CONFIDENTIAL INFORMATION-SHARING FOR AUTOMATED SUSTAINABILITY BENCHMARKS

Completed Research Paper

Florian Kerschbaum
SAP Research
Vincenz-Prießnitz-Str. 1,
76131 Karlsruhe, Germany
florian.kerschbaum@sap.com

Jens Strüker
University of Freiburg
Friedrichstr. 50,
79098 Freiburg, Germany
strueker@iig.uni-freiburg.de

Thomas Koslowski
University of Freiburg
Friedrichstr. 50
79098 Freiburg, Germany
koslowski@iig.uni-freiburg.de

Abstract

The pressure on enterprises to manage and improve their environmental sustainability is steadily increasing. Despite the growing awareness in the IS community and business practice, current IS solutions remain in an initial state. Sustainability benchmarking is seen as a novel and effective tool in this context. However, sustainability benchmarking faces two major obstacles: First, the heterogeneity of the data requires significant pre-processing, and, second, the sensitivity of the data causes enterprises to reluctantly share this data. Our contribution is twofold: After analyzing the data input problem and identifying appropriate and available solutions, we present a secure sustainability benchmarking service (SBS) to overcome the information-sharing problem. Our service uses homomorphic encryption to protect the data during processing and differential privacy to protect against leakages from the reports. Finally, we evaluate in detail a prototypical implementation of this secure sustainability benchmarking service and illustrate its applicability in industry.

Keywords: sustainability benchmarking service, information-sharing, enterprise resource planning, sustainability performance, secure software-as-a-service

Introduction

Business is recognized as being a critical contributor in realizing the challenges of environmental sustainability (Elliot 2011). Consequently, requirements from stakeholders on sustainability measurement have steadily grown (Chatterjee and Toffel 2010). Moreover, research increasingly demonstrates benefits of proactive sustainability management (Burnett and Hansen 2008). We show that while sustainability benchmarking, in particular, is a promising approach of proactive sustainability management, it faces a significant data input and information-sharing problem. Research recently proposed ways to get rid of the data quality and quantity problem with the help of innovative data capturing approaches (Butler 2011; Koslowski and Strüker 2011). The information-sharing problem is reflected in the fact that enterprises refrain from releasing the necessary data for benchmarks, as they fear that the information may be used for purposes other than those specified (Hervani et al. 2005). We propose a solution to overcome this information-sharing problem for sustainability benchmarking.

Note that the multidisciplinary field of environmental sustainability developed a variety of definitions and conceptualizations leading to confusion of terminology (Elliot 2011). For example, according to the triple-bottom-line accounting framework, sustainability incorporates the three dimensions of economic, social and environmental performance, while Elliott (2011) states that environmental sustainability is an essential prerequisite of social development. As we see our contribution rooted in the green IS research field (e.g., Dedrick 2010; Melville 2010), we utilize environmental sustainability proposed by Elliot (2011) that focuses on impacts on the environment without explicitly reconsidering an extra social dimension.

The remainder of the paper is structured as follows: The next section describes our research approach. Subsequently, we illustrate the trend to more sophisticated sustainability measurement and proactive sustainability management in detail. We then describe the data input problem for sustainability benchmarking and identify appropriate solutions to these data quality and quantity problems. By screening prior research, we then show that there is, however, a lack of research on the information-sharing problem. Finally, we present our solution for a secure sustainability benchmarking service (SBS) and discuss pros and cons.

Research Design

The problem we tackle in this research is the lack of data for sustainability benchmarking due to cost-intensive manual data collection and insufficient willingness of information-sharing across organizations. We address this problem by using the well-known design science research approach (e.g., Hevner et al. 2004) to develop an IT artifact that enables enterprises to measure and compare sustainability performance in a confidential manner. Melville (2010) states that "design research is essential to developing innovative IS-enabled solutions to environmental problems and evaluating their effectiveness" (pp. 8). The design science methodology seeks to create IT artifacts that are intended to solve specific organizational problems and provide rigorous evaluation of these artifacts based on utility rather than an empirical test of theories. This encompasses successive steps of problem identification, definition of objectives for a solution, design or development of a suitable IT artifact, and demonstration of the proof of concept, evaluation, and communication (Hevner et al. 2004).

Accordingly, we first identify the data input problem and its relevance by screening the literature. We then discuss proposed solutions to this problem and present a hybrid model based on homomorphic encryption and differential privacy in order to overcome the information-sharing problem. Afterwards, we derive functional and security objectives for the SBS and develop the corresponding method with an instantiation. Subsequently, we evaluate security using theoretical, cryptographic proofs, performance via measuring a prototypical implementation and functionality by comparing with non-secure benchmarking initiatives. We follow rigorous cryptographic proofs for security. Our method is secure if the underlying encryption system is secure and Paillier's encryption is provably secure if the decisional composite residuosity assumption holds (Paillier 1999). We use measurement of a prototypical implementation using the statistically sound methodology of Georges et al. (2007). We compare our functionality with non-secure benchmarking initiatives, e.g., (SAP 2011), discuss our solution and highlight implications for business practice and further research.

Trend to Comprehensive Sustainability Reporting and Proactive Sustainability Management

Stakeholders such as customers, investors or legislators are increasingly confronting enterprises with expectations for more sustainable business practices (Sharma and Henriques 2005). In the European Union, for instance, the so-called 'climate and energy package' (20-20-20 targets) became law in June 2009. The goal was to reduce the output of greenhouse gases by 20%, improving energy efficiency by 20% and increasing the percentage of renewable energy by 20% by the year 2020 (Melville 2010). This finally meant enterprises having to comply with many environmental laws (Hoffman and Busch 2008). These rules include to a greater extent the measurement and documentation of effects on the environment in the form of sustainability reports and eco-efficiency labeling of products, besides the avoidance and reduction of ecologically harmful substances (Cho and Patten 2007). The European Accountants Modernization Directive wants enterprises to reveal environmental information in the annual report as part of their annual accounts. More than 80 percent of the Global Fortune 250 published sustainability reports (KPMG 2009). Moreover, public, media and non-governmental organizations, such as the Carbon Disclosure Project, ask enterprises to produce proof of sustainable management, such as certificates or sustainability reports (Dedrick 2010). Finally, the growing demand for green products calls for environmental sustainability information (Sharma and Henriques 2005). Besides publishing sustainability reports, enterprises have met this demand by implementing corporate environmental management systems for quite a while. These measures are especially supposed to fulfill the compliance requirements of the stakeholders and, in this manner, help to avoid liability claims, reputation damage and consumer boycotts (Chatterji and Toffel 2010; Sharma and Henriques 2005).

Sustainability reporting has also changed over the years by expanding from an internal to an external, i.e., cross-enterprise perspective. By establishing methods like Life Cycle Assessment (LCA) (Reap et al. 2008) or Carbon Footprint (Weidema 2008), a more systematic and comprehensive covering of environmental impacts is increasingly gaining traction. The procedures of LCA are part of the ISO 14000 environmental management standards (e.g., Reap et al. 2008). The basic idea is that environmental impacts are always assigned to the segment that caused them. This so-called "cradle-to-grave" principle means to assess environmental impacts associated with all the stages of a product's life cycle (i.e., from raw material extraction through manufacturing to recycling and disposal). This becomes relevant as more stringent environmental laws and reporting standards require tracing and accounting of indirect emissions and also taking pre-chain and post-chain services into consideration. Thus, the scope of environmental sustainability is far beyond a single organization and requires a systematic understanding of an organization's interconnected value net (Watson 2010).

