sustainability

MDPI

Article

Corporate Data Sharing, Leakage, and Supervision Mechanism Research

Haifei Yu * and Xinyu He

School of Business Administration, Northeastern University, Shenyang 110819, China; 1801133@stu.neu.edu.cn
* Correspondence: hfyu@mail.neu.edu.cn

Abstract: Data sharing helps to make full use of each other's data and enable the digital economy. With the gradual rise of corporate data sharing, the frequent occurrence of data leakage events highlights the dilemma of data sharing, leakage and supervision, which infringes on the data assets of the leaked party. Our paper aims to design an effective data supervision mechanism and achieve the stability of data sharing alliance. Therefore, this paper considers the data technology capabilities of both parties of the data sharing alliance and the benefits and loss of data leakage, establishes the game model and supervision mechanism of data sharing, leakage and supervision under the condition of complete information, and analyzes the game equilibrium and the influence of different supervision levels on the company's data sharing and leakage behavior. The results show that the company sharing and leaking behavior is affected by both the level of data supervision fines and the relative technical level. Our model can make up for the weakness of the low-tech company, control the company's choice of leaking behaviors, and ensure the stability of data sharing alliance by designing reasonable data supervision mechanism, especially the severe data supervision strategy.

Keywords: data sharing; data leakage; complete information game; supervision mechanism

Citation: Yu, H.; He, X. Corporate Data Sharing, Leakage, and Supervision Mechanism Research. *Sustainability* **2021**, *13*, 931. https://doi.org/10.3390/su13020931

Received: 9 December 2020
Accepted: 14 January 2021
Published: 18 January 2021

1. Introduction

In recent years, data has become an important asset for many organizations, providing new business opportunities for enterprises to improve their business operations [1]. The increasing need for large-scale and interdisciplinary research provides momentum for initiating data sharing [2]. Data sharing refers to sharing one's original data with others in a formal or informal way, which provides "raw materials" for data analysis, reduces repetitive labor, and enables data to be acquired by stakeholders in a timely manner to release data value [3]. Enterprises often achieve significant results in strategic technology, economic benefits, and risk control by establishing data sharing alliance to achieve data sharing [4,5]. Therefore, this study considers that data sharing is a new cooperative mode for data enterprises through transferring the right to use data to its data partner, obtaining more external data, improving enterprise innovation ability, and reducing social costs through data fusion.

The data sharing alliance based on protocol can drive the development of related industries. But in recent years, frequent data leakage events also cause enterprise data sharing to face challenges [6,7]. Data leakage usually involves the large-scale release of customers' sensitive data to external parties. Customers may feel more vulnerable about their information privacy [8]. The loss of sensitive information can lead to significant reputational damage and financial losses, and can even be detrimental to the long-term stability of an organization [9]. Over the past few years, there have been many data loss incidents that cost companies millions of dollars. For example, in 2017, Equifax announced that more than 145 million customers' sensitive information had been stolen, resulting in 240 consumer lawsuits resulting in nearly $90 million in default-related costs [10,11]. Previous studies have shown that data leakage can reduce the market value of enterprises, cause large

fluctuations in the stock market [12], and even affect the behaviors of competitors in the market [13].

Data leakage not only affects the standard operation of the data market, but also threatens the property of enterprises and individual users, so it has been of wide concern in recent years [14]. In order to prevent data leakage, some regulators have introduced data protection policies, using national regulations to avoid the risk of data leakage. In addition, there are also studies from the perspective of data technology to fill technical loopholes and reduce the risk of data leakage through technology upgrading and improvement. However, different from data leakage caused by external attacks, data sharing enterprises need to exchange their data, so it is difficult to prevent data leakage by technical means. Meanwhile, current regulatory measures at the legal level only provide limited insights for management of data leakage events [15]. Therefore, it is urgent to effectively manage data leakage events in the process of enterprise data sharing, solve enterprises' concerns about data leakage, and maintain the stability of the data sharing alliance [16,17].

