Spring 6-15-2016

BUSINESS INTELLIGENCE FOR BUSINESS PROCESSES: THE CASE OF IT INCIDENT MANAGEMENT

Niklas Goby
University of Freiburg, niklas.goby@is.uni-freiburg.de

Tobias Brandt
University of Freiburg, tobias.brandt@is.uni-freiburg.de

Stefan Feuerriegel
University of Freiburg, stefan.feuerriegel@is.uni-freiburg.de

Dirk Neumann
University of Freiburg, dirk.neumann@is.uni-freiburg.de

BUSINESS INTELLIGENCE FOR BUSINESS PROCESSES: THE CASE OF IT INCIDENT MANAGEMENT

Complete Research

Goby, Niklas, University of Freiburg, Freiburg, Germany, niklas.goby@is.uni-freiburg.de
Brandt, Tobias, University of Freiburg, Freiburg, Germany, tobias.brandt@is.uni-freiburg.de
Feuerriegel, Stefan, University of Freiburg, Freiburg, Germany, stefan.feuerriegel@is.uni-freiburg.de
Neumann, Dirk, University of Freiburg, Freiburg, Germany, dirk.neumann@is.uni-freiburg.de

Abstract

IT service desks have become an integral part of intra-enterprise ecosystems, keeping IT hardware and software services within the company running. Business Intelligence methods have an enormous potential to support IT helpdesk employees by making implicit knowledge explicit, accelerating business processes throughout the entire company, and retaining the knowledge of experienced employees upon retirement. In this paper, we investigate these benefits by showing how analytics can automate the assignment of helpdesk tasks, enable early warning mechanisms for accumulated incidents, and enhance knowledge sharing among helpdesk users. For this purpose, we use a combination of topic modeling and predictive analytics, which is applied to an extensive dataset of support tickets from a global automotive supplier. Our approach identifies relevant topics and assigns these to helpdesk tickets, thereby decoding implicit knowledge into formal rules and business processes.

Keywords: Knowledge Management, Business Intelligence, Business Process Engineering, Text Mining, IT Incident Management, Decision Support, Case Study, Latent Dirichlet Allocation

1 Introduction

Over the past decades, Information Technology (IT) services have become an essential part of enterprise operations (Iden and Eikebrokk, 2013). Consequently, the efficient operation of these services represents a crucial component of corporate success, reflected in the vast IT support (or IT helpdesk, IT service desk) departments found at medium-sized and large companies. The purpose of service desk employees is to support other departments with problems arising from the introduction and use of hardware and enterprise software products.

In this paper, we build upon previous works related to IT incident management (e. g. Diao, Jamjoom, and Loewenstern, 2009; Kadar, Wiesmann, Iria, Husemann, and Lucic, 2011; Maksai, Bogojeska, and Wiesmann, 2014). We contribute to the existing literature by showing how text mining methods can support knowledge management in IT helpdesk departments from two perspectives. On the one hand, the often repetitive nature of manual assignment tasks (which ticket should be processed by which group within the department) leads over time to a build-up of knowledge regarding which group handles specific types of tickets best. In the current model, this knowledge is lost once a long-time employee leaves the company. On the other hand, in cases of large-scale incidents, individual tickets contain a kind of spontaneous knowledge on the occurrence of this emergency that is only visible when tickets are

considered from an aggregate perspective. Individual employees are unaware of other tickets on the same topics and the dimension of the incident.
As a remedy, we utilize a combination of Latent Dirichlet Allocation (LDA) and ensemble learning to make this knowledge explicit by identifying and assigning tickets to topic clusters. Through the use of a software solution, knowledge regarding ticket allocation is separated from specific employees and sudden changes in topical clusters creates improved awareness of large-scale incidents. Hence, our approach translates into the following objectives:

- **Problem prevention**. Uncover automation potentials, such that users are enabled to solve certain problems on their own. Enable early warning mechanisms for large-scale incidents.
- **Solution acceleration**. Decision support and automated assignment.
- **Organizational learning**. Retain knowledge of employees in the company and uncover improved organizational structures.

We substantiate our research using the showcase of a global automotive supplier. However, the insights gained in this paper are applicable to a broad range of large companies facing similar problems. Throughout the study we follow the Cross Industry Standard Process for Data Mining, CRISP-DM, as shown in Figure 1 (Chapman et al., 2000).

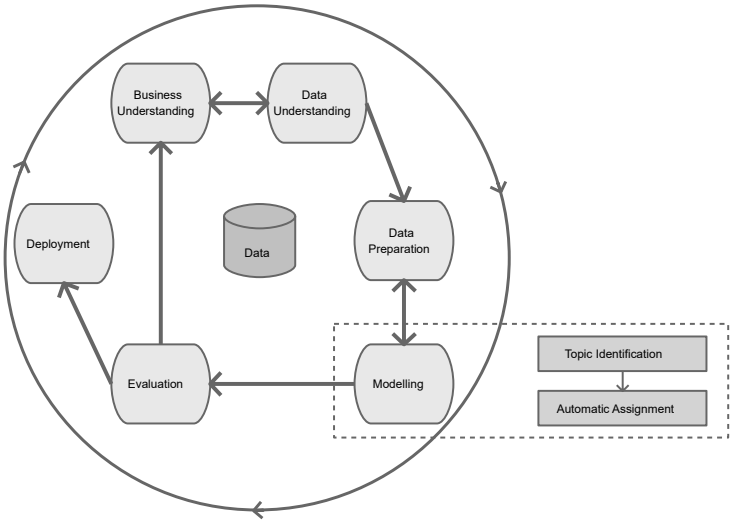

Figure 1. Iterative CRISP-DM (Cross Industry Standard Process for Data Mining and Used Methods) process adapted to our modeling as part of improving IT incident management.

Our paper is structured as follows. Section 2 provides an overview of related works. Section 3 introduces the dataset we analyze and the methods we employ. Section 4 introduces the case study and contains the actual application of the methods to the dataset, while we discuss the results in Section 5. Section 6 provides a conclusion and an outlook.

2 Related Work

This section presents related literature grouped according to three research streams: first, we present applications of text mining for knowledge management. Second, we focus on studies related to IT service management and, third, revisit previous publications that propose the use of analytics for IT incident management. This survey reveals a research gap and thus sheds light on the motivation for our work.