Accordingly, Shaw et al. (2010) highlight the importance of managing and reporting on sustainability indicators to gain significant cost savings and enhanced productivity. Widely used productivity indicators, such as carbon productivity or eco-efficiency, represent the relationship of output from a productive activity to its inputs (e.g., Dedrick 2010; Hoffman and Busch 2008; Wiedmann et al. 2009). However, as the productivity methodology is a comparative analysis, determining and interpreting the efficiency of enterprise units or processes requires the use of a reference object to identify a performance gap (Figge and Hahn 2005). Hence, benchmarking is seen as a promising tool for sustainability performance measurement and management (Sarkis 2010). Benchmarking, in general, means the "search for industry best practices that leads to superior performance" (Camp 1989) and as a continuous and systematic process that compares specific research objects with reference partners using diverse measurements (Spendolini 1992). In line with the prevailing view in theory and practice, we define sustainability benchmarking as a management tool to identify sustainability performance gaps between business objects for facilitating continuous improvement and organizational learning (e.g., Shaw et al 2010; Wiedmann et al. 2009). We distinguish between three types of sustainability benchmarking:

(1) *Benchmarking as aggregation* of data along the supply chain: To assess the sustainability performance of products or processes adequately, a comprehensive approach, such as LCA or Carbon Footprint, is desirable. This means, the value of LCA increases with the integrity of data collected from actors involved in the production process. If sufficient supply chain partners participate in the SBS, we then can compute and compare aggregated indicators for the entire supply chain or the final product item (Hoffmann and Busch 2008).

(2) Second, we consider *generic benchmarking* where a market actor compares its performance to its direct competitors (Spendolini 1992). Using generic benchmarking, an actor can compare its performance, determine improvement potential and initiate measures to close the gap to the competition.
(3) As supplier selection also plays an important role in the greening of a supply chain, we thirdly implement *competitive benchmarking for supplier evaluation and selection,* which provides a comparative overview over several market actors (Sarkis and Talluri 2002).

A multitude of benefits is associated with sustainability benchmarking (e.g., Björklund 2010; Miakisz 1999; Sarkis 2010; Shaw et al. 2010):

- By tracing environmental impacts across the entire supply chain, sustainability benchmarking improves the accountability and transparency of an enterprise by fulfilling a cradle-to-grave perspective, allows measuring and communicating the improvements made and enables stakeholders to judge the level of responsibility of an enterprise.
- It identifies problem areas that might be overseen and therefore provides opportunities to improve environmental and economic performance simultaneously.
- Comparisons within and between entire supply chains allow enterprises to choose suppliers according to sustainability criteria.

In the following, we show why sustainability benchmarking – in spite of the aforementioned benefits – is still in an early stage of development.

From the Data Input to the Information-Sharing Problem for Sustainability Benchmarking

The quantity and availability of environmental data makes the benchmarking process very difficult to execute today (Shaw et al. 2010). While typical challenges of benchmarking exercises, such as scope selection, time, common accepted indicators and cost (Shaw et al. 2010), are also relevant for sustainability benchmarking, cost, in particular, hinders sustainability benchmarking from a wide use (Matthews and Lave 2003). As we show in the following sections, data capturing and data adaptation are so costly because both are still mainly manual operations.

ERP Systems as a Solution to the Manual Data Gathering Problem

Regardless of which of the sustainability benchmarking types is to be conducted, the relevant data first has to be gathered from the actor(s) and reference object(s) before the benchmark is processed. ERP systems are considered as key in order to automate the data capturing process (Funk et al. 2009). They provide the necessary data such as consumption of energy, water and materials (Makrinou et al. 2008) as indicated in Table 1 and, in this manner, they can be used as a basis for sustainability performance evaluations, such as ISO 14000 series or environmental reporting as Global Reporting Initiative (Shaw et al. 2010). Important sources of data based on ERP modules are bills of material and work plans for the production processes. The integration of this data enables assigning environmental impacts to the corresponding business objects.

Automating the process of extracting and processing the necessary environmental data requires specific sustainability management applications that are integrated into ERP systems. Such applications are not only able to integrate management information including manufacturing, accounting or sales across an entire organization. They can also account for anthropogenic material and energy flows occurring in production processes. This requires the consideration of environmental impacts, for example in material management, transport planning or business process management.

Table 1. Data Collected and Indicators for Sustainability Benchmarking

Categories	Data Collected				Sustainability Indicators
Energy	Forms of energy	Annual consumption	Energy costs	Emissions	• Carbon productivity • Product Carbon Footprint • Percentage of recycled products • Eco-Efficiency • Transport intensity • …
Water	Annual consumption	Costs of water	Effluent		
Materials	Material used	Annual consumption	Material costs		
Waste	Hazardous waste	Recycled waste	Disposal costs	Recycling revenues	
Production	Production costs		Annual sales		

Although the systematic and deep integration of sustainability management information systems and ERP systems is comprehensively discussed in IS (e.g., Funk et al. 2009), these conceptualizations and reference architectures have mainly prototypical status at best, and are not yet widely diffused in companies. Nevertheless, first experiences with business software solutions are promising. For instance, Butler (2011) reports time savings of more than 90% when an ad hoc evaluation of a product is calculated with SAP's "Compliance for Product" compared to the still dominating manual spreadsheet solution. These significant savings in terms of working hours can be achieved when sustainability applications comprise widely accepted environmental compliance repositories and frameworks for reporting and management purposes (s. Figure 1). Existing conceptional IS architectures often suggest the extension of the ERP data model by description rules (process libraries) to derive ecological transformations (Funk et al. 2009). Against the background of current research and development activities and the increasing number of software solutions on the market (Butler 2011), it seems to be only a question of time before data input cost will no longer be prohibitively high.