To address this gap, we ask the following research questions: How do data sharing companies manage data leakage by monitoring each other? To solve this problem and protect the rights and interests of data sharing enterprises, consider data sharing subject to sharing costs and returns arising from sharing activities, and the extent of encryption, Data Leakage Protection, and other related technologies [18]. This paper proposes a data sharing, leakage, and supervision model that influences different data sharing and leakage behaviors of companies through mutual supervision of data sharing companies. The main contributions of this paper are as follows:

(1) Considering the influencing factors of inter-company data sharing, leakage, and supervision behaviors, establish a data sharing, leakage, and supervision model, and analyze corporate data sharing and leakage behaviors.
(2) Considering the data technical capabilities of both parties of the data sharing alliance and the revenue or loss of data leakage, design a data supervision mechanism based on fines and analyze how different levels of supervision affect data sharing and leakage behavior.
(3) Solve the game equilibrium and conditions of company supervision under different technical levels, data leaking behaviors, and data leaking penalty levels, and then discuss the stability conditions of Data Sharing Alliance, as well as data sharing, data leakage, and data supervision of companies' effectiveness strategies.
(4) Simulation analysis is used to verify the validity and accuracy of the model, analyze the impact of data supervision mechanism on the game decision-making of data sharing alliance, and provide a scientific basis for enterprise data sharing, data leakage, and supervision. In the extended discussion, the case of "SF: Data War" from Harvard Business School is cited to further discuss the management role of regulatory mechanism in the actual data sharing process.

The rest of the paper is organized as follows: Section 2 discusses related work. Section 3 introduces the system model. In Section 4, we make a Nash equilibrium analysis of the data sharing, data leakage, and data supervision models established in this paper. Section 5 validates the validity of the model using simulation analysis and draws some management implications of enterprise data sharing through the analysis of the real case's background. Section 6 summarizes this work and puts forward some policies on data sharing, data leakage, and data supervision.

2. Theoretical Background

2.1. Data Sharing

With the rapid development of Artificial Intelligence, Internet of Things, and other emerging technologies, and the arrival of the data economy era, more organizations are aware of the considerable role that data may play indeed. In the field of scientific research, due to the great value of data sharing for science and data research, developed countries are actively promoting the sharing of scientific research data, and a nationwide research

data platform was designed in 2008 [19]. On the business side, the vast amount of data generated in the big data age makes companies interested in sharing data with each other for greater value [20]. In the research of the Internet of Things which is closely related to data sharing, facing the dramatic increase of data amount, how to establish an effective data sharing mechanism for different organizations in the Internet of Things has become a new challenge [21]. However, ensuring the security of sensitive data is an important issue in the process of data processing, storage, and sharing [22].

With the increasing use of large data, it is necessary to share data of different quality to expand data dissemination, and also to control data acquisition and ensure the security of data sharing [23]. The data war between SF Express and Cainiao Company in 2017 exposed the real dilemma of data sharing facing potential data leakage [24]. In recent years, data leakage events have occurred frequently, and due to the lack of effective data supervision strategy, it is difficult to define responsibility after data leaks, which hinders the development of data sharing [25].

2.2. Data Leakage

In recent years, to overcome the threat of data leakage, many enterprises begin to control the access and use of data. However, they do not effectively protect data assets [26]. According to Data Loss, about 50% of data leaks occur in the business sector in 2014. When commercial secrets and customer data are leaked to competitors, it can cause millions of dollars of business loss [27]. The Guardian revealed in April 2018 that Facebook, the largest SNS website, leaked about 87 million personal user's data [28]. The data leakage events indicated that data leakage will incur enormous financial costs, affect the company's market reputation, harm the interests of stakeholders, and expose personal data to security risks [29].

Based on the impact of data leakage on the development of enterprise data sharing, scholars have studied data leakage. Data leakage is a condition where data is confidentiality compromised. There are several main reasons for data leakage, as follows: (1) intentional disclosure of data by opponents within the organization; (2) disclosure by people outside the organization who have temporary access to the resources of the victim organization; (3) unintentional disclosure by internal users or administrators [30]. From the above reasons for data leakage, there are two ways for enterprise data leakage: internal and external. Both ways can be solved by strengthening training and education within the enterprise; for external leaks, existing research mainly focuses on technical solutions to data leaks. For example, considering the leak problem in the development of big data, which restricts the development of industry, based on block chain technology, a large data sharing model of smart contract is proposed to ensure the safe sharing of data [31]. To address the security and effectiveness of corporate data sharing, a group data sharing protocol is proposed using Symmetric Balanced Incomplete Block Design, which implements data sharing in cloud computing [32]. However, data sharing allows arbitrary access to data, leading to unavoidable external leaks of confidential data, causing greater disasters for enterprises. In the face of data leakage during data sharing, some existing solutions in the UK are to provide limited data filtering, but this method cannot avoid data leakage [33]. With frequent data leakages, data sharing transactions without regulatory control will fall into a highly unstable cycle [34]. In addition, the existing researches focuses on the sharing of "information security" through the disciplines of computer science and technology, and lacks the guiding and practical research on the supervision mechanism, process, and mode of large data sharing for security [35]. To reduce the risks of data leakage to user privacy and corporate reputation, effective data supervision is needed to maintain the order of the data market and promote the development of data sharing [36].