2.1 Applications of Text Mining for Knowledge Management

Today's fierce competition forces companies to collect literally all the data associated with that company (Turban, 2011). Effectively, any interactions with customers, as well as the entire production process, are extensively documented, resulting in massive data collections. Transforming the huge amount of knowledge implicitly contained in this data into valuable explicit knowledge is a challenging task (Berson, Smith, and Thearling, 1999). Therefore, organizations are constantly looking for ways to improve their knowledge discovery process.
In the case of unstructured data, text mining methods can be applied, for instance, to classify documents according to their quality of information (Ur-Rahman and Harding, 2012), cluster documents to create a representation of the underlying knowledge flow (Liu and Lai, 2011), or create value-adding content (Kruse, Schieber, Hilbert, and Schoop, 2013; Thorleuchter, van den Poel, and Prinzie, 2010). What these studies have in common is that the combination of text mining and knowledge management is shown to be a powerful tool that can help people or companies to become more effective and efficient.

2.2 IT Service Management

As this study deals with the domain of IT incident management, we introduce the underlying concept in the following. IT incident management belongs to the domain of *IT service management* (ITSM), which is implemented, for instance, as part of the *Information Technology Infrastructure Library (ITIL)*. Both have been research subjects of numerous studies in the past; for instance, Iden and Eikebrokk (2013) present a structured literature review in which the authors provide an overview of on-going research activities in this field. Accordingly, most studies are of empirical nature and address questions such as the following:

- Success factors for implementation (Cater-Steel, 2009; Cater-Steel and McBride, 2007; Cater-Steel, Tan, and Toleman, 2006; Hochstein, Tamm, and Brenner, 2005; Iden and Langeland, 2010; Kanapathy and Khan, 2012; Marrone and Kolbe, 2011a; McBride, 2009; Mohammed, 2008; Pollard and Cater-Steel, 2009; Tan, Cater-Steel, and Toleman, 2009; Wan and Wan, 2011)
- Implementation strategies (Arora and Bandara, 2006; Cater-Steel and McBride, 2007; Jin and Ray, 2008; McBride, 2009; Mohammed, 2008; Pollard and Cater-Steel, 2009; Wagner, 2006)
- Outcomes and implementation benefits (Cater-Steel, 2009; Disterer, 2012; Hochstein, Tamm, and Brenner, 2005; Marrone and Kolbe, 2011a; Marrone and Kolbe, 2011b; Wan, 2008)
- Performance measurement (Gacenga, Cater-Steel, Tan, and Toleman, 2011)
- How ITIL affects IT governance, as well as IT/business alignment (Duffy and Denison, 2008; Kashanchi and Toland, 2006; Lapão, 2011)

In addition, further studies focus on discussions about critical success factors and performance indicators for ITIL (Neničková, 2011), evaluation frameworks for ITSM efforts (McNaughton, Ray, and Lewis, 2010), standardization issues (Kumbakara, 2008; Mesquida, Mas, Amengual, and Calvo-Manzano, 2012) and ITSM process improvements (Galup and Dattero, 2010). In contrast, only a few studies actually address how knowledge management can be integrated into the IT service architecture (Nabiollahi, Alias, and Sahibuddin, 2011). This thus lays the groundwork for the following research objective.

2.3 Business Intelligence for IT Incident Management

In the field of Business Intelligence, we found only a few similar studies related to IT incident management. Among them, Maksai, Bogojeska, and Wiesmann (2014) investigate the labeling of tickets that are server-side and system-generated. Their approach draws on a hierarchical clustering in combination with a Latent Dirichlet Allocation and then compares it with other algorithms. Ultimately, their goal is to reduce manual labeling effort with consistently good predictive performance.

In a similar fashion, Diao, Jamjoom, and Loewenstern (2009) focus on problem-related tickets and develop a rule-based classifier which outperforms supervised learning methods when manual labeling is too costly. The authors use the resolution text for their analysis with the purpose of supporting the analysis of the true root cause and monitoring of failure trends (Kadar, Wiesmann, Iria, Husemann, and Lucic, 2011). Since we analyze user-reported issues, a rule-based classifier seems unsuitable in our case, since we cannot rely on a standardized format of the content within the tickets.

Several works focus on the methodological choices and compare different variants. For instance, Kadar, Wiesmann, Iria, Husemann, and Lucic (2011) present three approaches for classifying change requests. In their semi-supervised setting, the authors use the Latent Dirichlet Allocation (LDA) to discover topics and cluster unlabeled data. In addition to that, Di Lucca, Di Penta, and Gradara (2002) compare different machine learning classifiers such as support vector machine, decision trees, *k*-nearest neighbor and probabilistic models both with and without a reinforcement strategy. Similar to our set-up, their dataset consists of error-reporting logs with short texts in natural language. Despite this, they show that the first few words are enough to classify a ticket and assign it to the desired support team with relatively high accuracy. In contrast, we use a two-step approach whereby we first identify topics and corresponding service groups according to business needs and then automate the ticket assignment in a real company.

Based on these findings, our research was motivated as follows. None of the reviewed studies could satisfy our needs regarding the diagnosis of an automated incident management process for IT helpdesk ticket. Although some approaches seem promising, we decided that our unique set-up, with user-reported incidents in natural language and more than 300 support groups in the status quo, requires a comprehensive yet tailored approach which we present in the following.

3 Dataset and Methods

In brief, Figure 2 shows the overall process. First, we filter the ticket database to select relevant user issues in English. The resulting corpus is then transformed into a matrix representation. This then serves as input for the topic modeling via Latent Dirichlet Allocation and the random forest classification.

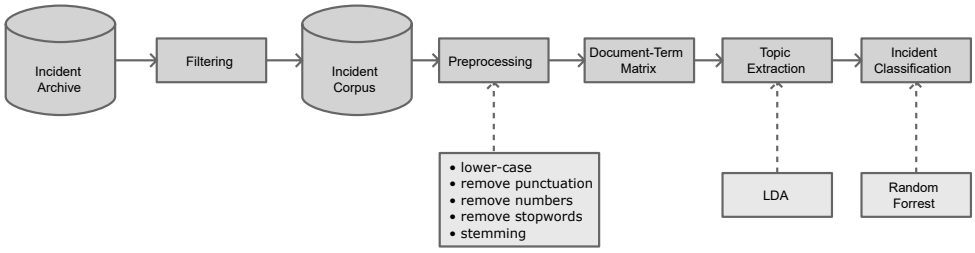

Figure 2. Process chart visualizes research model to improve IT incident management with the help of Business Intelligence.