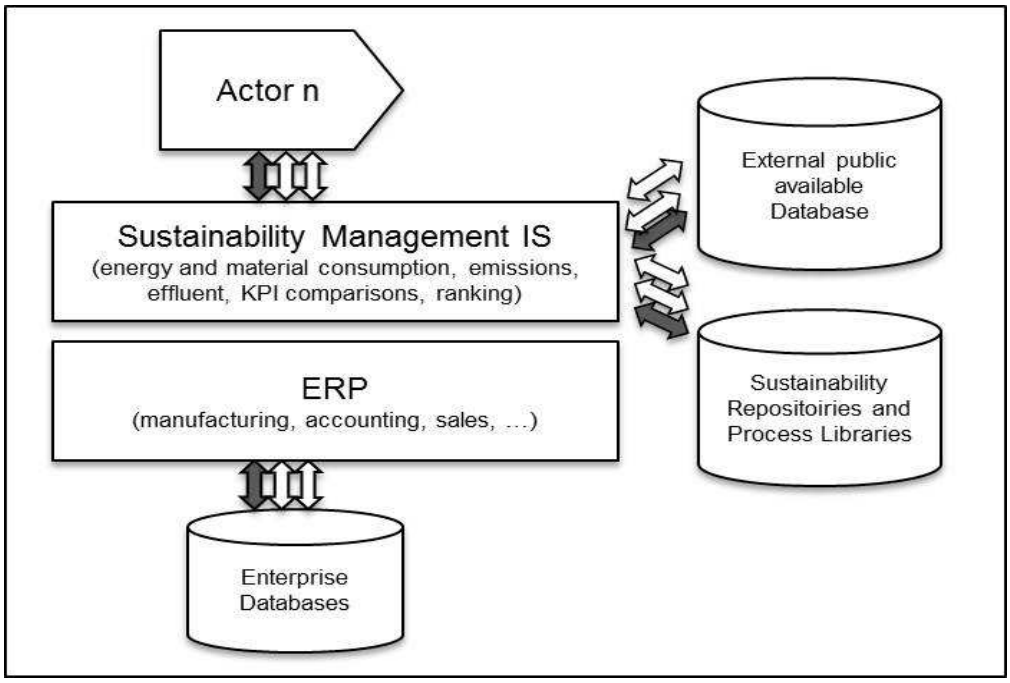

Figure 1 Automating the Data Gathering Process

Integrated ERP Platforms and Specialized Providers as Solution to the Data Heterogeneity and Quality Problem

Given a wide use of sustainability management applications that are integrated with ERP systems, the data input problem is still not completely solved. As sustainability benchmarking is an inter-organizational process, data gathering from various enterprises is faced with specific challenges (Hoffman and Busch 2008). ERP systems integrated with sustainability management systems, in principle, provide the necessary data. However, getting and making the data comparable and processable across different ERP and different sustainability management systems requires interoperability, i.e., commonly accepted standards on different layers. Otherwise, interoperability between applications across enterprises needs time-consuming agreements on the business process level which makes data gathering and adaptation very costly.

As mentioned above, current methodologies such as LCA or Carbon Footprint demand a cradle-to-grave perspective. Therefore, the environmental impacts of the upstream value chain must be determined, too. Today, the missing sustainability data in the ERP systems (e.g., environmental impacts of the in-use and end-of life phases) has to be entered *manually* or either replenished through external publicly available data sources like governmental statistical inventories, e.g., US Environmental Protection Agency or the ELCD core data base of the European Commission (European Commission 2011). These data sets usually rely on "typical" descriptions of material and energy flows that are often not up-to-date and rather estimated than measured (Chatterjee and Toffel 2010).

So-called ERP on-demand systems provide a promising solution to the data heterogeneity problem. If sustainability management applications are integrated with such an internet-based ERP software service, the data basis for sustainability benchmarks could be unified and all ERP on-demand customer data would be comparable. Assuming that ERP customers give access to their data, the use of the same ERP software service would widely solve the data heterogeneity problem. Such ERP on-demand applications have yet a low market share (Benlian et al. 2009). However, the ERP market leaders SAP and Oracle meanwhile provide their own ERP on-demand solutions and the platform integration model, in particular, is seen as an auspicious business model. Koslowski and Strüker (2011) show how the integration of a sustainability benchmarking service into an on-demand ERP platform provides added value beyond pure cost savings. They identify self-reinforcing mechanisms that allow a faster and more comprehensive market penetration than providing these services separately. Sustainability management applications as an independent software service are also an alternative to the platform approach. On-demand providers could specialize in offering standardized interfaces to a plethora of different ERP systems and sustainability management information systems. Even though they are likely to gain a considerable market share, enabling sustainability benchmarks by using the least common denominator between different applications comes with the price of quality-losses: As the functionalities and semantic of different ERP systems differs, cost-intensive adaptations and compromises seem to be inevitable. However, we firmly believe that ERP on-demand platforms will establish on the market and, in this way, the data heterogeneity problem for sustainability benchmarking will be increasingly manageable for enterprises.

Matthews and Lave (2003) point out that sustainability benchmarking also exhibits a considerable data quality problem. As soon as the data capturing for several enterprises is automated though, the data reliability of sustainability benchmarking is very likely to increase. This is because any data manipulation is a serious intervention in automated processes. Consequently, the resultant costs of data manipulation significantly rise compared to a world where excel spreadsheets are exchanged.

Next, we illustrate that there is at least one more obstacle to overcome for sustainability benchmarking.

The Unsolved Information-Sharing Problem for Sustainability Benchmarking

When it comes to exchanging sensitive data across enterprises, mistrust and fear for opportunistic behavior hinder collaboration. Research on inter-organizational systems shows how reserved and cautious enterprises still are today when it comes to the exchange of sensitive data (Kumar and Dissel 1996; Saunders et al. 2004). In order to track inter-organizational data in a reasonable granularity and precision for holistic sustainability assessments, a collaborative exchange of sensitive data like

environmental impacts and sustainability indicators is necessary (Elliot 2011). Enterprises will view sustainability benchmarking very critically, because competitors could simply imitate best practices or communicate superior performance to customers (Brewer and Speh 2001; Hervani et al. 2005). Apart from competitors, enterprises also regularly do not trust their supply chain partners and third parties (Saunders et al. 2004) and could therefore also fear opportunistic behavior of their partners.

There are a number of techniques in computer science to share sensitive, private data in a confidential manner. The underlying assumption is that trust in organizations and people can be substituted through trust in a security mechanism (cp. Anderson and Needham 1995). First, there are anonymization and randomization techniques, such as k-anonymity (Samarati and Sweeney 1998) and l-diversity (Machanavajjhala et al. 2007), which remove or blur information so that it is no longer identifiable. Such techniques lower the accuracy and utility of the data in favor of privacy (Brickell and Shmatikov 2008) and clearly prevent applications such as competitive benchmarking for supplier evaluation and selection. When using input randomization, it is not clear whether the necessary accuracy even for an average computation can be achieved using reasonable client population sizes (Bohli et al. 2010). Furthermore, most attempts at anonymizing data have been later broken (e.g., Narayanan and Shmatikov 2008; Narayanan and Shmatikov 2009).

Second, cryptography developed secure multi-party computation (SMC) (Ben-Or et al. 1988; Goldreich et al. 1987; Yao 1986). SMC substitutes computation with a trusted third party by an interactive protocol which achieves the same security properties as the fully trusted third party. An interactive protocol requires the simultaneous on-line availability of all parties, including all client enterprises, for each computation which is likely infeasible in our ERP outsourcing scenario, since the probability of all parties being available is negligible in the number of parties. We therefore leverage homomorphic encryption, which allows non-interactive computations on the plaintext using the ciphertexts only. Recently, fully homomorphic encryption, which enables any computation on the plaintext, has been introduced by Gentry (Gentry 2009), but is currently still too inefficient for practical application (Gentry and Halevi 2010; Liu et al. 2010).

Third, trusted computing (Anderson 2011) can be used to verify a computer's software integrity. It has been designed to protect digital rights on personal computers and its application to secure remote services is not yet clear. Furthermore, it cannot verify a computer's hardware integrity which always remains under the control of the service provider.