2.3. Data Supervision

Data sharing allows data exchange and is more difficult to monitor data leaks than traditional data regulation [37]. The supervision of data leakage can be divided into

nationwide level and enterprise level. Currently, the EU has introduced GDPR (General Data Protection Regulation) regulations to safeguard data security, but it is difficult to ensure that companies always comply with GDPR because regulatory verification of organizations' compliance with GDPR occurs at irregular intervals [38]. China has not yet legislated to provide "absolute" protection for privacy data [39]. In the current situation where the relevant laws are difficult to control data leaks, other supervision methods are needed, such as data providers to retain control over how data is to be used [40]. Newman proposes using distributed regulation to protect data privacy, with regulators relying on individuals and companies to monitor [41]. Sooksatra designs a new game theory algorithm. Users can unilaterally persuade service providers to cooperate in data transactions, to solve the problem of data leakage in the unequal relationship between users and service providers [42]. If an effective regulatory mechanism is provided to realize data sharing safely, it can eliminate the worries of data sharing and improve the enthusiasm of data sharing. Therefore, in view of the current situation of data leakage and lack of supervision in company data sharing, this paper establishes a model of data sharing, disclosure, and supervision. The model is that before data sharing, both parties formulate a supervision mechanism with fines as the main constraint, and supervise each other's corporate disclosure behavior, and use the regulatory mechanism to influence the company's behavior choice and solve the current data sharing, data leakage problem.

3. Data Sharing, Leakage, and Supervision Model

Based on the above analysis, in this section, we will establish a data sharing, leakage, and supervision model between the two companies to solve the problem of frequent data leakage in the process of data sharing, and provide new supervision ideas.

3.1. Problem Description

The two companies establish a data sharing alliance, and the alliance sharing process is shown in Figure 1.

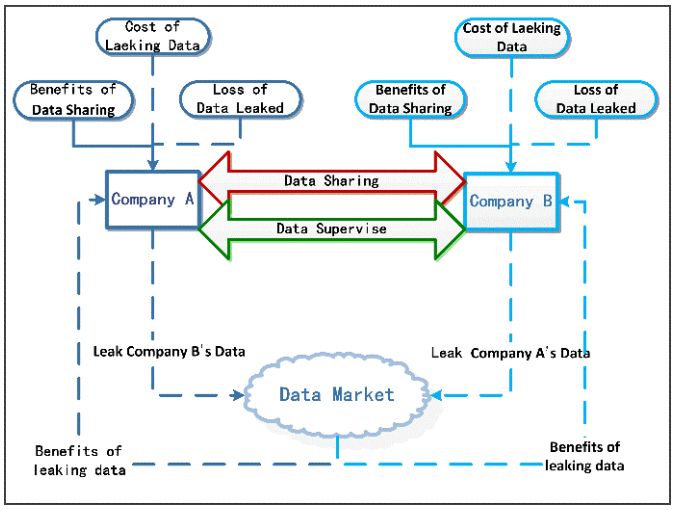

Figure 1. Data sharing, leak, and supervision.

Consider that company A and company B establish data sharing alliance due to business needs and share each other's data and obtain the data sharing utility (u_A, u_B); meanwhile, if company A or company B leak the other party's data to a third party (e.g., network Advertiser) through the data market, the company that leaks the data can obtain additional benefits (v_A, v_B), and the company whose data has been leaked faces a loss (l_A, l_B). In order to protect the rights and interests of alliance members and maintain the stability of data sharing alliance, company A and company B establish data supervision mechanism; in this supervision mechanism, leaking data will incur some leaking cost,

and if the data leakage behavior is found, there will be a fine penalty. The leakage cost is related to the probability of leaking data being detected (φ_A, φ_B) and the penalty (P_A, P_B), and the penalty is all given to the leaked data company as compensation. To establish and analyze the data sharing, leakage, and supervision model, the definition and description of relevant symbols are shown in Table 1.