3.1 Ticket Database

For this research, we have been granted access by our partner firm to their IT incident management system. The firm is a large German supplier in the automotive industry, employing around 140,000 people worldwide. This allows us to apply our research not only to a large dataset but also to provide evidence of how analytics can fundamentally improve business processes and knowledge retention in a real case study.

• Affected end-user	• Description	• Reporter
• Affected helpdesk	• Due date	• Resolution
• Archive date	• End-user details	• Resolution date
• Assigned group	• Id	• Root cause
• Assignee	• Impact	• Status
• Caller	• Incoming data	• **Summary**
• Caller details	• Last modified by	• Time zone
• Component	• Participant	• Type
• Configuration item	• Primary key	• Update
• Configuration item details	• Priority	• Urgency
• Created	• Project	• Workaround solution

Table 1. Variables describing a ticket within the database (in alphabetical order).

Our database describes each ticket in terms of 33 variables, presented in Table 1. Variables such as *summary* or *description* are filled out by the ticket creator. All other variables are automatically generated by the system or completed by the support team during the resolution process. Due to privacy policy law restrictions, all personal information is sanitized. All tickets originate from January through December 2014, accounting for a total of 425,936 tickets. This corresponds to an average of approximately 1166.95 tickets per day. In the following, we further filter the dataset by removing 75,999 tickets which have been generated by the system itself. This results in 349,937 tickets reporting IT-related problems. As the company is currently transitioning towards a single global helpdesk that employs English as the ticket language, we are interested only in English tickets. We utilize a heuristic to identify the language, yielding a final dataset of 35,495 tickets. This number is several times higher than any dataset used in related works (see Section 2).

In order to get a better understanding of ticket management, we investigate ticket lifetime in the following. Figure 3 shows a bar chart with the average lifetime, cropped to a maximum of 50 hours. We can see that almost 5000 tickets are resolved within less than 30 minutes; a total of approximately 8000 tickets are closed in less than 1.5 hours. The median value accounts for 24 hours, while the average is 213.8 hours with a standard deviation of 696.1 hours. This indicates a skew distribution with a long tail. For instance, the maximum time needed to resolve a ticket was 11,020 hours.

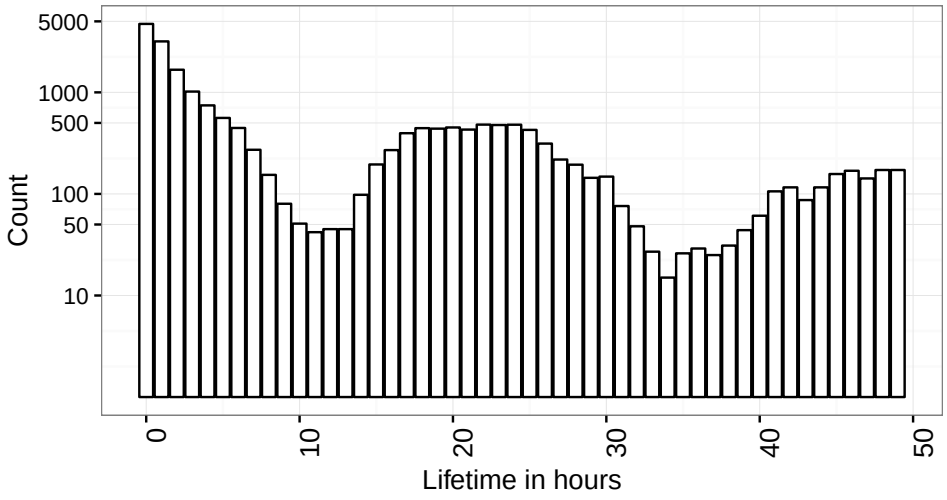

Figure 3. Ticket lifetime until resolution in hours (cropped to a maximum of 50 h; frequency as log-scale).

3.2 Preprocessing

We choose the running text originating from the summary field of the tickets as our predominant decision criterion. In fact, we ignore the detailed description which is collected alongside the ticket process for several reasons. For instance, long texts reduce noise and, on the other hand, short texts are sufficient to achieve acceptable results (Di Lucca, Di Penta, and Gradara, 2002). In addition, the detailed description is usually either empty or contains the same information as the summary. In the following, we first transform the running text into a matrix representation, the so-called *document-term matrix*. This matrix subsequently works as the input to the actual algorithms. In detail, we perform the steps as follows.
First of all, we remove numbers, punctuation and stop words from the running text and then split it into tokens and stem these (Manning and Schütze, 1999). Afterwards, we count the frequencies of how often terms occur in each ticket summary, remove sparse entries to reduce the dimensionality and store these values in a document-term matrix. The document-term matrix then represents the features. The actual values are weighted (Salton, Fox, and Wu, 1983) by the *term frequency-inverse document frequency* (tf-idf). This is a common approach in information retrieval to adjust the word frequencies by their importance.

3.3 Topic Modeling using Latent Dirichlet Allocation

One frequently utilizes the *Latent Dirichlet Allocation* (LDA) in text mining in order to perform topic modeling. The LDA is a generative probabilistic model (Blei, 2012), which assumes K pre-specified topics $\beta_{1:K}$ across all D tickets. While the topics themselves are not directly observable, one can only unveil the hidden structure, i. e. the topic distribution over each ticket and the topic assignment over each ticket and each word, given the observed tickets. Then, each topic β_k is defined as a distribution over a fixed vocabulary w_d in document d.
Let θ_d denote the distribution of topics for ticket d, while z_d gives the topic assignment for all words in d. Then, it is a computational problem to calculate the posterior distribution $P(\beta_{1:K}, \theta_{1:D}, z_{1:D} \mid w_{1:D})$. Since the number of topic structures is exponentially large, its value cannot be computed in practice. A remedy is the use probabilistic models, such as the Latent Dirichlet Allocation, that aim to approximate the posterior. This approximation can be achieved, for example, by the use of a variational expectation-maximization (EM) algorithm (Hornik and Grün, 2011). More precisely, the word count in each ticket follows a Poisson distribution, the distribution of topics $\theta_{1:D}$ is from Dirichlet distribution and the topic assignment for each word in each document $z_{d,n}$ follows a multinomial distribution (Blei, Ng, and Jordan, 2003).
In this paper, we employ a state-of-the-art method (Yi and Allan, 2009), the Latent Dirichlet Allocation, rather than a Latent Semantic Analysis (LSA). The LSA has received heavy criticism lately due to its inadequate statistical foundation. In fact, the LSA erroneously assumes Gaussian noise on term frequencies, which empirically follow a Poisson distribution. The extension of the LSA, the probabilistic version of the LSA (pLSA), regards each word in a document as a sample from a mixture model representing different topics. The pLSA thus models the probability that word-document combinations occur as a mixture of conditionally independent multinomial distributions. However, the pLSA model is also incomplete, as it provides no statistical model at the document level. It can be shown that this limitation results in severe overfitting. However, the LDA addresses this shortcoming by using a Dirichlet prior for the topic distribution within documents (Blei, Ng, and Jordan, 2003).

