Knowledge Leakage in Collaborative Projects: Application of the ISM-MICMAC Model

Samuel Foli
Tallinn University of Technology,
Estonia
samuel.foli@taltech.ee

Susanne Durst
Tallinn University of Technology,
Estonia
susanne.durst@taltech.ee

Abstract

In this paper, we propose a holistic model that highlights the interrelationships among factors that contribute to knowledge leakage in collaborative projects using the interpretive structural modeling (ISM) technique and cross-impact matrix multiplication (MICMAC) analysis. Our study suggests that nine relevant factors influence knowledge leakage in collaborative projects. Incomplete contracts and insufficient technological competence are the root cause of knowledge leakage. Furthermore, the nine factors are categorized into two main clusters, namely dependency cluster - strong dependence power with weak driving power, and independent cluster - weak dependence power with strong driving power. Our study contributes several valuable insights to both theory and practice.

Keywords: Knowledge risk, Knowledge leakage, Collaborative projects, Interpretive structural model, MICMAC analysis, Knowledge leakage factor

1. Introduction

The role of networks, collaboration, and business relations as a pivotal factor for organizational performance is generally known (Laursen & Salter, 2006). Companies are increasingly embedded in ecosystems, a structure (governance form) designed to align the interests of different partners to create and capture value (Jacobides et al., 2018). Collaboration becomes even more valuable within such an environment; however, the valuable knowledge of partner organizations is also put at risk. This introduces the concept of knowledge risk, which is defined as "a measure of the probability and severity of adverse effects of any activities engaging or related somehow to knowledge that can affect the functioning of an organization on any level" (Durst & Zieba, 2019, p. 2). According to this definition, knowledge risk can arise at all levels of an organization, including operational or strategic levels. Similarly, in the case of collaboration, it is the decision-makers who decide at the strategic level, which then results in the implementation of the decision at the operational level, thus involving all levels of the organization. Due to these overlaps, it is not surprising that collaborative activities have been strongly associated with knowledge risk, as several studies have asserted (e.g. Foli, 2022, Temel & Vanhaverbeke, 2020). It is only when knowledge risk results in undesirable contingent events such as reputational damage, sustainability damage, and knowledge leakage (Durst & Zieba, 2019) that it becomes critical for organizations. Among the consequences of knowledge risks, the present paper concentrates on knowledge leakage, which is arguably one of the most pressing issues facing contemporary organizations (Martin et al., 2022). In this study, we define knowledge leakage as the occurrence of valuable organizational knowledge, such as best practices, strategies, and trade secrets, ending up in the hands of unauthorized parties.

In collaborative projects where organizations actively engage to achieve a common aim, protecting valuable organizational knowledge seems to be a difficult task, since the devices or technologies that facilitate seamless collaboration may also expose knowledge to leakage (Norman, 2002; Foli, 2022, Frishammar et al., 2015). This has made it very challenging for companies to find a balance between knowledge exchange and knowledge protection in order to reduce leakages. Due to this, academics (e.g. Ahlfänger et al., 2022; Qiu et al., 2016; Durst & Ferenhof, 2014; Parker, 2012) have extensively studied knowledge leakage in an attempt to achieve an equilibrium between these two opposing mechanisms (i.e., knowledge exchange and knowledge protection), however little is known about the factors that contribute to knowledge leakage.

Thus, in recent years, researchers have become increasingly interested in studying the factors that influence knowledge leakage in collaborative projects. For example, Fawad Sharif et al. (2022) examine how distrust, partner learning intent, and human resource

URI: https://hdl.handle.net/10125/103230
978-0-9981331-6-4

management influence knowledge leakage in collaboration projects. Jiang et al. (2016) test the link between partners' trustworthiness and knowledge leakage in a strategic alliance. Most of these studies primarily address external links (i.e. between influencing factors and knowledge leakage) but ignore the interrelationships between these influencing factors, which needs to be explored further. In understanding the interrelationships between these factors, causal links may be established, which is a requirement for theory building (Whetten, 1989). On this basis, the purpose of the present study is to develop and propose a holistic model that highlights the interrelationships among key factors that influence knowledge leakage in collaborative projects. To address the overall aim of the study, we formulate the following objectives:

- To identify relevant factors that have a significant influence on knowledge leakage in collaborative projects.
- To analyze and establish interrelationship among all the factors by using the interpretive structural model (ISM) technique.
- To categorize the factors based on driving and dependence power using the cross-impact matrix multiplication (MICMAC) analysis.

The paper is organized into five sections. Section two provides the background of knowledge leakage in collaborative projects. Section three provides a review of the knowledge leakage literature from the collaboration standpoint. In section four, the study's methodology and procedures are explained, while section five describes the model development and results. The discussion and conclusions are presented in section six.

2. Background

2.1. Knowledge leakage

Knowledge leakage is characterized by either inadvertent or intentional actions (Agudelo-Serna et al., 2017; Ahmad et al., 2014). This suggests that there are two types of knowledge leaks, namely intentional knowledge leakage and unintentional knowledge leakage. An intentional knowledge leak occurs when an employee of the focal firm unlawfully discloses the company's critical knowledge to other parties with the intent of benefiting themselves (Ritala et al., 2013). Alternatively, unintentional knowledge leakage is a situation where the focal firm is unaware that the knowledge is being transferred (Mohr & Sengupta, 2002), which is generally caused by frequent communication and interactions among employees often through strategic alliances (Kale et al., 2000).