Table 1. Symbol definition, description, and range.

Symbol	Definition	Range
u	Benefits of data sharing	$u \in (0, +\infty)$
v	Benefits of leaking other company data	$v \in (0, +\infty)$
l	Loss of data leaked	$l \in (0, +\infty)$
q	Data quality	$q \in (0, 1)$
D	Scale of shared data	$D \in (0, +\infty)$
φ	Probability of leak data being discovered	$\varphi \in (0, 1)$
t	Relative technical level between companies	$t_{AB} \in (0, 1), t_{BA} \in (0, 1)$
d	Scale of leaked data	$d_A \in (0, D_A), d_B \in (0, D_B)$,
x, y	Proportion of leaking data	$x \in (0, 1), y \in (0, 1)$,
k	Relevance degree between data Leaked loss and benefits of Data Leaking	$k \in (0, 1)$
ω	Degree of punishment	$\omega \in (0, +\infty)$
P	Fines for companies that leaking data	$P \in (0, +\infty)$

The assumptions of this model are as follows:

(1) Company A and company B establish a data sharing alliance and sign a data sharing agreement for mutual data supervision. To maximize the benefits of the two companies, both companies have the potential to leak data to obtain additional benefits.

(2) The two companies are rational players, and the information between the players is symmetrical. The relevant parameters, strategy space, and payment function are all public information, which is in line with the complete information game.

(3) The strategies of game players are as follows:

$$\text{Company A} : \mathrm{S_A} = \{\mathrm{S_{NA}}, \mathrm{S_{LA}}\} = \{\text{Sharing and No Leaking, Sharing and Leaking}\}$$

where $\mathrm{S_{NA}}$ means that company A selects the sub-strategy "sharing and no leaking data, meanwhile $\mathrm{S_{LA}}$ means that company A selects the sub-strategy "sharing and leaking data."

$$\text{Company B} : \mathrm{S_B} = \{\mathrm{S_{NB}}, \mathrm{S_{LB}}\} = \{\text{Sharing and No Leaking, Sharing and Leaking}\}$$

where $\mathrm{S_{NB}}$ means that company B selects the sub-strategy "sharing and no leaking data, meanwhile $\mathrm{S_{LB}}$ means that company B selects the sub-strategy "sharing and leaking data."

Different behavior choices of companies A and B can form four different strategy combinations, resulting in totally different data sharing benefits and consequences of data leakage. Due to the different technical level and the ability of data leakage screening, the willingness of data sharing and the behavior of data leakage are different between companies. To obtain the Nash equilibrium conditions of different strategy combinations, we will firstly build the data sharing, leakage, and supervision mechanism models in the next section.

3.2. Model Analysis of Data Sharing, Leakage and Supervision Mechanism

On the one hand, companies can gain additional benefits from leaking data, such as leaking shared data to online advertising companies or other stakeholders. On the other hand, the leaked party may cause loss of data assets. To gain more benefits from data sharing alliance, companies A and B have the potential to leak data. Therefore, it is critical to design a reasonable data supervising mechanism to control leak behaviors and maintain the stability of the alliance.

3.2.1. Data Shared Benefit Analysis

In this paper, we only consider the direct benefits of data sharing and do not consider the cross-effect of data association. The utility function of data sharing is determined by the quality and scale of shared data. Let D_A, D_B denote the data sharing scale of company A and B respectively, and q_A, q_B is the quality of shared data, then the data sharing utility, of company A and B is $u_A = D_B q_B$, $u_B = D_A q_A$.

3.2.2. Scale Analysis of Data Leakage

The scale of data leakage will affect the cost of data leakage and then affect the choices of corporate behavior. The proportion of leaked data from the company is x, y. Let d_A, d_B be the scale of company A and company B leaking each other's data, the proportion of company A's leaking data is $x = d_A/D_B$, and the proportion of company B's leaking data is $y = d_B/D_A$.

3.2.3. Benefit and Cost Analysis of Data Leakage

The benefit of leaking data and the loss of leaked data are related to the value of leaked data, if the benefit of company A and company B leaking data is v_A, v_B, and then $v_A = xu_A, v_B = yu_B$; the loss of company data leakage is l_A, l_B, and $l_A = kv_B$, $l_B = kv_A$.