3.4 Ticket Assignment with Predictive Analytics

One common approach to classification tasks is the so-called *random forest* (Breiman, 2001). In the following evaluation, we utilize random forests as a benchmark classifier. Random forests represent one of the most popular machine learning algorithms due to their favorable predictive accuracy, relatively low computational requirements and robustness (Breiman, 2001; Hastie, Tibshirani, and Friedman, 2009).

Random forests are an ensemble learning method for classification and regression, which is based on the construction and combination of many de-correlated decision trees.
Given a training set $X = \{x_1, \ldots, x_N\}$ with associated responses $Y = \{y_1, \ldots, y_N\}$, the algorithm repeats the following steps B times (we choose $B = 500$):

1. Sample with replacement from X and Y to generate new subsets X' and Y'.
2. Train a decision tree t_b using X' and Y'.

The individual decision trees t_b, $b = 1, \ldots, B$, can be combined to predict a response $\hat{y}$ for unseen values x as follows. One calculates individual predictions $t_b(x)$, $b = 1, \ldots, B$, from each tree and then aggregates these predictions by simply using the majority vote to get the final response.

4 Case Study: Improving IT Incident Management with Business Intelligence

In the following, we present a real case study as implemented by our collaborating partner in order to improve their knowledge-intensive process of IT incident management.

4.1 Description of Case Study

In this case study, we have closely collaborated with our partner firm in order to utilize Business Intelligence as a lever for improving process performance and retain, respectively uncover, knowledge hidden in the tickets. Hence, we conducted several interviews with the IT leadership of our partner firm, ultimately concluding that the current incident management constitutes an expensive undertaking.
The current process is modeled via a ticket system whereby users can report issues that are then handled by the IT department. The incident management process follows the *Information Technology Infrastructure Library* (ITIL) standard and can be briefly described as follows: users who experience issues report these to the helpdesk. The support team then identifies the problem and classifies the ticket according to a pre-defined list of around 300 categories. If the issue can be resolved directly, the support team will do so; otherwise, the ticket will be assigned to a second-level support group. In either case, the resolution is documented inside the ticket and the user is informed as soon as the ticket is resolved.
However, the current process entails several major drawbacks:

1. The process is error-prone since users sometimes assign topics to the wrong categories, resulting in significant delays until resolution.
2. The assignment process is fully non-automated and thus demanding intensive manual labor. Because of the high number of different support groups, the presence of expert knowledge is crucial and has thus increased the cost of staff training in the past.
3. All issues are resolved by humans. Many tickets are relatively easy to solve but, nevertheless, their manual resolution is tedious work. However, even for standardized problems, such as installing software or a password reset, no automated process exists thus far.
4. The system does not feature a mechanism for event detection when a high number of (similar) incidents accumulates. Accumulations indicate deeper problems, which stay undetected most of the time until solutions become challenging and expensive. Today, a coordinated communication effort between employees is necessary to detect such clusters manually. As an alternative, an automated mechanism could improve the quality of the support process drastically.

As a solution to the aforementioned problems, we decided in concert with our industry partner to develop and implement the following Business Intelligence application. Based on our previous literature review in Section 2, we identified several business applications in the IT incident management field that could benefit from advanced analytics as presented in the following section.

4.2 Approach Based on CRISP-DM Process

During this research project, we have been in close contact with the department dedicated to providing third-level IT support. This department actually fulfills two roles: they not only resolve incidents as support team members, but also create incidents themselves when they experience shortcomings in the software landscape. Altogether, the leadership of the partner firm regards IT not only as a supporting instrument but aims at evolving IT as an enabler.

The subsequent application of Business Intelligence was jointly developed and implemented with the partner firm. The predominant goal was to improve incident management with regard to several quality indicators. While this describes the overall objective, we now present the underlying process of how we improved the IT incident management process. Due to the data-intensive characteristics and unknown outcome, we decided to apply an iterative process, namely, the *Cross Industry Standard Process for Data Mining*, CRISP-DM for short (Chapman et al., 2000). We followed the CRISP-DM approach closely and, in the following, present the final outcome of our proposed methodology.

Based on the drawbacks presented in the previous section and our experience with the department, we derived the following user stories:

- *"As a Support Team Member, I want a mechanism that helps me to identify the best-suited support group that can resolve the issue because I am interested in a fast solution and I want to avoid false assignments which prolong the process."*
- *"As a Support Team Member, I want to analyze tickets with the same topic among all support groups within the company in order to detect ticket accumulations as early as possible and with high likelihood."*
- *"As a Support Team Member, I want a system that empowers users to solve simple issues by themselves and reduces the possible causes of issues, so that the total number of tickets is reduced."*

These requirements match with our goal of revealing knowledge based on the ticket system in order to improve the process of incident management. The actual approach to achieve this goal can be briefly summarized as follows: we first identify the number of desired support groups or specializations based on the business context. We then utilize a method for topic modeling to extract the underlying themes within the tickets. One then inspects the most prominent words of each topic in order to determine the overall category and assign this to a support group or specialization. Finally, we train a predictive model to automatically infer the pre-defined assignment from the textual content of a ticket. We provide evidence that our approach has a satisfying accuracy by evaluating its predictive performance on a test set.

4.3 Data Understanding

We pursue an exploratory approach in order to first obtain an understanding of our corpus. For this purpose, we utilize hierarchical clustering, which groups similar information from the summary field of the tickets based on the distance between words within a corpus. More precisely, we create a dendrogram from the term-document matrix using Ward's clustering method together with an Euclidean distance.

The result is shown in Figure 4, where the similarity of words provides information about how they are clustered together. At first glance, we observe words, such as *malwareadwar* and *potenti*, that are located relatively close to one another. The same is valid for the big clade in the middle with words like *pleas*, *user* and so on. In addition, the distances of the leaves *full*, *administr* and *control* seem relatively small, thus suggesting another cluster. According to Figure 4, we can identify further large-scale groups. For example, the clade on the left also forms a potential cluster with words related to installing software, while the big clade on the right seems as though it might require further splitting operations in order to have suitable, self-explanatory clusters.