2.2. Collaboration amid knowledge leakage

Global business environments are characterized by fierce competition, which discourages firms from entering into collaborations. However, as the saying goes “firms cannot operate in isolation”. Thus, collaboration among firms is inevitable. Regardless of the type of collaboration - whether being it internal or external, it aims to create an avenue for innovation through knowledge exchange (Fawad Sharif et al., 2021). Essentially, external collaboration comes in two forms, namely strategic alliances and co-opetition. Strategic alliance refers to “interfirm cooperative arrangements aimed at achieving the strategic objectives of the partners” (Das & Teng, 1998, p. 491). In other words, it involves two or more firms working together on a temporary basis to achieve a specific task through knowledge exchange. With co-opetition, the firms that enter into such collaborations are regarded as more or less competitors (Jiang et al., 2013), sharing the same resources, and competing for market shares and power. As Frishammar et al. (2015) indicate, knowledge leakage is an important concern in inter-organizational collaboration. Similarly, Inkpen et al. (2019) emphasize that knowledge leakage is unavoidable and naturally occurs in any cross-border inter-firm collaboration. Tan et al. (2016) also contend that supply chain processes can sometimes erode organizations' competitive edge and critical skills. Thus, we argue that while partners collaborate to achieve common benefits, they also compete to obtain private benefits. These partners tend to be even more selfish if their personal gain overrides the common objective, therefore posing a threat to misappropriating knowledge (Ritala et al., 2015).

3. Literature review of relevant factors selected for the study

3.1. Article selection protocol

In order to identify relevant factors influencing knowledge leakage in collaborative projects, a thorough literature review was conducted. We adopted a comprehensive search strategy adapted from Durst et al.'s (2015) work by using keyword combinations as follows: knowledge leakage OR information leakage OR knowledge risk OR knowledge loss. The Web of Science (WoS) database was used in the search. This database supposedly contains the largest repository of

academic social science papers (Kraus et al., 2022). As a result of the initial search, 1,558 full-text records were found. The authors then limited the initial search result to peer-reviewed research articles written in English language and in business/management subjects, thus resulting in 407 articles. Thereafter, we screened the abstract of the articles to remove irrelevant items (e.g. papers that are not aimed at knowledge leakage but mention it in the abstract), which resulted in 120 articles. In addition, the authors performed a full-text screening to exclude articles that do not relate to the topic area and only include those that address knowledge leakage from a collaboration point of view. This process yielded 32 peer-reviewed articles that met the inclusion and exclusion criteria. In the next section, we examine the final selected papers to identify the factors.

3.2. Factors of knowledge leakage in collaborative projects

Generally, knowledge leakage appears to be a topic that appears in a variety of academic disciplines (Durst, 2019). For the purposes of this study, we focus on factors that contribute to knowledge leakage in collaborative projects. A substantial number of studies have discussed the use of trust and contracts as approaches to controlling knowledge leakage during collaborative projects. In Frishammar et al.'s (2015) view, legal contractual frameworks provide an effective solution for preventing knowledge leakage. Therefore, a weakened legal framework may encourage partners to engage in any opportunistic behavior that they see fit. Similarly, Vafaei-Zadeh et al. (2020) assert that formal contracts are required to prevent intentional leakage. According to Ritala et al. (2015), non-disclosure agreements are among the mechanisms used to prevent leaks while Palomeras and Wehrheim (2021) argue that strong legal protection limits partners' use of leaked information, and thus mitigates opportunities for opportunism among partners.

An empirical investigation conducted by Jiang et al. (2013), investigated the relationship between trust and formal contracts in relation to the leakage of knowledge by a survey of 205 Chinese partnering firms. Results from their study supported the underlying assumptions that trust influences knowledge leakage. Fawad Sharif et al. (2020) explored how knowledge leakage in collaborative projects could be minimized. They found that contract completeness negatively affected knowledge leakage. In a similarly collaborative project context, Fawad Sharif et al. (2022) investigated ways to prevent knowledge leakage. Specifically, the authors focused on the role of distrust and partners' opportunism in knowledge leakage. Data were collected from 398 firms located in Pakistan. They found that distrust and partners' learning intent have a positive effect on knowledge leakage.

In a collaborative environment where employees from different firms interact, failure to enforce security policies sets the stage for knowledge leakage (Durst & Zieba, 2019; Altukruni et al., 2021). Having security policies in place ensures that all employees operate within a safe and secure framework that does not compromise the security of the company. Companies are increasingly allowing their employees to use their own devices to reduce costs, so the bring-your-own-devices (BYOD) initiative - whose implications have been identified as a potential source of knowledge leakage (Agudelo-Serna et al., 2017) - can be managed effectively through these security policies. Additionally, with the rapid adoption of digital transformation, employees' skills and competencies may be outdated for handling these emerging technologies, posing the risk of knowledge leakage through unintentional sharing of valuable organizational knowledge with outsiders (Altukruni et al., 2021).

The individual incentive is one form of knowledge leakage (Tan et al., 2016). Employees are likely to leak confidential information about their organizations to outsiders by using fraudulent means when incentives are offered (Tan et al., 2016; Nishat Faisal et al., 2007). Such practices are likely to be engaged by disloyal employees with the aim of benefiting themselves. Despite its serious implications, the issue has not yet been thoroughly studied (Tan et al., 2016). Also, another form of knowledge leakage may arise from collaboration between two or more competing organizations (Lee, 2002; Zhao et al., 2002). Cooperation between competing firms can, in certain situations, contribute to the leakage of knowledge, particularly when the appropriation of knowledge is valued more than its creation (Raza-Ullah & Eriksson, 2017).