In the next section, we will introduce a solution for a sustainability benchmarking service (SBS) addressing the lack of trust for information sharing. We extend only additively homomorphic encryption, e.g., (Paillier 1999), which is limited to plaintext addition in order to implement all necessary benchmarking functionality, including comparison.

A Confidential SBS

The secure sustainability benchmarking service (SBS) is a software-as-a-service that integrates the sustainability data from multiple on-demand or on-premise ERP applications and provides the business user with the three types of benchmarking: benchmarking as aggregation, generic benchmarking and competitive benchmarking for supplier evaluation and selection. We refer to an actor as an enterprise either represented by an ERP system providing the necessary input or a business user accessing the sustainability benchmarking reports.

Benchmarking Types

The SBS must provide certain *benchmarking types* on the input data to enable business users to compare and improve their performance. These functions must respect the confidentiality requirements of the actors, but also implement the benefit of collaboration for the actors. In the remainder of the section, we present the implementation of the benchmarking types in detail, since we need to later reconciliate them with our confidentiality objectives.

Benchmarking as aggregation

Consider the example of Carbon Footprint where the carbon emissions broken down to product items need to be aggregated along the supply chain. Assume we have collected the sustainability data of all actors of an entire supply chain. We can compute aggregated data for specific products. Let $x_{i,j}$ be a sustainability indicator, e.g., Carbon Footprint, for an item of product i at actor j. From the meta-data, i.e., the bill of material, we can recursively compute an aggregate indicator $y_{i,j}$. Let $k \in M(x_{i,j})$ be the materials, $a_{k,i}$ be the number of units and $S_j(k)$ be the supplier of k to actor j. Then

$$y_{i,j} = x_{i,j} + \sum_{k \in M(x_{i,j})} a_{k,i} y_{k,S_j(k)}$$

Aggregate indicators can be input to generic or competitive benchmarking. Nevertheless, they require information from the entire supply chain as only available in ERP systems.

Generic Benchmarking

In generic benchmarking, an actor j compares its indicator $x_{i,j}$ to its peers. Peers are loosely formed groups of competitors offering substitutable goods. Generic benchmarking can be used to judge one's absolute position for an indicator. It allows determining improvement potentials by analyzing the absolute gap to the competition (Spendolini 1992).

Due to data confidentiality requirements of the actors, the SBS cannot disclose any actor-specific indicators. Instead, the SBS computes statistics about the peer group and distributes these. Good candidates for a secure implementation are mean μ and variance σ^2. Let $i \in P$ be the set of products in a peer group and $S'(i)$ be the set of supplier for product i. Then

$$\mu = \frac{1}{\left|\bigcup_{i \in P} S'(i)\right|} \sum_{i \in P} \sum_{j \in S'(i)} x_{i,j} \qquad \sigma^2 = \frac{1}{\left|\bigcup_{i \in P} S'(i)\right| - 1} \sum_{i \in P} \sum_{j \in S'(i)} \left(x_{i,j} - \mu\right)^2$$

All statistics are published anonymously, i.e., except the peer group, no individual identifiers are attached to the data.

Competitive Benchmarking for Supplier Evaluation and Selection

Competitive benchmarking can be used for supplier selection (Sarkis and Talluri 2002). The evaluation of suppliers will usually not only base on sustainability criteria but also on traditional indicators, such as service levels, prices and responsiveness. Therefore, the supplier selection represents a multi-attributive decision-making problem which requires a ranking of actors using weighted indicators. A wide range of powerful decision-making approaches has been proposed, e.g., Analytic Hierarchy Process or Data Envelopment Analysis (Ho et al. 2010) which are also applied in sustainability performance measurement and life cycle assessment (Pineda-Henson et al. 2002; Zhou et al. 2008). Such a required weighted indicator $z_{i,j}$ is similar to an aggregated indicator. The weights are public, such that all actors are aware of the scoring mechanism. We chose fixed weights, because user-set weights may allow inferences about the indicators. While user-set weights per se are not a problem – as long as they are fixed –, the user's choices must be rate-limited, i.e., he must be restricted to perform at most a fixed number of weight updates per period. Balancing the rate of updates and the implied inferences about private indicators is very delicate and in order to avoid this issue we chose fixed, public weights.

Let w_y be the weight for indicator y and Y be set of indicators. Then

$$z_j = \sum_{y \in Y} w_y y_{i,j}$$

The result of the competitive benchmarking is a ranking of actors from best to worst, i.e., it is not anonymous. Instead, no numerical data except the rank is released.

Security Objectives

A necessary objective of the SBS is to provide security of the sustainability indicators (despite providing the types of benchmarking reports). As seen in Section 3, it is required for the uptake of benchmarking by the market. Our main security objective is confidentiality of the indicators, i.e., no party other than the source of the indicator should be able to learn its value. We distinguish two distinct confidentiality objectives.

Confidentiality During Processing

The SBS itself when computing the benchmarking reports should not learn the indicator values. Instead, it should remain oblivious to the values. The SBS should not be entrusted with the indicator values. First, the actors may not trust the SBS provider to use the indicators for different purposes than intended. Second, the SBS may not want to carry the burden of securing such sensitive data. The collected storage may make the SBS an attractive target for hackers. Third, if the SBS can be implemented adhering to these security objectives, there is no reason not to do so. Nevertheless, trust the SBS not to collaborate with individual actors on espionage of competitors.

Confidentiality Given Results

While confidentiality against the SBS is necessary, it is not sufficient. Even given the results of the benchmarking reports, the actors should not be able to discern additional information about another actor's indicator values. While this is not critical for competitive benchmarking, which only releases the ranking of the actors, this can be difficult in generic benchmarking where the actors learn statistics about the indicator values. These statistics should disclose only limited information about a specific actor's indicator. We summarize the features and benefits of the SBS in Table 2.

Table 2. Features and Benefits of SBS

SBS Features	Benefits
Confidentiality During Processing	• No trust in service provider necessary • Simplified data management at service provider
Confidentiality Given Results	• Collaborative Benchmarking functionality • Controlled leakage to competitors

Implementation

We implement the security objectives of the SBS using two mechanisms: homomorphic encryption and differential privacy. Our choice can be explained as follows. There are essentially two methods for providing confidentiality during processing: homomorphic encryption and SMC. Homomorphic encryption has the advantage that the computation can be performed non-interactively as opposed to an interactive protocol. This allows us to maintain the usual service communication pattern of submitting input and then receiving the result. Among all methods to provide confidentiality given results differential privacy is the first that is independent of the previous knowledge of the adversary. This allows us to design the SBS without making any assumption about the knowledge of actors about each others' indicators. Each indicator is stored encrypted at the SBS. We process the data in encrypted form computing the three types of benchmarking reports. We then prepare the results using differential privacy, if needed.