Altogether, this gives a first indication of how possible clusters can be formed from the content. Based on our explanatory insights, our findings suggest that a small number of around five to seven clusters can provide a good starting point for the subsequent topic modeling.

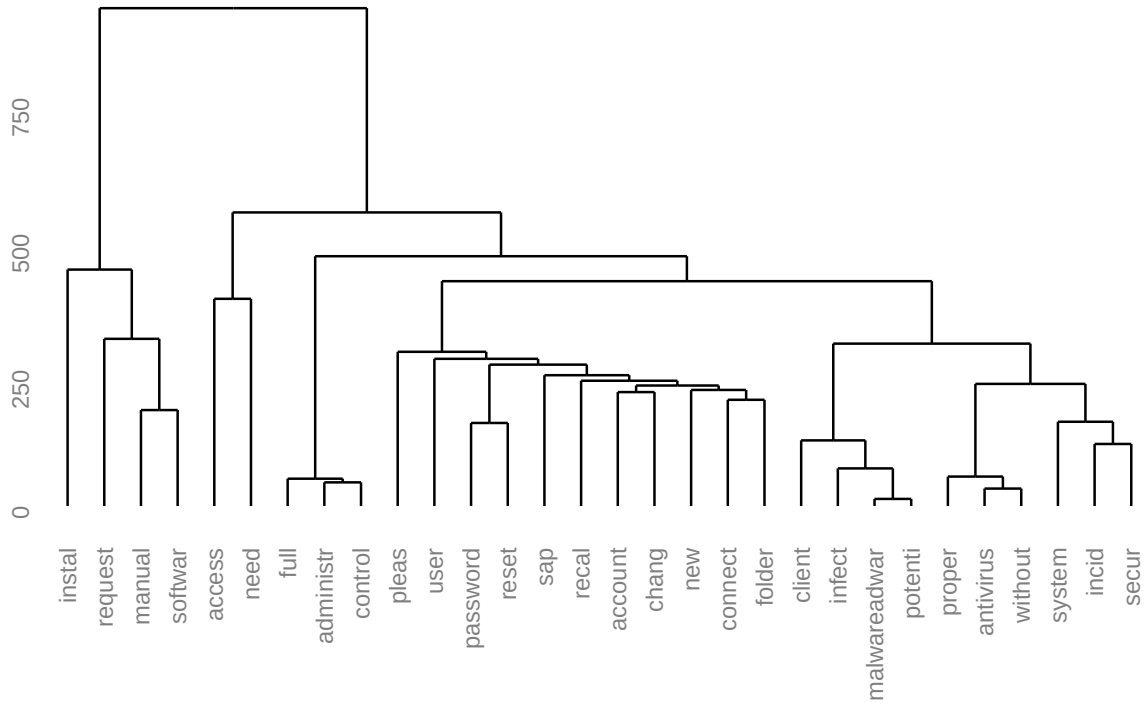

Figure 4. Dendrogram with a hierarchical clustering of words.

4.4 Business Needs: Service Groups and Ticket Assignment

To perform topic modeling, we have to choose the number of topics and service groups in advance, which entails a trade-off between business needs and statistical indications. The Latent Dirichlet Allocation is different from other machine learning algorithms where one optimizes, for example, the number of clusters by cross-validation or heuristics. In contrast, we have to choose the number of extracted topics *ex ante*. We present in the following our arguments for having decided to run our analysis with 5 topics extracted from the underlying corpus. This choice is justified by our interviews with members of the helpdesk, the IT management and additional experiments (see Figure 5) in which we varied the number of topics. We also tested a wide range, from merely 3 topics up to 100 topics, finding affirmative insights as follows:

- Each topic should reflect the skills and expertise of a service group. For fewer than 5 topics, we quickly run into problems since job requirements are not mutually exclusive and collectively exhaustive. Furthermore, important and inseparable topics are merged together. As a consequence, we cannot distinguish or name certain topics and, in addition, we lose several topics. However, we want to include these topics specifically and believe that too small a number of topics might lead to an oversimplified model.
- When allocating more than 5 topics, the service groups become highly specialized. While this might seem a benefit at first glance, it causes severe problems when balancing the degree of capacity utilization of each service group over time. In addition, more service units necessitates a rearrangement

of office space, resulting in additional cost drivers. Furthermore, the Latent Dirichlet Allocation seems to find problem-specific topics rather than topics that are logically similar in terms of IT knowledge.

Keeping the above business needs in mind, we decided to set the number of topics to 5 throughout the case study.

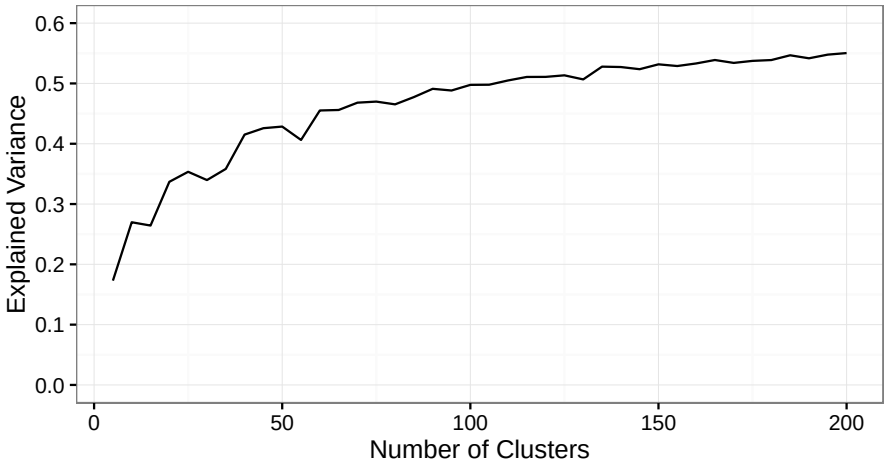

Figure 5. Elbow plots explaining variance for each number of clusters from k-means algorithm; even a small number of topics provides a relatively good fit to the underlying cluster structure with only minor improvements for a large number of clusters.