4. Research methodology

To develop a holistic model of knowledge leakage in collaborative projects, the study is conducted in accordance with a three-step methodology which includes the following:

- Identification of factors that influence knowledge leakage in collaborative projects.
- Implementation of the ISM technique to build interrelationships between factors based on experts' opinions.

- Application of MICMAC analysis to determine the driving and dependent power of each factor.

The rationale behind the selection of the ISM technique in this study is based on the fact that the factors influencing knowledge leakage are complex in nature. In the context of this study, which focuses on collaborative projects, powerful techniques are needed to overcome such complexity, and ISM meets that need. Moreover, the application of the ISM technique allows input from experts during the analysis process, which is vital to producing an accurate and relevant model. Furthermore, the MICMAC analysis is useful for classifying factors according to their driving and dependence power. In this way, the properties of factors can be examined to gain a better understanding of how they behave.

4.1. Identification of factors of knowledge leakage in collaborative projects

In Table 1, we summarized factors that influence the occurrence of knowledge leakage in collaborative projects. Each factor has been assigned a code to facilitate the analysis phase. An explanation of how these factors relate to knowledge leakage in collaborative projects has been provided. Furthermore, references have been provided to support the factors identified.

Table 1. Literature support to the identified factors

Code	Factors	Descriptions	Supported literature
F1	Distrust	Neither of the partners involved in collaborative projects can be relied upon by the other.	(Qiu & Haugland, 2019; Jiang et al., 2016; Yang et al., 2019; Taylor, 2005; Guo et al., 2020; Deniaud et al., 2016; Fawad Sharif et al., 2020, 2022; Vafaei-Zadeh et al., 2020)
F2	Incomplete contracts	Weak or no legal contract in place to protect the core knowledge of partners involved in the collaboration.	(Jiang et al., 2013; Yang et al., 2019; Taylor, 2005; Guo et al., 2020; Ahlfänger et al., 2022; Deniaud et al., 2016; Fawad Sharif et al., 2020)
F3	Substandard security measures	Lack or inadequate security guidelines to oversee knowledge exchange between partners in collaborative projects.	(Hislop et al., 2018; Durst & Zieba, 2019; Frishammar et al., 2015; Altukruni et al., 2021)
F4	Weak BYOD policies	A lack of strict rules underpinning bring your own device (BYOD) policies could expose the focal and partner firms' core knowledge to cyberattacks.	(Agudelo-Serna et al., 2017; Shabtai et al., 2012; Altukruni et al., 2021)
F5	Insufficient technological competence	Emerging technologies used in collaborative projects put a firm's core knowledge at risk of leakage due to a lack of tech know-how.	(Ahmad et al., 2014; Hislop et al., 2018; Jiang et al., 2013; Christina et al., 2016; Altukruni et al., 2021; Zeiringer & Thalmann, 2021)
F6	Perceived opportunism	Partner's attempt to gain an advantage by misappropriating the core knowledge of the focal firm.	(Estrada et al., 2016; Fawad Sharif et al., 2020, 2022)
F7	Expected incentives	The act of exposing core knowledge to a partner or external party for an incentive by a player in collaborative projects.	(Tan et al., 2016)
F8	Existence of horizontal competition	Cooperation encourages partners to take advantage of exposed core knowledge.	(Lee, 2002; Zhao et al., 2002)
F9	Sub-contracting activities	Cooperation agreements between firms often result in subcontracting activities rather than collaborations, which often result in unknowingly transferred core knowledge.	(Tan et al., 2016; Foli, 2022; Nishat Faisal et al., 2007; Norman, 2004; Oxley & Wada, 2009; Li et al., 2012; Dye & Sridhar, 2003; Zhang et al., 2011)

4.2. Interpretive Structural Modeling (ISM)

The ISM is a multi-criteria decision analysis technique developed by Warfield (1973) to understand complex issues in which unorganized factors are analyzed and converted into a well-structured model. Interpretive nature of this technique is derived from its ability to utilize experts in its application. Using this

technique, the practical knowledge and experiences of experts are used to identify the inter-relationships among the factors and represent them in a systematic model. ISM is widely considered to be a powerful technique for identifying relationships between complex variables (Ahmad et al., 2019; Valmohammadi & Dashti, 2016). A number of fields have successfully applied ISM, including business and management (e.g. Pandey et al., 2022), economics (e.g. Gupta & Dhingra, 2022), and others. The following sections describe how we developed the ISM model.

4.2.1. Structural Self-Interaction Matrix (SSIM). The SSIM is created through the establishment of contextual relationships among the identified factors. A contextual relationship is established first based on the opinions of the experts involved. To establish the contextual relationship between the nine identified factors, a group of three experts - which met the minimum criteria in ISM application (Foli, 2022; Sivaprakasam et al., 2015) - were consulted. The three experts included two PhD researchers with expertise in knowledge risks and information systems, each with two to three years of experience, and one KM consultant with more than eight years of experience. Using four symbols, we solicited their opinions on the direction of the relationship between any two of the factors (i and j) as shown below:

- V: factor i leads to factor j (relation from i to j, but not vice versa)
- A: factor j leads to factor i (relation from j to i, but not vice versa)
- X: factor i and j leads to each other (relation from i to j and j to i)
- O: factor i and j not lead to each other (no relationship exists)

Based on the individual opinions that we have received from each expert, we aggregated the inputs into a single SSIM by applying the majority rule.