Homomorphic Encryption

Homomorphic encryption is an encryption technique that allows certain operations on the ciphertexts mapping to homomorphic operations on the plaintexts. Specifically, we use Paillier's encryption scheme (Paillier, 1999). Paillier's encryption scheme allows the addition (modulo a key-dependent constant) of plaintexts using the ciphertexts only. Let $E(x)$ denote the encryption of plaintext x and $D(c)$ the decryption of ciphertext c. Then

$$D(E(x) \cdot E(y)) = x + y$$

With simple arithmetic the following formula can be derived

$$D(E(x)^y) = x \cdot y$$

Paillier's encryption scheme has several other interesting properties. First, it is a public-key scheme, i.e., one can encrypt without being able to decrypt. Second, it is proven secure against chosen plaintext attacks. Loosely speaking, an adversary cannot distinguish any two ciphertexts, even if he knows the plaintexts. Third, it can be implemented reasonably efficiently. Its performance is comparable to the popular RSA encryption scheme.

Key Management

Key Management is critical for any encryption scheme. We share the public key among all actors and the SBS, i.e., every party can encrypt and perform homomorphic operations on the ciphertexts. We then offer two choices for managing the private key. In the simple case, each actor has access to the same private key. Of course, this private key needs to be safeguarded, e.g., by safely embedding it in the software. In the complex case, the key is shared among several participants. We can use Damgard and Jurik's variant of Paillier's encryption scheme (Damgard and Jurik 2001) in order to facilitate the decryption process without reconstructing the key first. It is a threshold scheme, i.e., any *t* out of *n* actors can jointly decrypt a ciphertext.

Differential Privacy

Differential Privacy is a technique for protecting against leakages from results of statistical functions (Dwork, 2006). It guarantees that the difference in the probability of an output between two data sets differing in just one element is at most a factor of e^{ε}. Then, the probability of successfully deciding whether an actor's data is in the set or not becomes negligible in ε. One can achieve ε-differential privacy in any statistical function *f* by adding Laplacian noise proportional to maximum difference Δf any element can cause in the result. An ε-differential private function *f'* is then

$$f'(x) = f(x) + Lap(\Delta f / \varepsilon)$$

where $Lap(\Delta f/\varepsilon)$ is drawn from the symmetric exponential distribution with standard deviation $\Delta f/\varepsilon$.

Determining the impact on utility of differential privacy is multi-faceted. First, the usefulness of the results depends on the usage of the results which can only be assessed in a particular application context. Second, there are a number of parameters that influence the distribution of random noise. There is the parameter Δf which is computed as the fraction of the size of the domain of the indicators over the number of peers in the group. Then one can also choose the privacy parameter ε. This choice should be made according to the sensitivity of the indicators. Using this parameter, we can provide exemplary calculations: For an indicator domain size of *16* bits (indicator values ranging between 0 and 65535), a peer group size of *50* and a privacy parameter of ε*=0.33*, the random noise is in the range *[-6392, 6392]* (less than *19,5%* deviation from the expected mean) with *80%* probability and in the range *[-9144, 9144]* (less than 27,9% deviation from the expected mean) with *90%* probability.

System Architecture

Our SBS operates non-interactively on the encrypted input by the ERP systems of the actors. It then computes the benchmarking reports on this encrypted data and reports the results to the business users of the actors, i.e., our SBS has never access to the unencrypted sustainability data. Information sharing across the supply chain – either on the product or item level – is accomplished via ciphertexts encrypted under the same public key. The SBS can aggregate these ciphertexts without granting the actors access to these cipheretexts, but only the aggregated indicators. Any indicator value never leaves an actor-controlled ERP system (be it on-demand or on-premise) in plaintext. The actors can therefore be ensured that their data is not abused and the SBS provider may not need to implement certain additional safeguards, such as file system or hard disk encryption, for this data – presuming customer acceptance. We show a picture of this system architecture in Figure 2. Next, we describe how we can implement the benchmarking report computation on encrypted data.

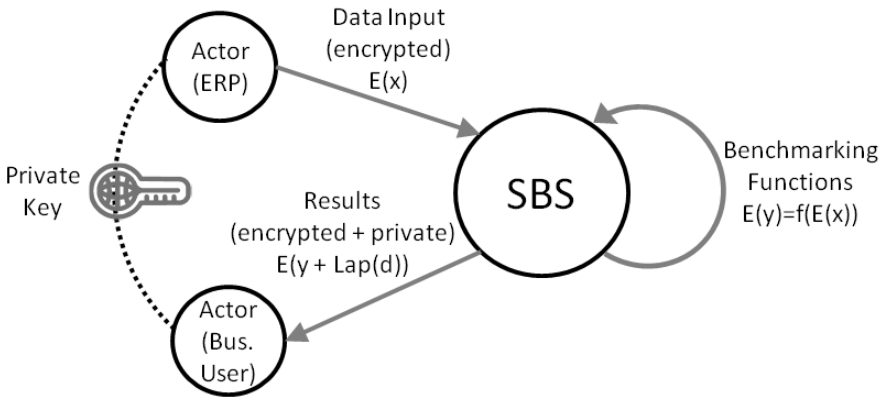

Figure 2 SBS system architecture

Aggregation

We can now describe our implementation of the three benchmarking types while meeting the confidentiality objectives using homomorphic encryption and differential privacy. For the ease of the exposition, we use a different denotation of the indices in this section. Let x_i be indicators stored at the SBS. Recall that each indicator is stored encrypted as $E(x_i)$. Let w_i be the weights for each indicator. We can then compute an aggregated indicator y as

$$E(y) = \prod E(x_i)^{w_i} = E\left(\sum w_i \cdot x_i\right)$$

The same computation can be used for weighted indicators in competitive benchmarking. Note that the result is encrypted and can only be used as such in further processing.

Statistics

We first consider the generic benchmarking. For computing the mean μ, we emphasize that the number n of actors in a peer group is known from competitive benchmarking where a ranking is computed. So, we can compute the sum $n\mu$ instead. Furthermore, we now need to take care of differential privacy, since we need to protect against inferences from the statistical quantity itself. We therefore choose a random noise. Let $d = max(x_i) - min(x_i)$ be the domain-size of the indicators. Then we compute

$$E(n\mu) = E\left(Lap(d/\varepsilon)\right)\prod E(x_i) = E\left(\sum x_i + Lap(d/\varepsilon)\right)$$

The result of this computation can be sent to the actors where it is decrypted, i.e., the SBS never learns the results of its computations. It only stores the data, performs the computation and provides the (encrypted) results to the actors. We can perform a similar computation for the variance. We first note that the variance can be computed from the power sums

$$\sigma^2 = \frac{n\sum x_i^2 - \left(\sum x_i\right)^2}{n^2}$$

We note that the actor has already received $E(n\mu)$ and knows n. We therefore need to only send the (ε-differential private and encrypted) second power sum S_2. We store the (encrypted) square x_i^2 for each indicator x_i at the SBS and compute

$$E(S_2) = E\left(Lap(d^2/\varepsilon)\right)\prod E(x_i^2) = E\left(\sum x_i^2 + Lap(d^2/\varepsilon)\right)$$

The (encrypted) second order moment is sent to the actor which can decrypt it and compute the variance. The (encrypted) square can be submitted to the SBS along with the encrypted indicators. The SBS maintains them in the same database of ciphertexts.