Topic 1: Malware Detection	**Topic 2: Credentials**	**Topic 3: Access Request**	**Topic 4: Software Installation**	**Topic 5: Administrator Rights**
incid	password	access	instal	full
secur	pleas	need	softwar	control
client	reset	folder	manual	request
infect	account	drive	request	administr
potenti	user	file	sap	instal
malwareadwar	sap	workstat	dokument	system
extend	new	share	teamcent	secur
permiss	recal	ticket	adob	incid
request	connect	phone	win	proper
system	add	guest	deinstal	softwar

Table 2. Table shows topics identified in ticket database, as well as the top 10 word stems for each topic.

4.5 Topic Identification of Tickets

We now perform the Latent Dirichlet Allocation in order to extract topics from the tickets. As a result, Table 2 presents the top 10 likeliest words for each of the 5 topics. Based on these words, we assign names to the topics as follows: topic 1 addresses *Malware Detection* since words, such as *malwareadwar*, *infect* and *secur* strongly suggest a security-related focus. In addition, we bundle all subjects related to passwords and accounts into topic 2, named *Credentials*. Furthermore, topic 3 focuses on *Access Request*, while topic 4 (*Software Installation*) handles requests of new software and topic 5 is related to *Administrator Rights*.

In order to validate the robustness of our approach, we proceed as follows: we check whether the assigned topics are a good fit to the tickets by calculating the maximum topic probabilities for each ticket. Most

tickets are assigned to a topic with a clear probability of more than 50 %. Hence, this contributes to our confidence in the ticket assignment.

Figure 6 compares the distribution of ticket lifetime across different topics. We immediately realize that the tickets of most categories (except topic 5) are resolved in the first hour, whereas topic 5 peaks between 1 h and 2 h. Furthermore, we see a quick drop after the first hour for topics 1, 3 and 4, where the first lifetime hour has, respectively, 1.773, 2.70 and 2.51 times more successful resolutions than the second hourly slot. In the case of topic 2, this difference accounts for only a marginal 0.16 percentage points and topic 5 even shows a rise of 0.28 percentage points. In summary, we find clear evidence that tickets related to *Malware Detection*, *Access Request* and *Software Installation* can be handled fairly quickly and might thus suggest viable options for automation.

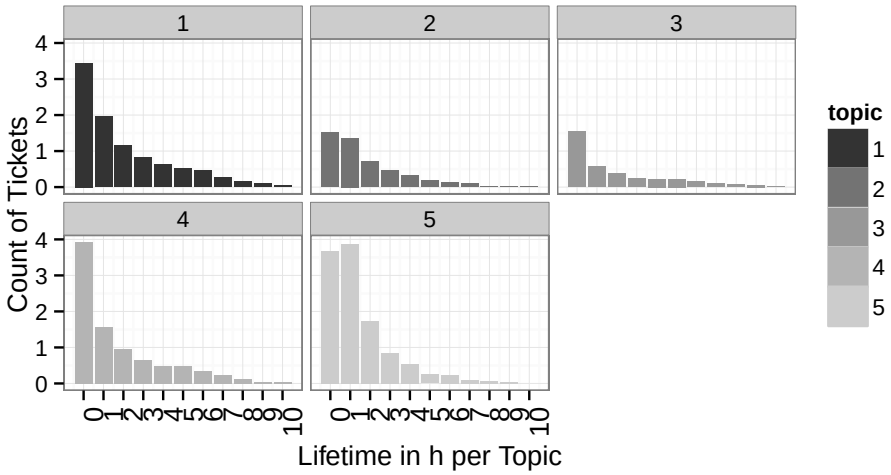

Figure 6. Ticket lifetime until resolution in hours presented for each topic (cropped to a max. of 10 h).

4.6 Results

In the final step, we use predictive analytics to automatically allocate tickets to their service group. For this, we use a random forest classifier, since it usually reveals a reliable out-of-the-box performance. We split the dataset into a training and test set at a ratio of 80 % to 20 %.[1] The random forest is trained with 500 trees with 14 randomly sampled variables evaluated at each split.

We apply the trained model to the test set and measure its predictive performance, as presented in Table 3. The random forest classifier achieves an overall accuracy of 92.72 %. Even when weighting the 5 classes by the frequency of their occurrences, this value is significantly higher than the performance of random guessing, which accounts for 20.00 %.

	Topic 1	**Topic 2**	**Topic 3**	**Topic 4**	**Topic 5**
Precision	85.53	94.15	90.32	96.22	95.16
Recall	95.29	88.14	91.31	96.99	96.07

Table 3. Predictive performance (in %) of random forest classifier on test set.

[1] We avoid the use of *k*-fold cross-validation as this would neglect the timing of tickets. For instance, we would evaluate our models with tickets on Windows 7 before changes in the IT landscape, while the same models were previously trained with later knowledge on the use of Windows 8. This approach thus better reflects the set-up in practice.

In summary, our incident management system proves to be highly accurate and very precise with a precision value of more than 85.00 % for all classes. This demonstrates how Business Intelligence can facilitate and improve the knowledge management processes of firms. In the future, our partner firm is going to improve the classifier further. The firm collects all erroneously classified tickets and integrates these into the training algorithm, thus constantly improving the knowledge database of the system.
We also seek to develop mechanisms for identifying ticket accumulations as an early warning system for fraudulent behavior or critical conditions of the IT architecture. As such, Figure 7 compares the frequency distributions for incoming tickets belonging to *Malware Detection* across each weekday. Once the actual arrival exceeds a certain threshold, e. g. 75 %, an alarm is triggered to demand a manual inspection. With this approach, our partner company can recognize large-scale attacks threatening the IT infrastructure.

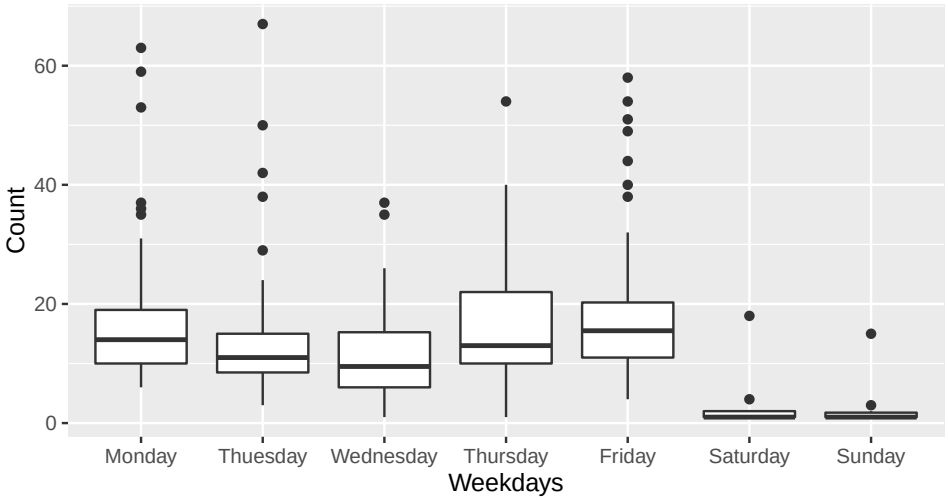

Figure 7. Boxplot compares distribution of incoming tickets for "Malware Detection" (topic 1) across weekdays.