4.2.2. Reachability matrix. The reachability matrix is divided into two components, the initial reachability matrix and the final reachability matrix. The initial reachability matrix is derived directly from SSIM, where SSIM is converted to a binary matrix. This can be achieved using a simple set of rules including the following:

- If the (i, j) entry in the SSIM is V, then the (i, j) entry in the reachability matrix becomes 1, and the (j, i) entry becomes 0.
- If the (i, j) entry in the SSIM is A, then the (i, j) entry in the reachability matrix becomes 0, and the (j, i) entry becomes 1.
- If the (i, j) entry in the SSIM is X, then both the (i, j) and (j, i) entries of the reachability matrix become 1.
- If the (i, j) entry of the SSIM is O, then both the (i, j) and (j, i) entries of the reachability matrix become 0.

The final reachability matrix is then constructed based on the transitivity rule which states that if a factor i leads to factor j and factor j to factor k, factor i is directly related to factor k.

4.2.3. Level partitions. In this step, the reachability matrix is systematically partitioned into different levels. The reachability and antecedent sets are first obtained from the final reachability matrix, where the reachability set (Rsi) consists of the element itself and the other elements it may impact from in each column of the reachability matrix (RM), while the antecedent set (Asi) consists of the element itself and the other elements it may impact from in each row of the RM. An intersection set (Isi) is then derived based on the common elements found in the reachability set as well as the antecedent set in order to construct a level. Factors are assigned to a common level when all elements in its reachability set intersect with some of the elements in its antecedents set at a given iteration. Following each iteration, the factors that are successfully placed in a specific level are removed, allowing the process to continue until all factors have been partitioned exhaustively.

4.2.4. ISM based model. The final reachability matrix is used to construct a structured model. A form of graph known as a Digraph is initially created by illustrating relationships between any two factors using arrows, and representing each factor with a node. The term Digraph refers to a set of nodes (i.e., representing factors) interconnected with arrows indicating the direction between each node. The initial Digraph is derived from the reachability matrix containing the transitive links. After eliminating the transitive links, a final Digraph is obtained. The finalized digraph is then converted into ISM model. Finally, the ISM model visualizes the interrelationships between each factor according to the assigned level obtained during the iteration process.

4.3. MICMAC analysis

MICMAC analysis was originally proposed by Duperrin and Godet (1973), which is useful for

determining the driving power and dependence power of variables. To perform the MICMAC analysis in this study, we plotted the factors' dependence versus the factors' driving power, which is derived from the final reachability matrix. On the basis of the plotted location, factors are grouped into four clusters: autonomous, dependent, linkage, and independent. The autonomous cluster contains factors with low driving power and low dependent power. These factors are often referred to as excluded factors due to their limited influence. The dependent cluster contain factors with a low driving power but high dependence power. The linkage cluster consists of factors with high dependence and driving power and are typically unstable. Lastly, the independent cluster contains factors with low dependence power and high driving power, which are referred to as drivers. As a general rule, each factor falls into one cluster and is illustrated visually using a four-quadrant graph (Jain & Sharma, 2019).

5. ISM-MICMAC model

The integrated ISM-MICMAC model was applied to the nine factors associated with knowledge leakage in collaborative projects. Based on the contextual relationships established by the experts, the aggregate result is represented as the SSIM using the dominant opinion, with equal weight given to all experts. In the results, incomplete contracts (F2), substandard security measures (F3), weak BYOD policies (F4), and insufficient technological competence (F5) lead to perceived opportunism (F6). In addition, the results indicate that substandard security measures (F3), weak BYOD policies (F4), and insufficient technological competence (F5) are not related to the existence of horizontal competition (F8). Table 2 summarizes the SSIM.

Table 2. Structural self-interaction matrix

F's	F1	F2	F3	F4	F5	F6	F7	F8	F9
F1	X	A	O	O	O	X	A	X	O
F2		X	O	O	O	V	V	V	V
F3			X	X	O	V	V	O	O
F4				X	O	V	O	O	O
F5					X	V	O	O	V
F6						X	X	X	A
F7							X	X	A
F8								X	O
F9									X

Following the rules outlined in the research methodology, the SSIM is successfully transformed into a binary matrix. This binary matrix is also referred to as the initial reachability matrix, as shown in Table 3.

Table 3. Initial reachability matrix

	F1	F2	F3	F4	F5	F6	F7	F8	F9
F1	1	0	0	0	0	1	0	1	0
F2	1	1	0	0	0	1	1	1	1
F3	0	0	1	1	0	1	1	0	0
F4	0	0	1	1	0	1	0	0	0
F5	0	0	0	0	1	1	0	0	1
F6	1	0	0	0	0	1	1	1	0
F7	1	0	0	0	0	1	1	1	0
F8	1	0	0	0	0	1	1	1	0
F9	0	0	0	0	0	1	1	0	1

The conversion of the initial reachability matrix into the final reachability matrix is executed according to the transitivity rule (see research methodology). With the rule applied, eleven of the entries in the initial reachability matrix are transformed from "0" to "1" in the final reachability matrix. They are designated as "*1" as shown in Table 4. In addition, the final reachability matrix provides each factor's driving power (DrP) and dependence power (DeP) derived from counts of the matrix columns and rows respectively, for later use in the MICMAC analysis.