Comparison

For competitive benchmarking, we need to compare encrypted (weighted) indicators. This is challenging, since additively homomorphic encryption, such as Paillier's encryption, does not directly support this operation. Instead, we can use the technique of Kerschbaum et al. (2009), which operates on such data directly. It leaks information proportional to the bit length of the plaintext, but nothing else (Wibmer et al. 2010). It works as follows: Choose a large random number $r > o$ (at least three times the bit length of d). Then choose a second random number r', such that $o \leq r' < r$. Given two indicators x_i and x_j we compute a comparison operand c as

$$E(c) = \left(E(x_i) \cdot E(x_j)^{-1}\right)^r E(r') = E\left(r(x_i - x_j) + r'\right)$$

This comparison operand c can now be sent to an actor which decrypts it. It holds that

$$c < 0 \Leftrightarrow x_i < x_j$$

but reveals nothing else about x_i or x_j. Using this comparison operation we can implement a ranking of actors. Let x_i $(1 \leq i \leq n)$ be the set of (weighted) indicators of the peer group. Then we compute a comparison operand c_{ij} for each pair x_i and x_j $(1 \leq j \leq n)$. Note that if $c_{ij} \geq o$ and $c_{ji} \geq o$, then $x_i = x_j$. We sent all comparison operands to the actor for decryption, which can then compute the ranking.

Analysis

Security

All security objectives of the SBS are met and the computation of the three benchmarking types succeeds. Regarding confidentiality during processing, we note that all stored and processed indicators by the SBS are encrypted. They are submitted to the SBS as ciphertexts and later processed. Regarding confidentiality given results, we note that all revealed numerical values are ε-differential private. The actors only learn ε-differential private statistics in generic benchmarking and secure comparison operators in competitive benchmarking. In summary, both security objectives are met by the SBS.

Performance

Performance remains a critical aspect for encrypted computations. A single arithmetic operation in fully homomorphic encryption can take up to an hour (Gentry and Halevi 2010; Liu et al. 2010) rendering enterprise-size computations infeasible. We therefore use only partially homomorphic encryption, which has performance comparable to regular public-key cryptography. Nevertheless, measurements are necessary in order to size the computational resources. Furthermore, although many of our computations can be performed off-line, some are tied to user interaction, such as decryption. Additionally, benchmarking information is supposed to be available for a proactive sustainability management at the time when decisions are made (Matthews and Lave 2003). Beside the customers, an SBS provider also has a strong interest in keeping computing time as low as possible: the less computing time needed, the lower the capital costs of computing. The performance of operations is therefore critical for market acceptance of the SBS.

We benchmark a prototypical implementation of our SBS. We consider the use case for one single indicator which may be either for a single product or a single item and also may be either computed cross-company or intra-company. Our system scales linearly with the number of such indicators only. We focus on the most performance-critical operation of competitive benchmarking. We distinguish three phases: weighted indicator preparation, comparison operand computation and decryption. Weighted indicator preparation and comparison operand computation are performed off-line by the SBS provider while decryption is performed by each actor on-line. We can solely focus on the computational performance, since our entire SBS operates non-interactively. The encrypted indicators are submitted and – either on request or off-line – the benchmarking reports are computed, i.e., the computational performance is the decisive factor for our SBS.

We performed all computations single-threaded on a 2.4 GHz Intel Xeon processor with 64 GB of memory. We used Java SDK 1.6. We report the mean and 99% confidence interval of 20 experiments. We used a 1024-bit RSA key for the encryption. We depict the runtime in seconds of each of the three operations in Table 3. Weighted indicator preparation (Aggregation) grows linearly with the number of input indicators while comparison operand computation (Comparison) and decryption (Decryption) grow quadratically with the number of actors in the peer group.

We can compare our performance results to fully homomorphic encryption and to some extent to standard public-key encryption. For a peer group size of n and a bit length l of the indicators, we need roughly $5l(n-1)$ gates for aggregation (without any weights) and $5l(n \log^2 n)$ gates for comparison. We obtain circuit sizes for $n=10$ (our smallest peer group size) and $l=32$ bits of 1440 gates and 12800 gates, respectively. Using the implementation results of Gentry and Halevi (2010) for a realistic key size of 32768 and assuming 30 gates per re-encryption operation, we can estimate the performance of fully homomorphic encryption to be roughly 24 hours for aggregation and 220 hours for comparison, respectively. Compared to our results measured in seconds, this is a factor of more than 50.000. Standard public-key encryption cannot implement aggregation or comparison, so we can only compare decryption. Decrypting a single value in the homomorphic encryption scheme takes approximately 0.024 seconds. Decrypting a single value in standard RSA encryption with the same key length takes approximately 0.0045 seconds. This small factor of 5 is not surprising, since both encryption schemes use the same key generation algorithm, but homomorphic encryption operates in the double field size.

Table 3. Performance Results in Seconds

Peer Group Size	Aggregation		Comparison		Decryption	
	Mean	99% CI	Mean	99% CI	Mean	99% CI
10	0.47	±0.003	11.19	±0.043	2.16	±0.003
20	0.94	±0.003	47.10	±0.033	9.10	±0.005
30	1.42	±0.005	107.82	±0.112	20.83	±0.005
40	1.89	±0.005	193.14	±0.137	37.35	±0.006
50	2.36	±0.006	303.21	±0.180	58.65	±0.008

Discussion

The starting point of our exploration has been the observation that sustainability measurement and management is increasingly used to improve not only sustainability but also productivity. As the automation of the data capturing process is the necessary condition in order to overcome today's expensive manual data gathering, IS research comprehensively addressed this so-called data input problem of sustainability benchmarking. Concretely, the focus has so far been on the integration of sustainability management information systems and ERP systems within an enterprise. As we have shown, a wide use of sustainability applications integrated with ERP systems at enterprise level is likely to improve the quantity and availability of digital environmental data. However, the data input problem is still not completely solved: sustainability benchmarking as a more and more inter-organizational process requires data gathering from various enterprises. Thus, getting and making the data comparable and processable across different ERP and different sustainability management systems is very costly. In our contribution, we have argued that a sustainability benchmarking service integrated in an ERP on-demand platform can overcome this data heterogeneity problem. We have identified an additional information-sharing problem as part of the inter-organizational data input problem and have proposed a secure sustainability benchmarking service (SBS) as solution.

Our research contribution is twofold: We have identified an inter-organizational dimension of the data input problem as a yet underrepresented research area. In spite of its importance for sustainability benchmarking, there has been – according to our best knowledge – only little research into this question

so far. Sustainability benchmarking as a management tool aims to identify sustainability performance gaps between business objects for facilitating continuous improvement and organizational learning. All three sustainability benchmarking types that we have discussed – benchmarking as aggregation of data along the supply chain, generic and competitive benchmarking – are based on real and precise data for the first time – instead of rough estimates or obscure reference enterprises usually used. Consequently, the validity of aggregated indicators such as LCA or Carbon Footprint for the entire supply chain or the final product item is supposed to significantly increase.

Besides the data heterogeneity problem, we have also identified and analyzed an information-sharing problem. This is likely to prevent a wide use of sustainability benchmarking – even if the data heterogeneity problem is solved. Based on a discussion about several techniques in computer science to exchange sensitive data in a confidential manner, we have tackled this crucial hurdle for inter-organizational sustainability benchmarking services by developing a secure sustainability benchmarking service (SBS). It uses homomorphic encryption to protect the data during processing and differential privacy to protect against leakages from the reports. We have implemented the SBS and our measurements show that the performance is manageable for the business user as well as the service provider.