Although the data leakage will bring additional benefits, the leakage data behavior faces the risk of being detected, resulting in the data leakage fine P. The cost of data leakage is represented by the probability of data leakage being detected φ and penalty P; and the probability of data leakage being detected is related to the technical level of both companies; the penalty of data leakage is affected by the scale of leaked data.

3.2.4. Analysis of the Impact of Related Data Technology Levels

According to the IBM data leakage report, the company's cost of leaking data is related to its technical level, such as encryption technology, automation security technology, big data management ability, etc. and its relative technical advantages [43]. According to the agreement, the level of supervision depends on the difference of data technology capability between the two companies. So, the relative technical level t, t_{AB} is the technical level of A company relative to B company, and $t_{AB} > 1$ shows that the technical level of company A is higher than that of company B; meanwhile, t_{BA} is the technical level of A company relative to B company.

As mentioned above, the higher the technical advantage, the lower the cost of data leakage. The relative technical advantage is related to the probability of data leakage detection φ, and is inversely proportional. The company with higher technology level will reduce the probability of being detected and the cost of leakage will be reduced; on the contrary, the leakage cost of the company with lower technical capability will increase. Let φ_A, φ_B be the probability that the company leaks data and $\varphi_A = 1/t_{AB}, \varphi_B = 1/t_{BA}$.

3.2.5. Analysis of Data Supervision Mechanism

To prevent the data leakage behavior, companies A and B use a kind of data supervision mechanism. Once a data leak is discovered, the penalty will be imposed, and all fines will be paid to the leaked company; the fine depends on the level of penalty and the value of the leaked data. Company A and B are fined $P_A = \omega(xu_A)$, $P_B = \omega(yu_B)$ for leaking data, and ω is the degree of punishment. The larger the scale of data leakage, the greater the impact on the leaked data company and the higher the penalty for the leakage, and vice versa.

3.3. Basic Model

Based on the parameter analysis of data sharing, data leakage, and supervision mechanism, the combination payment matrix of company game strategy is shown in Table 2.

Table 2. Penalty payment matrix of data breach.

Company A/B	SN_B	SL_B
SN_A	u_A, u_B	$u_A - l_A + \varphi_B P_B$, $u_B + v_B - \varphi_B P_B$
SL_A	$u_A + v_A - \varphi_A P_A$, $u_B - l_B + \varphi_A P_A$	$u_A + v_A - l_A - \varphi_A P_A + \varphi_B P_B$, $u_B + v_B - l_B + \varphi_A P_A - \varphi_B P_B$

The choice of corporate strategy depends on the return of different strategic combinations. Based on the payment matrix in Table 2 above, the company aims to maximize the benefits of the enterprise, compares the payment functions under different strategies, and obtains four different combinations of strategies. The four equilibrium boundary conditions derived from Table 2 payment matrix are: $\omega = t_{AB} = 1/t_{AB}$, $P_A = xu_A$, $P_B = yu_B$, that is, the two companies have the same technical level. If the parameters satisfy the boundary conditions, the company loses its potential to leak data for it cannot benefit from data leakage. As long as the parameters deviate from the boundary value, corporate behavior choices can be controlled by the penalty level, resulting in different combinations of strategies. Specific parameter ranges and balanced analysis are given in the next section.

4. Model Analysis

In this section, we will analyze the Nash equilibrium of enterprise data sharing, leakage, and supervision models, and then discuss the Nash equilibrium conditions and the parameters for four different pure strategies.

4.1. Equilibrium Analysis of S_1 Strategy

In the first case, $S_1 = \{SN_A, SN_B\}$ becomes the Nash equilibrium strategy, and both companies choose the sub strategy of "sharing and no leaking data" as the optimal strategy. Data sharing alliance members find that leaking data may not be profitable. The S_1 equilibrium condition is:

$$\begin{cases} u_A \geq u_A + v_A - \varphi_A P_A \\ u_B \geq u_B + v_B - \varphi_B P_B \end{cases} \tag{1}$$

At this time, the relationship between supervision fines caused by data leakage and relative technical level should be satisfied:

$$\omega \geq max\left\{t_{AB}, \frac{1}{t_{AB}}\right\} \tag{2}$$

The fine of data leaking supervision should meet the follow conditions:

$$\begin{cases} P_A \geq xD_B q_B t_{AB} \\ P_B \geq yD_A q_A t_{BA} \end{cases} \tag{3}$$