Table 4. Final reachability matrix

F's	F1	F2	F3	F4	F5	F6	F7	F8	F9	**DrP**
F1	1	0	0	0	0	1	*1	1	0	**4**
F2	1	1	0	0	0	1	1	1	1	**6**
F3	*1	0	1	1	0	1	1	*1	0	**6**
F4	*1	0	1	1	0	1	*1	*1	0	**6**
F5	*1	0	0	0	1	1	*1	*1	1	**6**
F6	1	0	0	0	0	1	1	1	0	**4**
F7	1	0	0	0	0	1	1	1	0	**4**
F8	1	0	0	0	0	1	1	1	0	**4**
F9	*1	0	0	0	0	1	1	*1	1	**5**
DeP	**9**	**1**	**2**	**2**	**1**	**9**	**9**	**9**	**3**	

After three iterations (Iters) on the final reachability matrix, three levels were determined as shown in Table 5. Level 1 includes four factors, namely distrust (F1), perceived opportunism (F6), expected incentives (F7), and horizontal competition (F8). Level 2 contains substandard security measures (F3), weak BYOD policies (F4) and subcontracting activities (F9). Lastly, level 3 includes incomplete contracts (F2) and insufficient technological competence (F5).

Table 5. Partition of factor level

F's	Rsi	Asi	Isi	Level
Iter 1				
F1	1,6,7,8	1,2,3,4,5,6,7,8,9	1,6,7,8	I
F2	1,2,6,7,8,9	2	2	
F3	1,3,4,6,7,8	3,4	3,4	
F4	1,3,4,6,7,8	3,4	3,4	
F5	1,5,6,7,8,9	5	5	
F6	1,6,7,8	1,2,3,4,5,6,7,8,9	1,6,7,8	I
F7	1,6,7,8	1,2,3,4,5,6,7,8,9	1,6,7,8	I
F8	1,6,7,8	1,2,3,4,5,6,7,8,9	1,6,7,8	I
F9	1,6,7,8,9	2,5,9	9	
Iter 2				
F2	2,9	2	2	
F3	3,4	3,4	3,4	II
F4	3,4	3,4	3,4	II
F5	5,9	5	5	
F9	9	2,5,9	9	II
Iter 3				
F2	2	2	2	III
F5	5	5	5	III

The ISM model, after partitioning the factors, displays the results in a hierarchical structure (see Figure 2). MICMAC analysis is also represented in Figure 1 using the driving power and dependence power derived from the final reachability matrix.

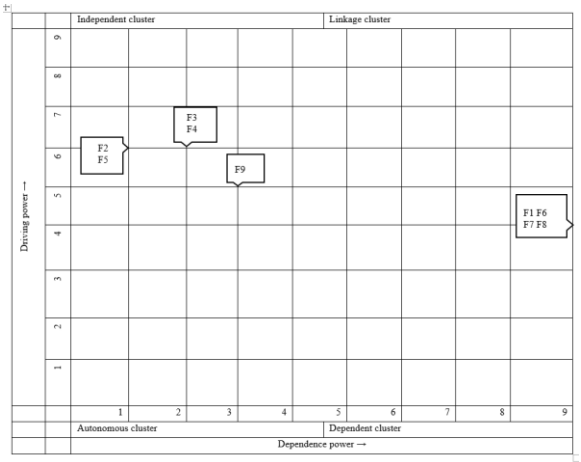

Figure 1. MICMAC analysis

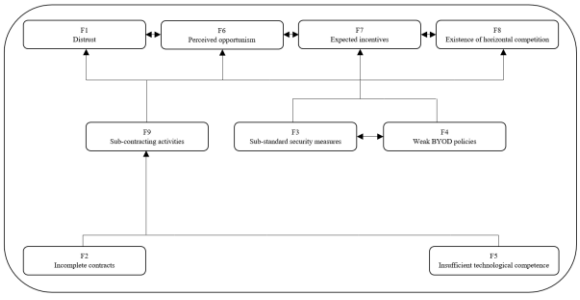

Figure 2. ISM model.

6. Discussion and conclusion

Following the objectives set forth in this paper, we discuss each as follows:

Objective 1: To identify relevant factors that have a significant influence on knowledge leakage in collaborative projects.

Our findings reveal nine key factors associated with knowledge leakage in collaborative projects. Accordingly, these factors include distrust, incomplete contracts, sub-standard security measures, weak BYOD policies, insufficient technological competence, perceived opportunism, expected incentives, existence of horizontal competition and sub-contracting activities. Given that these factors were derived from literature, they were subjected to expert evaluation in order to determine their relevance. Also, the expert opinions provided a strong foundation for minimizing biases. We, therefore, consider these factors relevant to knowledge leakage in collaborative projects.

Objective 2: To analyze and establish interrelationship among all the factors by using the interpretive structural model (ISM) technique.

The main findings are summarized in the ISM model. According to our model, incomplete contracts and insufficient technological competence are the principal factors contributing to knowledge leakage within collaborative projects. In other words, incomplete contracts and insufficient technological expertise influence the greatest number of factors. Besides the sub-standard security measures and weak BYOD policies, incomplete contracts and insufficient technological competence are the only factors that have links to any other factor.

Several studies have evaluated the occurrence of knowledge leakage in collaborative projects using contract completeness. Most findings indicate a negative relationship between contract completeness and knowledge leakage (e.g. Fawad Sharif et al., 2022).

On the contrary, their research implies that partners will display opportunistic behavior in a situation where intellectual property rights, roles and responsibilities in each partner are not clearly defined by the agreement.