5 Discussion and Managerial Implications

This paper details a method of making implicit knowledge explicit. For that reason, our case study draws upon 35,495 tickets from IT incidents, extracts underlying themes and then integrates this knowledge into an automated process for ticket assignments. We can also obtain further insights by analyzing combinations of issue (i. e. topic of the ticket) and average lifetime. In fact, around 25.00 % of all tickets are solved within less than 1.5 hours. This totals to 11.09 % of all tickets in topics 1, 4 and 5, which can all be fixed by introducing automation and self-service mechanisms.
As a result of our findings, our industry partner initiated discussions regarding the high number of requests related to manual software installations and situations requiring administrator privileges. However, these can predominantly be attributed to the tight security rules of the company. For instance, normal employees do not have administrator rights on their computers and therefore are not able to install software themselves. Consequently, any installation request has to follow a predefined process which is started by opening a ticket via a web interface. In a similar fashion, we can explain the high number of account resets due to forgotten log-in credentials. Here, each password must satisfy several requirements and needs to be changed every three months, which might challenge some users.
As a further implication for IT management, cases related to malware detection are highly critical and must be inspected individually. Therefore, it was decided to avoid implementing an automated mechanism for such incidents beyond initiating an immediate virus scan.

Introducing additional mechanisms, which target the root cause of each topic, could further decrease the number of tickets drastically. For example, a single sign-on mechanism could be a viable solution in case of forgotten passwords. Similarly, the company could consider the use of a self-service approach in order to deal with software requests. For instance, platforms such as Matrix42[2] allow IT departments to implement an in-house app store. This empowers employees to handle software installation requests on their own, which not only shortens the overall process but, based on the mentioned user concerns, results in a more satisfying IT service experience.

6 Conclusion

Nowadays, a company's helpdesk department has to deal with two major challenges: first, current IT management tools do not offer any means of discovering incident accumulations of the same type of issue. Instead, diligent communication is needed in order to identify hidden problems and to avoid the same work being done by different people. Second, the only way to deal with the huge number of daily tickets is to manually inspect and assign each individual ticket, on its own, to dedicated support groups. This step is highly time consuming and error-prone since the assignment process totally depends on the experience and knowledge of support team members.

We use a combination of Latent Dirichlet Allocation to identify topics within tickets and combine this with predictive analytics. This suggests a way to automate the process of ticket assignments and thus makes implicit knowledge explicit. We show that around 25 % of all tickets feature a lifetime of less than 1.5 hours and predominantly focus on *Malware Detection*, *Manual Software Installation* and *Administrator Rights*. This presents several compelling managerial implications as we can give advice on how to reduce the total number of tickets with automation, accelerate the finding of resolutions and enhance knowledge sharing among helpdesk employees.

In future work, we intend to extend our case study in the following directions. First of all, we need to improve our predictive framework such that it can deal with multiple languages. Second, our results can benefit from additional A/B testing when evaluating the performance of our application in a productive environment over a longer period. Third, firms could benefit from a mechanism for predicting IT incidents. Therefore, we want to link different datasets on e. g. server log-files or service monitoring with the occurrence of incidents.

References

Arora, A. and W. Bandara (2006). "IT Service Desk Process Improvement: A Narrative Style Case Study." In: *10th Pacific Asian Conference on Information Systems (PACIS 2006)*.

Berson, A., S. J. Smith, and K. Thearling (1999). *Building Data Mining Applications for CRM*. New York, NY: McGraw-Hill.

Blei, D. M. (2012). "Probabilistic Topic Models." *Communications of the ACM* 55 (4), 77–84.

Blei, D. M., A. Y. Ng, and M. I. Jordan (2003). "Latent Dirichlet Allocation." *Journal of Machine Learning Research* 3, 993–1022.

Breiman, L. (2001). "Random Forests." *Machine Learning* 45 (1), 5–32.

Cater-Steel, A. (2009). "IT Service Departments Struggle to Adopt a Service-Oriented Philosophy." *International Journal of Information Systems in the Service Sector* 1 (2), 69–77.

Cater-Steel, A. and N. McBride (2007). "IT Service Management Improvement: Actor Network Perspective." In: *15th European Conference on Information Systems (ECIS 2007)*.

Cater-Steel, A., W.-G. Tan, and M. Toleman (2006). "Challenge of Adopting Multiple Process Improvement Frameworks." In: *14th European Conference on Information Systems (ECIS 2006)*, pp. 1375–1386.

[2] URL: `https://www.matrix42.com/de/`. Last accessed on March 28, 2016.

Chapman, P. et al. (2000). *CRISP-DM 1.0: Step-by-Step Data Mining Guide*. URL: https://the-modeling-agency.com/crisp-dm.pdf (visited on 03/22/2016).

Di Lucca, G. A., M. Di Penta, and S. Gradara (2002). "An Approach to Classify Software Maintenance Requests: Maintaining Distributed Heterogeneous Systems." In: *18th International Conference on Software Maintenance (ICSM 2002)*. IEEE Computer Society.

Diao, Y., H. Jamjoom, and D. Loewenstern (2009). "Rule-Based Problem Classification in IT Service Management." In: *IEEE International Conference on Cloud Computing*, pp. 221–228.

Disterer, G. (2012). "Why Firms Seek ISO 20000 Certification: A Study of ISO 20000 Adoption." In: *20th European Conference on Information Systems (ECIS 2012)*.

Duffy, K. P. and B. B. Denison (2008). "Using ITIL to Improve IT Services." In: *14th Americas Conference on Information Systems (AMCIS 2008)*.

Gacenga, F., A. Cater-Steel, W.-G. Tan, and M. Toleman (2011). "IT Service Management: Towards a Contingency Theory of Performance Measurement." In: *32nd International Conference on Information Systems (ICIS 2011)*.

Galup, S. D. and R. Dattero (2010). "A Five-Step Method to Tune Your ITSM Processes." *Information Systems Management* 27 (2), 156–167.