Our security solution in the scope of an integrated ERP platform primarily aims to solve the information-sharing problem of sensitive data known, for instance, from business relationships in supply chains. Using the SBS, enterprises can give a benchmarking service provider access to the relevant data without the risk of revealing this sensitive data to other enterprises. Enterprises then have to trust their provider's security mechanisms instead of building trustworthy relationships to the provider over time. However, we see the security mechanism not only as a key element for a widespread use of automated sustainability benchmarking services. Additionally, it could help ERP platform providers to faster reach the critical mass of customers for utilizing self-reinforcing effects, so-called positive feedback loops, of an ERP on-demand platform (Koslowski and Strüker 2011).

Sustainability benchmarking services that are integrated into ERP on-demand platforms are supposed to significantly decrease the cost of gathering environmental data. So far, however, as there are several competing platforms and supply chain partners use different ones, there will remain considerable coordination costs: Ensuring interoperability between different data formats and semantics of different ERP applications might even outweigh the cost benefits of the ERP on-demand platforms. Our contribution is also limited by our assumptions regarding trust: While research clearly shows that enterprises in supply chains regularly refrain from exchanging sensitive data, attitudes as well as routines of organizational members can significantly change over time. Moreover, substituting trust in organizations and people by trust in technology, as we propose to do with our SBS, is merely one solution - an alternative are trust-building measures, such as reputation - and has strong assumptions with regard to individual's behavior. Accordingly, empirical evaluation, and by this testing the behavioral assumptions, is an important next step.

With regard to its practical application, our conceptual SBS supports business professionals in both discovering and evaluating possible applications in a systematic way, which extends beyond juxtaposing concrete application examples. Concretely, an SBS will enable procurement managers to base their decisions on more accurate (unbiased) environmental data. In this context, we work on a modified algorithm for applicability of advanced non-parametric benchmarking methods such as DEA (Data Envelopment Analysis). The holistic cross-organizational assessment of environmental impacts provided by the SBS may encourage supply chain managers to rethink inventory and response management: collaborative optimization of sustainability performance of several actors within the value chain becomes much easier. This might pave the way for realizing a more sustainable supply chain management. Finally, results derived by the sustainability benchmarking service may also encourage corporate sustainability officers or board members in their decision to defend superior sustainable performance or to make up the gap in case of inferior performance.

Conclusion

Is there a solution to the information-sharing problem in the scope of inter-organizational sustainability benchmarking? Based on our findings, the answer to that question is yes: Our secure sustainability

benchmarking service (SBS) integrates ERP sustainability data in a secure and privacy-preserving manner. It uses homomorphic encryption to protect the data during processing and differential privacy to protect against leakages from the reports. The implementation of the SBS and our measurements show that the performance is manageable for the business user as well as the service provider. As our underlying assumption is that substituting trust in organizations and people through trust in a security mechanism, we will next try to build a prototype with industry partners in order to evaluate the SBS in a real environment. The current study offers a first step toward this goal.

References

Anderson, R. 2011. *Trusted Computing FAQ* http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html. Accessed 28 April 2011.

Anderson, R. and Needham, R. 1995. Programming Satan's Computer. In *Computer Science Today, LNCS 1000,* van Leeuwen, J. (ed.), pp. 426-440.

Benlian, A., Hess, T., and Buxmann, P. 2009. "Drivers of SaaS-Adoption – An Empirical Study of Different Application Types," *Business & Information Systems Engineering* (1:5), pp. 357–369.

Ben-Or, M., Goldwasser, S. and Wigderson, A. 1988. "Completeness theorems for non-cryptographic fault-tolerant distributed computation", in *Proceedings of the 20th ACM Symposium on Theory of Computing*, Chicago, IL, pp. 1-10.

Björklund, M. 'Benchmarking tool for improved corporate social responsibility in purchasing,' Benchmarking: An International Journal, (17:3), 2010, pp. 340–362.

Bohli, J.-M., Sorge, C. and Ugus O. 2010. "A Privacy Model for Smart Metering", in *Proceedings of the 1st IEEE International Workshop on Smart Grid Communications*, Cape Town, South Africa, pp. 1-5.

Brickell, J. and Shmatikov, V. 2008. "The cost of privacy: destruction of data-mining utility in anonymized data publishing", in *Proceedings of the 14th ACM Conference on Knowledge Discovery and Data Mining*, Li, Y., Liu, B., Sarawagi, S. (eds.), Las Vegas, NV, pp. 70-78.

Butler, T. 2011. "Compliance with institutional imperatives on environmental sustainability: Building theory on the role of Green IS," *Journal of Strategic Information Systems* (20:1), pp. 6–26.

Chatterji, A. K., and Toffel, M. W. 2010. "How firms respond to being rated," *Strategic Management Journal* (31:9), pp. 917–945.

Cho, C. H., and Patten, D. M. 2007. "The role of environmental disclosures as tools of legitimacy: A research note," *Accounting, Organizations and Society* (32:7-8), pp. 639–647.

Damgard, I. and Jurik, M. 2001. "A Generalisation, a Simplification and Some Applications of Paillier's Probabilistic Public-Key System," in *Proceedings of the 4th International Workshop on Practice and Theory in Public Key Cryptography*, Kim, K. (ed.), Cheju Island, Korea, pp. 119-136.

Dedrick, J. 2010. "Green IS: Concepts and Issues for Information Systems Research," *Communications of the Association for Information Systems* (27:1), pp. 173–184.

Dwork, C. 2006. "Differential Privacy," in *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming*, Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.), Venice, Italy, pp. 1-12.

Elliot, S. 2011. "Transdisciplinary Perspectives on Environmental Sustainability: A Resource Base and Framework for IT-Enabled Business Transformation," *MIS Quarterly*, (35: 1) pp.197-236.

European Comission 2011. *ELCD core database version II*. http://lca.jrc.ec.europa.eu/lcainfohub/datasetArea.vm. Accessed 15 April 2011.

Figge, F., and Hahn, T. 2005. "The Cost of Sustainability Capital and the Creation of Sustainable Value by Companies," *Journal of Industrial Ecology* (9:4), pp. 47–58.

Funk, B. Niemeyer, P. and Möller, A. 2009. "Integration of Environmental Management Information Systems and ERP systems using Integration Platforms" in *Information Technologies in Environmental Engineering,* Athanasiadis, I.N.; Mitkas, P.A.; Rizzoli, A.E.; Marx Gómez, J. (eds.) *Thessaloniki, Greece*, pp. 53-63.

Gentry, C. 2009. "Fully homomorphic encryption using ideal lattices," in *Proceedings of the 41st ACM Symposium on Theory of Computing*, Mitzenmacher, M. (ed.), Bethesda, MD, pp. 169-178.

Gentry, C. and Halevi, S. 2010. "Implementing Gentry's Fully-Homomorphic Encryption Scheme," *IBM Technical Report*.