According to our findings, weak BYOD policies with sub-substance security measures are inextricably linked. Given that both factors are characteristically policy-oriented, it is not surprising that they are interrelated. Interestingly, this result agrees with Altukruni et al. 's study (2021) which referred to the two practices as poor security practices interchangeably. Similarly, Agudelo-Serna et al. (2017) group them together under technical factors

that affect knowledge leakage. Consequently, our findings are consistent with those of these studies.

Our findings suggest there is a connection between distrust, perceived opportunism, expected incentive, and existence of horizontal competition. Prior studies have investigated the relationship between distrust and perceived opportunism. In a study by Fawad Sharif et al. (2022), it was confirmed that partners' learning intent and knowledge leakage is mediated by distrust. Therefore, in the presence of distrust, partners are likely to change their learning intent by misappropriating knowledge opportunistically. This is in line with their findings. A further study can test the remaining relationships that lack sufficient support in the literature.

Objective 3: To categorize the factors based on driving and dependence power using MICMAC analysis.

Our results, according to the MICMAC analysis, indicate two clusters of factors associated with knowledge leakage in collaborative projects. These include:

Independent cluster – This cluster consists of factors with a strong driving power but a weak dependence power. Based on our findings, incomplete contracts (F2), sub-standard security measures (F3), weak BYOD policies (F4), insufficient technological competence (F5) and sub-contracting activities (F9) are grouped in this cluster. Generally, driving forces are more powerful than dependence forces, since a high level of driving power can stimulate other factors, ultimately increasing the likelihood of knowledge leakage. For this reason, the findings suggest that F2, F3, F4, F5 and F9 should be given the utmost attention to narrow the likelihood of such an event occurring.

Dependent cluster – In this cluster of factors, they exhibit strong dependency power, but weak driving power. Our results indicate distrust (F1), perceived opportunism (F6), expected incentives (F7), and existence of horizontal competition (F8) all fall into this cluster. The dependence force of F1, F6, F7 and F8 is relatively higher than their driving force, which makes them less influential in comparison with the previous factors in the independent cluster.

Our study contributes to both theory and practice in several ways. This paper fills a theoretical gap on the development of a holistic model that explains the interrelationship between factors of knowledge leakage. This is of particular importance since in earlier studies of knowledge leakage, only a few factors were considered without any consideration of their interconnections. In addition, the study theoretically contributes to previous literature by demonstrating that incomplete contracts and insufficient technological competence play a significant role in the occurrence of knowledge leakage, particularly in collaborative projects. This research demonstrates the complexity of knowledge leakage, thereby addressing an issue that is often mentioned, but never explicitly demonstrated. Finally, the use of ISM and MICMAC techniques provides methodological contributions in the knowledge risk and leakage literature since this appears to be the first successful study using these approaches.

This study has profound implications for practitioners in the following ways, as demonstrated by its findings. First of all, we have concluded that knowledge leakages are influenced by a number of factors, especially within the context of collaboration. As a result, firms that collaborate are more vulnerable if they are unaware of these factors or pretend not to be concerned when these factors arise. Despite the fact that knowledge leakage cannot be totally eradicated, it can be managed through a proactive and holistic approach, as we have seen from studies (e.g., Durst & Ferenhof, 2014). However, it is essential to have a thorough understanding of the factors that may influence its occurrence before pursuing measures to address knowledge leakage. While not exhaustive, this present paper has attempted to provide a comprehensive list of these factors. Additionally, the developed ISM model would assist risk managers in understanding the relative importance of these factors, i.e., to identify the most significant factors that require immediate attention. The proposed model and results of this study are not limited to evaluating the factors, but aim also to provide insights for risk and project managers to understand the nature and properties of these factors based on the MICMAC diagram. Further, the results of this study would inform CEOs, managers, and directors in making strategic decisions regarding the selection of partnerships that are trustworthy with the knowledge shared in order to control opportunism and misappropriation.

In our study, we found that there are several unexplored areas of knowledge leakage which can be tested using structural equation modeling (SEM). We have formulated these areas into research questions as follows: (1) What are the mediating effects of sub-contracting activities on the relationship between contract completeness and knowledge leakage? (2) What role do sub-contracting activities play in the relationship between insufficient technological competence and knowledge leakage? and (3) To what extent does individual incentive contribute to knowledge leakage?

7. References

Agudelo-Serna, C. A., Bosua, R., Ahmad, A., & Maynard, S. (2017). Strategies to Mitigate Knowledge Leakage Risk caused by the use of mobile devices: A Preliminary Study. *Proceedings of the 38th International Conference on Information Systems*, Seoul, Korea, 1-24. https://aisel.aisnet.org/icis2017/Security/Presentations/24.

Ahlfänger, M., Gemünden, H. G., & Leker, J. (2022). Balancing knowledge sharing with protecting: The efficacy of formal control in open innovation projects. *International Journal of Project Management*, *40*(2), 105-19.

Ahmad, A., Bosua, R., & Scheepers, R. (2014). Protecting organizational competitive advantage: A knowledge leakage perspective. *Computers & Security*, *42*, 27-39.

Ahmad, M., Tang, X. W., Qiu, J. N., & Ahmad, F. (2019). Interpretive structural modeling and MICMAC analysis for identifying and benchmarking significant factors of seismic soil liquefaction. *Applied Sciences*, *9*(2), 233.

