pp 91-96.