Proposition 1. *In the first case, S_1 becomes the Nash equilibrium strategy. S_1 strategy combination is the optimal sharing strategy of data alliance, and the supervision penalty level condition is $\omega \geq max\{t_{AB}, 1/t_{AB}\}$, otherwise it cannot maintain the optimal sharing strategy.*

To avoid the risk of data leakage, the alliance members expect that the alliance partner will share and not leak its data, that is, S_1 equilibrium. The company's data strategy depends on the cost and benefits of data leakage. If the benefit of data leakage is less than the cost of leakage, the enterprise will choose not to leak data. Conversely, if the leaking data is profitable, the enterprise chooses the leaking behavior. The cost of leaking data depends on both penalty level ω and relative technical level t, so the supervision mechanism can base on the technical level of both parties. Where the fine meet $P_A \geq xD_B q_B t_{AB}$, $P_B \geq yD_A q_A t_{BA}$, it may increase the cost of leaking data and control the behavior of company data leakage.

4.2. Equilibrium Analysis of S_2 and S_3 Strategy

In the second/third case, $S_2 = \{SN_A, SL_B\}$ or $S_3 = \{SL_A, SN_B\}$ becomes the Nash equilibrium strategy, where one company chooses the sub strategy of "sharing and no leaking data," but the other one chooses the sub strategy of "sharing and leaking data." The Nash equilibrium conditions of S_2 and S_3 games are:

$$\begin{cases} u_A - l_A + \varphi_B P_B \geq u_A + v_A - l_A - \varphi_A P_A + \varphi_B P_B \\ u_B + v_B - \varphi_B P_B \geq u_B \end{cases} \tag{4}$$

$$\begin{cases} u_A + v_A - \varphi_A P_A \geq u_A \\ u_B + v_B - l_B + \varphi_A P_A - \varphi_B P_B \geq u_B - l_B + \varphi_A P_A \end{cases} \tag{5}$$

At this time, the relationship between the punishment level of S_2 and S_3 data supervision and the relative technical level should be satisfied, respectively:

$$t_{AB} \leq \omega \leq \frac{1}{t_{AB}} \tag{6}$$

$$\text{Or } \frac{1}{t_{AB}} \leq \omega \leq t_{AB} \tag{7}$$

Data leaking supervision fines should be met:

$$\begin{cases} P_A \geq x D_B q_B t_{AB} \\ P_B \leq y D_A q_A t_{BA} \end{cases} \tag{8}$$

$$\text{Or } \begin{cases} P_A \geq x D_B q_B t_{AB} \\ P_B \leq y D_A q_A t_{BA} \end{cases} \tag{9}$$

If companies A and B achieve S_2 or S_3 Nash equilibrium, their fines should meet $t_{AB} \leq \omega \leq 1/t_{AB}$ or $1/t_{AB} \leq \omega \leq t_{AB}$, from which proposition 2 can be obtained.

Proposition 2. *If the fine is satisfied $t_{AB} \leq \omega \leq 1/t_{AB}$ or $1/t_{AB} \leq \omega \leq t_{AB}$, one of the two companies may leak the other company's data, while the other party does not leak, and the leaking data behavior only occurs in the company with higher data technology level.*

If the penalty level is set, the behavior of company data leakage is determined by the relative technical level. As Figure 2 shows, we can see that the technical advantage of company A increases along the transverse axis, and the technical level of the company A is higher if t_{AB} larger than 1. S_2 only exists if $t_{AB} < 1$. If company B's technical level is higher than company A's, company B may leak data; meanwhile company A does not leak any data; S_3 is similar to S_2. At the same time, if the relative technical level becomes wider, ω needs to be increased to prevent the company with higher technical level from leaking data.

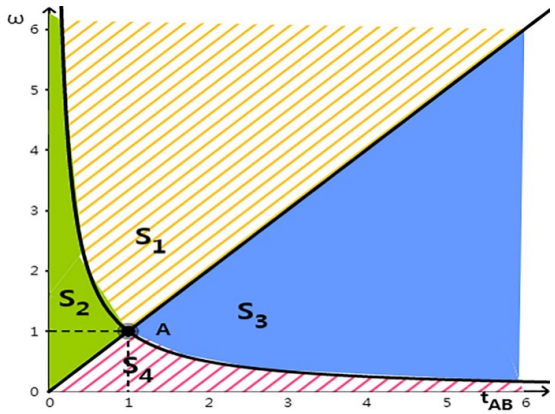

Figure 2. Nash equilibrium distribution under different supervision mechanisms.