Altukruni, H., Maynard, S. B., Alshaikh, M., & Ahmad, A. (2021). Exploring Knowledge Leakage Risk in Knowledge-Intensive Organisations: behavioural aspects and key controls. *Australasian Conference on Information Systems*, Perth, Australia.

Christina, S., Stefan, T., & Markus, M. (2016). Protecting knowledge in the financial sector: An analysis of knowledge risks arising from social media. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 4031-4040). IEEE.

Das, T. K., & Teng, B. S. (1998). Between Trust and Control: Developing Confidence in Partner Cooperation in Alliances. *The Academy of Management Review*, *23*(3), 491-512.

Deniaud, I. F., Marmier, F., Gourc, D., & Bougaret, S. (2016). A risk management approach for collaborative NPD project. In *2016 International Conference on Industrial Engineering, Management Science and Application (ICIMSA)* (pp. 1-5). IEEE.

Duperrin, J., & Godet, M. (1973). Methode De Hierar Chization Des Elements D'um System. *Rapport Economique De CEA*, *1*(2), 45–51.

Durst, S. (2019). How far have we come with the study of knowledge risks? *Vine Journal of Information and Knowledge Management Systems*, *49*(1), 21-34.

Durst, S., Aggestam, L., & Ferenhof, H. A. (2015). Understanding knowledge leakage: a review of previous studies. *Vine Journal of Information and Knowledge Management Systems*, *45*(4), 568-586.

Durst, S., & Ferenhof H. A. (2014). Knowledge Leakages and Ways to Reduce Them in Small and Medium-Sized Enterprises (SMEs). *Information*, *5*(3), 440-450.

Durst, S., & Zieba, M. (2019). Mapping knowledge risks: towards a better understanding of knowledge management. *Knowledge Management Research & Practice*, *17*(1), 1-13.

Dye, R. A., & Sridhar, S. S. (2003). Investment Implications of Information Acquisition and Leakage. *Management Science*, *49*(6), 767-83.

Estrada, I., Faems, D., & de Faria, P. (2016). Coopetition and product innovation performance: The role of internal knowledge sharing mechanisms and formal knowledge protection mechanisms. *Industrial Marketing Management*, *53*, 56-65.

Fawad Sharif, S. M., Naiding, Y., & Kifayat Shah, S. (2022). Restraining knowledge leakage in collaborative projects through HRM. Vine Journal of Information and Knowledge Management Systems. https://doi.org/10.1108/VJIKMS-09-2021-0228.

Fawad Sharif, S. M., Naiding, Y., Xu, Y., & Rehman, A. u. (2020). The effect of contract completeness on knowledge leakages in collaborative construction projects: a moderated mediation study. *Journal of Knowledge Management*, *24*(9), 2057-78.

Fawad Sharif, S. M., Yang, N., Rehman, A. u., Kanwal, F., & WangDu, F. (2021). *Protecting organizational competitiveness from the hazards of knowledge leakage through HRM. Management Decision*, *59*(10), 2405-20.

Foli, S. (2022). Total interpretive structural modelling (TISM) and MICMAC approach in analysing knowledge risks in ICT-supported collaborative project. *Vine Journal of Information and Knowledge Management Systems*. https://doi.org/10.1108/VJIKMS-09-2021-0205.

Frishammar, J., Ericsson, K., & Patel, P. C. (2015). The dark side of knowledge transfer: Exploring knowledge leakage in joint R&D projects. *Technovation*, *41*, 75-88.

Guo, W., Yang, J., Li, D., & Lyu, C. (2020). Knowledge sharing and knowledge protection in strategic alliances: the effects of trust and formal contracts. *Technology Analysis & Strategic Management*, *32*(11), 1366-78.

Gupta, S., & Dhingra, S. (2022). Modeling the key factors influencing the adoption of mobile financial services: an interpretive structural modeling approach. *Journal of Financial Services Marketing*, *27*(2), 96-110.

Hislop, D., Bosua, R., & Helms, R. (2018). *Knowledge management in organizations: A critical introduction*. Oxford university press.

Inkpen, A., Minbaeva, D., & Tsang, E. W. (2019). Unintentional, unavoidable, and beneficial knowledge leakage from the multinational enterprise. *Journal of International Business Studies*, *50*(2), 250-260.

Jacobides, M. G., Cennamo, C., & Gawer, A. (2018). Towards a theory of ecosystems. *Strategic Management Journal*, *39*(8), 2255-76.

Jain, P., & Sharma, S. (2019). Prioritizing factors used in designing of test cases: An ISM-MICMAC based analysis. In *2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)* (Vol. 1, pp. 1-4). IEEE.

Jiang, X., Bao, Y., Xie, Y., & Gao, S. (2016). Partner trustworthiness, knowledge flow in strategic alliances, and firm competitiveness: *A contingency perspective. Journal of Business Research*, *69*(2), 804-14.

Jiang, X., Li, M., Gao, S., Bao, Y., & Jiang, F. (2013). Managing knowledge leakage in strategic alliances: The effects of trust and formal contracts. *Industrial Marketing Management*, *42*(6), 983-91.

Kale, P., Singh, H., & Perlmutter, H. (2000). Learning and protection of proprietary assets in strategic alliances: Building relational capital. *Strategic management journal*, *21*(3), 217-237.

Kraus, S., Durst, S., Ferreira, J. J., Veiga, P., Kailer, N., & Weinmann, A. (2022). Digital transformation in business and management research: An overview of the current status quo. *International Journal of Information Management*, *63*, 102466.