Hastie, T., R. Tibshirani, and J. Friedman (2009). *The Elements of Statistical Learning: Data Mining, Inference and Prediction*. New York, NY: Springer.

Hochstein, A., G. Tamm, and W. Brenner (2005). "Service Oriented IT Management: Benefit, Cost and Success Factors." In: *13th European Conference on Information Systems (ECIS 2005)*.

Hornik, K. and B. Grün (2011). "Topicmodels: An R Package for Fitting Topic Models." *Journal of Statistical Software* 40 (13), 1–30.

Iden, J. and T. R. Eikebrokk (2013). "Implementing IT Service Management: A Systematic Literature Review." *International Journal of Information Management* 33 (3), 512–523.

Iden, J. and L. Langeland (2010). "Setting the Stage for a Successful ITIL Adoption: A Delphi Study of IT Experts in the Norwegian Armed Forces." *Information Systems Management* 27 (2), 103–112.

Jin, K. and P. Ray (2008). "Business-Oriented Development Methodology for IT Service Management." In: *41st Hawaii International Conference on System Sciences (HICSS 2008)*.

Kadar, C., D. Wiesmann, J. Iria, D. Husemann, and M. Lucic (2011). "Automatic Classification of Change Requests for Improved IT Service Quality." In: *Annual SRII Global Conference 2011*, pp. 430–439.

Kanapathy, K. and K. I. Khan (2012). "Assessing the Relationship Between ITIL Implementation Progress and Firm Size: Evidence from Malaysia." *International Journal of Business and Management* 7 (2), 194–199.

Kashanchi, R. and J. Toland (2006). "Can ITIL Contribute to IT/Business Alignment? An Initial Investigation." *Wirtschaftsinformatik* 48 (5), 340–348.

Kruse, P., A. Schieber, A. Hilbert, and E. Schoop (2013). "Idea Mining: Text Mining Supported Knowledge Management for Innovation Purposes." In: *19th Americas Conference on Information Systems (AMCIS 2013)*.

Kumbakara, N. (2008). "Managed IT Services: The Role of IT Standards." *Information Management & Computer Security* 16 (4), 336–359.

Lapão, L. V. (2011). "Organizational Challenges and Barriers to Implementing 'IT Governance' in a Hospital." *Electronic Journal of Information Systems Evaluation* 14 (1), 37–45.

Liu, D. and C. Lai (2011). "Mining Group-based Knowledge Flows for Sharing Task Knowledge." *Decision Support Systems* 50 (2), 370–386.

Maksai, A., J. Bogojeska, and D. Wiesmann (2014). "Hierarchical Incident Ticket Classification with Minimal Supervision." In: *IEEE International Conference on Data Mining (ICDM)*. IEEE Computer Society, pp. 923–928.

Manning, C. D. and H. Schütze (1999). *Foundations of Statistical Natural Language Processing*. Cambridge, MA: MIT Press.

Marrone, M. and L. Kolbe (2011a). "Impact of IT Service Management Frameworks on the IT Organization An Empirical Study on Benefits, Challenges, and Processes." *Business & Information Systems Engineering* 3 (1), 5–18.

Marrone, M. and L. M. Kolbe (2011b). "Uncovering ITIL Claims: IT Executives' Perception on Benefits and Business-IT Alignment." *Information Systems and e-Business Management* 9 (3), 363–380.

McBride, N. (2009). "Exploring Service Issues Within the IT Organisation: Four Mini-Case Studies." *International Journal of Information Management* 29 (3), 237–243.

McNaughton, B., P. Ray, and L. Lewis (2010). "Designing an Evaluation Framework for IT Service Management." *Information & Management* 47 (4), 219–225.

Mesquida, A. L., A. Mas, E. Amengual, and J. A. Calvo-Manzano (2012). "IT Service Management Process Improvement Based on ISO/IEC 15504: A Systematic Review." *Information and Software Technology* 54 (3), 239–247.

Mohammed, T. A. (2008). "The Art of Existence and the Regimes of IS-Enabled Customer Service Rationalization: A Study of IT Service Management in the UK Higher Education." In: *29th International Conference on Information Systems (ICIS 2008)*.

Nabiollahi, A., R. A. Alias, and S. Sahibuddin (2011). "Involvement of Service Knowledge Management System in Integration of ITIL V3 and Enterprise Architecture." *American Journal of Economics and Business Administration* 3 (1), 165–170.

Neničková, H. (2011). "Critical Success Factors for ITIL Best Practices Usage." *Economics & Management* 16, 839–844.

Pollard, C. and A. Cater-Steel (2009). "Justifications, Strategies, and Critical Success Factors in Successful ITIL Implementations in US and Australian Companies: An Exploratory Study." *Information Systems Management* 26 (2), 164–175.

Salton, G., E. A. Fox, and H. Wu (1983). "Extended Boolean Information Retrieval." *Communications of the ACM* 26 (11), 1022–1036.

Tan, W.-G., A. Cater-Steel, and M. Toleman (2009). "Implementing IT Service Management: A Case Study Focussing on Critical Success Factors." *Journal of Computer Information Systems* 50 (2), 1–12.

Thorleuchter, D., D. van den Poel, and A. Prinzie (2010). "Mining Ideas from Textual Information." *Expert Systems with Applications* 37 (10), 7182–7188.

Turban, E. (2011). *Business Intelligence: A Managerial Approach*. 2nd Edition. Boston, MA: Prentice Hall.

Ur-Rahman, N. and J. A. Harding (2012). "Textual Data Mining for Industrial Knowledge Management and Text Classification: A Business Oriented Approach." *Expert Systems with Applications* 39 (5), 4729–4739.

Wagner, H.-T. (2006). "Managing the Impact of IT on Firm Success: The Link Between the Resource-Based View and the IT Infrastructure Library." In: *39th Hawaii International Conference on System Sciences (HICSS 2006)*.

Wan, J. and D. Wan (2011). "Analysis on the Mindbugs in Information Technology Service Management Project Implementation." *Technology and Investment* 2 (3), 184–192.

Wan, S. H. C. (2008). "Improving Service Management in Campus IT Operations." *Campus-Wide Information Systems* 25 (1), 30–49.

Yi, X. and J. Allan (2009). "A Comparative Study of Utilizing Topic Models for Information Retrieval." In: *Advances in Information Retrieval*. Ed. by D. Hutchison et al. Vol. 5478. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, pp. 29–41.