4.3. Nash Equilibrium Analysis of S_4 Strategy

$S_4 = \{SL_A, SL_B\}$. Under the Nash equilibrium, companies A and B choose the "share and leak the other party's data" sub-strategy. At this time, companies A and B consider the sub-strategy "sharing and leaking data" as the optimal strategy, but the Nash equilibrium is the worst game equilibrium solution. The S_4 equilibrium condition is:

$$\begin{cases} u_A - l_A + \varphi_B P_B \geq u_A + v_A - l_A - \varphi_A P_A + \varphi_B P_B \\ u_B - l_B + \varphi_A P_A \geq u_B + v_B - l_B + \varphi_A P_A - \varphi_B P_B \end{cases} \tag{10}$$

At this time, the relationship between supervision fines caused by data leakage and the relative technical level should be satisfied:

$$\omega \leq min\left\{t_{AB}, \frac{1}{t_{AB}}\right\} \tag{11}$$

Data leaking supervision fines should be met:

$$\begin{cases} P_A \leq xD_B q_B t_{AB} \\ P_B \leq yD_A q_A t_{BA} \end{cases} \tag{12}$$

If company A and B achieve the S_4 Nash equilibrium, the penalty level for leaking data is $\omega \leq min\{t_{AB}, 1/t_{AB}\}$, and the penalty for data leaking is not larger than the additional benefits of data leaking. Therefore, if the penalty level meets the above conditions and the penalty amount is set low enough, the S_4 Nash equilibrium can occur; that is, companies A and B choose the "sharing and leaking data" sub-strategy.

Proposition 3. *If the penalty level ω of the supervision mechanism is bigger than the equilibrium point 1 (Figure 2), the S_4 equilibrium does not exist; if the penalty level is less than the equilibrium point, the S_1 equilibrium does not exist.*

If there is no data supervision, and $\omega = 0$, the S_4 equilibrium condition means that the companies will leak data for greater benefit. It is also difficult to avoid data leakage if the level of supervision is less than 1. Figure 2 shows that S_1 and S_4 are mutually exclusive and the boundary is point A (1,1). If $\omega < 1$, there will be leakage from both companies, otherwise S_4 will not exist. In this case, it is a mild punishment level, and the supervision is relatively loose. At the same time, the penalty for leaking data is relatively low compared with the benefit from leaking data, so both companies choose to leak each other's data.

4.4. Nash Game Equilibrium Distribution under Different Supervision Mechanisms

The choice of leaking behavior of companies A and B is determined by the level of punishment ω and the relative technical level t of companies A and B together. Therefore, according to the parameter conditions obtained in this section, the relationship between the level of punishment ω and the relative technical level t is drawn as shown in Figure 2.

Propositions 1 to 3 indicate that corporate behaviors are determined by ω and t together. The wider the gap of data technology level, the looser the supervision, the greater the probability of data leak events; if the supervision mechanism is set with $\omega = 0$, the entire distribution will fall within S_4, data leakage is unavoidable; if the supervision mechanism is set with $\omega < 1$, data leakage is certain to occur. If supervision penalties and leakage costs are lower, companies will tend to leak data and choose S_4 strategy. Therefore, the data sharing supervision mechanism should set an appropriate punishment level to prevent the data leakage behavior and ensure the data security of the alliance members.

5. Simulation Analysis

The model of data sharing, leakage, and supervision between the two companies is established, and the supervision mechanism of data sharing alliance is set up. The results of the model are analyzed, the relationship between different strategy distribution and

parameters is obtained, and three propositions are given. In this section, simulation will be used to further discuss the influence of ω and t parameter on the behavior of participants. We designed two different data supervision strategies, mild and severe penalty, to analyze the impact of data supervision mechanism on game decision-making of data sharing alliance. The specific values of each parameter in the simulation are shown in Table 3.

Table 3. Simulation parameters of data sharing alliance.