Georges, A., Buytaert, D. and Eeckhout, L. 2007. "Statistically rigorous java performance evaluation," In *Proceedings of ACM International Conference on Object-Oriented Programming, Systems,*

Languages and Applications, Gabriel, R. P., Bacon, D. F., Videira Lopes, C., Steele Jr., G. L. (eds.), Montreal, Canada, pp. 57–76.
Goldreich, O., Micali, S. and Wigderson, A. 1987 "How to play any mental game," in *Proceedings of the 19th ACM Symposium on Theory of Computing*, New York, NY, pp. 218-229.
Hevner, A., March, S., Park, J., Ram, S. 2004. "Design Science Research in Information Systems," *MIS Quarterly* (28:1), pp. 75-105.
Hervani, A. A., Helms, M. M., and Sarkis, J. 2005. "Performance measurement for green supply chain management," *Benchmarking: An International Journal* (12:4), p. 330-353.
Ho, W., Xu, X., and Dey, P. K. 2010. "Multi-criteria decision making approaches for supplier evaluation and selection: A literature review," *European Journal of Operational Research* (202:1), pp. 16–24.
Hoffmann, V. H. and Busch, T. 2008. "Corporate Carbon Performance Indicators," *Journal of Industrial Ecology* (12:4), pp. 505–520.
Kerschbaum, F., Dahlmeier, D., Schropfer, A. and Biswas, D. 2009. "On the Practical Importance of Communication Complexity for Secure Multi-Party Computation Protocols," in *Proceedings of the 24th ACM Symposium on Applied Computing*, Shin, S. Y., Ossowski, S. (eds.), Honolulu, HI, pp. 2008-2015.
Koslowski, T. and Strüker, J. 2011. "Complementary effects and a Sustainability Benchmarking Software Service," *Business & Information Systems Engineering,* (forthcoming).
KPMG 2009. *KPMG International Survey of Corporate Responsibility Reporting 2008*. http://www.kpmg.nl/Docs/Corporate_Site/Publicaties/Corp_responsibility_Survey_2008.pdf. Accessed 15 August 2010.
Kumar, K. and Diesel, H. G. 1996. „Sustainable Collaboration: Managing Conflict and Cooperation in Interorganizational Systems", *MIS Quarterly,* (20:3), pp. 279-300.
Liu, J., Lu, Y.-H. and Koh, C.-K. 2010. "Performance Analysis of Arithmetic Operations in Homomorphic Encryption," *Purdue Technical Report TR-ECE-10-08*.
Machanavajjhala, A., Kifer, D., Gehrke, J. and Venkitasubramaniam, M. 2007. "L-diversity: Privacy beyond k-anonymity," *ACM Transactions on Knowledge Discovery from Data* (1:1),pp. 24-35.
Makrinou, A., Mandaraka, M., and Assimakopoulos, D. 2008. "Environmental benchmarking for management of energy and water use: A study of SMEs in the Mediterranean region," *Environmental Quality Management* (17:3), pp. 31–44.
Matthews, H. S., and Lave, L. B. 2003. "Using input-output analysis for corporate benchmarking," *Benchmarking: An International Journal* (10:2), pp. 153–168.
Melville, N. P. 2010. "Information Systems Innovation For Environmental Sustainability," *MIS Quarterly* (34:1), pp. 1–21.
Miakisz, J.A. 1999. "Measuring and Benchmarking Environmental Performance in the Electric Utility Sector," in *Sustainable Measures - Evaluation and Reporting of Environmental and Social Performance*, M. Bennett, P. James & L. Klinkers (eds.), Sheffield: Greenleaf Publishing, pp. 221-245.
Narayanan, A. and Shmatikov, V. 2009. "De-anonymizing social networks," in *Proceedings of the IEEE Symposium on Research in Security and Privacy,* Oakland, CA, pp. 173-187.
Narayanan, A. and Shmatikov, V. 2008. "Robust de-anonymization of large sparse datasets," in *Proceedings of the IEEE Symposium on Research in Security and Privacy*, Oakland, CA, pp. 111-125.
Paillier, P. 1999. "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," in *Advances in Cryptology – Proceedings of EUROCRPYT*, Stern, J. (ed.), Prague, Czech Republic, pp. 223-238.
Pineda-Henson, R., Culaba, A. B., and Mendoza, G. A. 2002. "Evaluating Environmental Performance of Pulp and Paper Manufacturing Using the Analytic Hierarchy Process and Life-Cycle Assessment," *Journal of Industrial Ecology* (6:1), pp. 15–28.
Reap, J., Roman, F., Duncan, S. and Bras, B. 2008 "A Survey of Unresolved Problems in Life Cycle Assessment. Part 2: Impact Assessment and Interpretation", *International Journal of Life Cycle Assessment* (13:5), pp. 374-388.
Rothenberg, S., Schenck, B. and Maxwell, J. 2005. "Lessons from benchmarking environmental performance at automobile assembly plants," *Benchmarking: An International Journal* (12:1), pp. 5–15.
Samarati, P. and Sweeney, L. 1998. "Generalizing data to provide anonymity when disclosing information (abstract)," in *Proceedings of the ACM Symposium on Principles of Database Systems,* Seattle, WA, p. 188.
SAP. 2011. *SAP Benchmarking - EMEA* http://benchmarking.sap.com/emea/. Accessed 28 April 2011.

Sarkis, J. 'Benchmarking the greening of business,' *Benchmarking: An International Journal*, (17:3), 2010, pp. 421–434.
Sarkis, J., and Talluri, S. 2002. "A Model for Strategic Supplier Selection," *Journal of Supply Chain Management* (38:1), pp. 18–28.
Saunders, C., Wu, Y. "., Li, Y., and Weisfeld, S. 2004. "Interorganizational trust in B2B relationships," in *Proceedings of the 6th international conference on Electronic commerce*, Janssen, M., Sol, H.G. and Wagenaar, R.W. (eds.), Delft, Netherlands, pp. 272–279.
Sharma, S., and Henriques, I. 2005. "Stakeholder influences on sustainability practices in the Canadian forest products industry," *Strategic Management Journal* (26:2), pp. 159–180.
Shaw, S., Grant, D. B. and Mangan, J. 2010. "Developing environmental supply chain performance measures," *Benchmarking: An International Journal* (17:3), pp. 320–339.
Watson, R. T., Boudreau, M.-C., and Chen, A. J. 2010. "Information Systems And Environmentally Sustainable Development: Energy Informatics and new Directions for the IS Community," *MIS Quarterly* (34:1), pp. 23–38.
Weidema, B. P., Thrane, M., Christensen, P., Schmidt, J., and Løkke, S. 2008. "Carbon Footprint," *Journal of Industrial Ecology* (12:1), pp. 3–6.
Wiedmann, T. O., Lenzen, M., and Barrett, J. R. 2009. "Companies on the Scale," *Journal of Industrial Ecology* (13:3), pp. 361–383.
Yao, A. 1986. "How to generate and exchange secrets," in *Proceedings of the 27th IEEE Symposium on Foundations of Computer Science*, Toronto, Canada, pp. 162-167.
Zhou, P., Ang, B. W., and Poh, K. L. 2008. "A survey of data envelopment analysis in energy and environmental studies," *European Journal of Operational Research* (189:1), pp. 1–18.