Laursen, K., & Salter, A. (2006). Open for innovation: the role of openness in explaining innovation performance among U.K. manufacturing firms. *Strategic Management Journal*, *27*(2), 131-50.

Lee, H. L. (2002). Aligning Supply Chain Strategies with Product Uncertainties. *California Management Review*, *44*(3), 105-19.

Martin, M., Sunmola, F., & Lauder, D. (2022). Unintentional Compromising Electromagnetic Emanations from IT Equipment: A Concept Map of Domain Knowledge. *Procedia Computer Science*, *200*, 1432-1441.

Mohr, J. J., & Sengupta, S. (2002). Managing the paradox of inter-firm learning: the role of governance mechanisms. *Journal of Business & Industrial Marketing*, *17*(4), 282-301

Nishat Faisal, M., Banwet, D. K. and Shankar, R. (2007). Information risks management in supply chains: an assessment and mitigation framework. *Journal of Enterprise Information Management*, *20*(6), 677-99.

Norman, P. M. (2002). Protecting knowledge in strategic alliances: Resource and relational characteristics. *The Journal of High Technology Management Research*, *13*(2), 177-202.

Norman, P. M. (2004). Knowledge acquisition, knowledge loss, and satisfaction in high technology alliances. *Journal of Business Research*, *57*(6), 610-19.

Oxley, J., & Wada, T. (2009). Alliance Structure and the Scope of Knowledge Transfer: Evidence from U.S.-Japan Agreements. *Management Science*, *55*(4), 635-49.

Palomeras, N., & Wehrheim, D. (2021). The strategic allocation of inventors to R&D collaborations. *Strategic Management Journal*, *42*(1), 144-69.

Pandey, P., Agrawal, N., Saharan, T., & Raut, R. D. (2022). Impact of human resource management practices on TQM: an ISM-DEMATEL approach. *The TQM Journal*, *34*(1), 199-228.

Parker, H. (2012). Knowledge acquisition and leakage in inter-firm relationships involving new technology-based firms. *Management Decision*, *50*(9), 1618-1633.

Qiu, X., & Haugland, S. A. (2019). The role of regulatory focus and trustworthiness in knowledge transfer and leakage in alliances. *Industrial Marketing Management*, *83*, 162-73.

Raza-Ullah, T., & Eriksson, J. (2017). Knowledge sharing and knowledge leakage in dyadic coopetitive alliances involving SMEs. In *Global opportunities for entrepreneurial growth: Coopetition and knowledge dynamics within and across firms*. Emerald Publishing Limited.

Ritala, P., Olander, H., Michailova, S., & Husted, K. (2013). Knowledge sharing, knowledge leaking and innovation performance: An empirical study. In *ISPIM Conference Proceedings* (p. 1). The International Society for Professional Innovation Management (ISPIM).

Ritala, P., Olander, H., Michailova, S., & Husted, K. (2015). Knowledge sharing, knowledge leaking and relative innovation performance: An empirical study. *Technovation*, *35*, 22-31.

Shabtai, A., Elovici, Y., & Rokach, L. (2012). *A survey of data leakage detection and prevention solutions*. Springer Science & Business Media.

Sivaprakasam, R., Selladurai, V., & Sasikumar, P. (2015). Implementation of interpretive structural modelling methodology as a strategic decision making tool in a Green Supply Chain Context. *Annals of Operations Research*, *233*(1), 423-448.

Tan, K. H., Wong, W. P., & Chung, L. (2016). Information and Knowledge Leakage in Supply Chain. *Information Systems Frontiers*, *18*(3), 621-38.

Taylor, A. (2005). An operations perspective on strategic alliance success factors. *International Journal of Operations & Production Management*, *25*(5), 469-90.

Temel, S., & Vanhaverbeke, W. (2020). Knowledge risk management during implementation of open innovation. In *Knowledge Risk Management* (pp. 207-227). Springer, Cham.

Vafaei-Zadeh, A., Ramayah, T., Hanifah, H., Kurnia, S., & Mahmud, I. (2020). Supply chain information integration and its impact on the operational performance of manufacturing firms in Malaysia. *Information & Management*, *57*(8), 103386.

Valmohammadi, C., & Dashti, S. (2016). Using interpretive structural modeling and fuzzy analytical process to identify and prioritize the interactive barriers of e-commerce implementation. *Information & Management*, *53*(2), 157-168.

Warfield, J. N. (1973). On arranging elements of a hierarchy in graphic form. *IEEE Transactions on Systems, Man, and Cybernetics*, (2), 121-132.

Whetten, D. A. (1989). What constitutes a theoretical contribution? *The Academy of Management Review*, *14*(4), 490-495.

Yang, Q., Liu, Y., & Li, Y. (2019). How do an alliance firm's strategic orientations drive its knowledge acquisition? Evidence from Sino-foreign alliance partnership. *Journal of Business & Industrial Marketing*, *34*(2), 505-17.

Zeiringer, J. P., & Thalmann, S. (2021). Knowledge sharing and protection in data-centric collaborations: An exploratory study. *Knowledge Management Research & Practice*, 1-13.

Zhang, D. Y., Zeng, Y., Wang, L., Li, H., & Geng, Y. (2011). Modeling and evaluating information leakage caused by inferences in supply chains. *Computers in Industry*, *62*(3), 351-63.

Zhao, X., Xie, J., & Zhang, W. J. (2002). The impact of information sharing and ordering co-ordination on supply chain performance. *Supply Chain Management: An International Journal*, *7*(1), 24-40.