Scale of shared data	$D_A = D_B = 1000$
Data quality	$q_A = q_B = 0.8$
Proportion of leaking data	$x = y = 1$
Degree of punishment	severe penalty $\omega = 2$, mild penalty $\omega = 0.5$
Relevance degree between data Leaked loss and benefits of Data Leaking	$k = 0.5$

5.1. Equilibrium Strategy Analysis under Different Data Supervision Mechanisms

We consider two kinds of penalty levels and analyze the Nash equilibrium benefits of both companies as follows:

5.1.1. Supervision Mechanism for Mild Penalties

Under the mild penalty level ($\omega < 1$), S_1 does not exist, and the possible equilibrium is S_2, S_3, S_4. The analysis results are as follows:

S_2: $0 < t_{AB} \leq 0.5, \pi_A = u_A - l_A + \varphi_B P_B, \pi_B = u_B + v_B - \varphi_B P_B$;
S_3: $t_{AB} \geq 2, \pi_A = u_A + v_A - \varphi_A P_A, \pi_B = u_B - l_B + \varphi_A P_A$;
S_4: $0.5 < t_{AB} < 2, \pi_A = u_A + v_A - l_A + \varphi_B P_B - \varphi_A P_A, \pi_B = u_B + v_B - l_B + \varphi_A P_A - \varphi_B P_B$.

In the mild penalty, the S_1 Nash equilibrium does not exist and cannot control the behavior of companies A and B leaking data, which verifies that in Proposition 3, if the penalty level is less than the equilibrium point, the S_1 equilibrium does not exist. It can be seen from Table 3 that under the mild punishment mechanism, the punishment coefficient is $\omega = 0.5$. It can be seen from the distribution of horizontal axis t and three kinds of equilibrium that when the value of t falls within the interval $[0.5, 2]$, ω is difficult to meet the condition $t_{AB} \leq \omega \leq 1/t_{AB}$ or $1/t_{AB} \leq \omega \leq t_{AB}$, and it is S_4 equilibrium. In other cases, when ω satisfies the above condition, it is the equilibrium that one party discloses data and the other party does not. This further verifies Proposition 2 proposed above.

In the S_4 equilibrium, as shown in Figure 3, the two companies earned the same utility and had the same technical level at point A. From Figure 3, we can see that under the mild penalty mechanism, the one with higher technical level will leak data, and the higher technical level company's benefit of data sharing will be greater than that of the weak one. Meanwhile, on the left side of point B, if company A leaks data, the utility from data sharing of company B is higher than that of company A, which does not leak any data; the point C is the same as the point B. Therefore, under the control of the mild supervision mechanism, it is not possible to change the leakage behavior of the technology-dominant party, and there is also the default leakage of each other's data.

5.1.2. Supervision Mechanism for Severe Penalties

Under the severe penalty mechanism ($\omega > 1$), S_4 does not exist, and the possible equilibrium is S_1, S_2, S_3. The analysis results are as follows:

S_1: $0.5 < t_{AB} < 2, \pi_A = u_A, \pi_B = u_B$;
S_2: $0 < t_{AB} \leq 0.5, \pi_A = u_A - l_A + \varphi_B P_B, \pi_B = u_B + v_B - \varphi_B P_B$;
S_3: $t_{AB} \geq 2, \pi_A = u_A + v_A - \varphi_A P_A, \pi_B = u_B - l_B + \varphi_A P_A$.

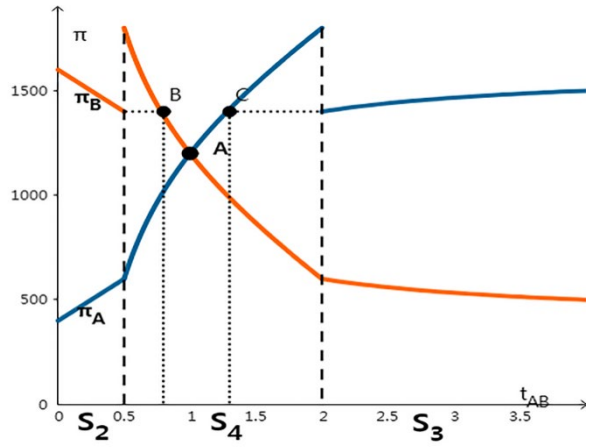

Figure 3. Three Kinds of Nash equilibrium under Mild Penalty.

When the supervision mechanism is severe punishment mechanism, it can be seen from Table 3 that $\omega = 2$. In Figure 4, S_4 equilibrium does not exist at this time, which verifies that in Proposition 3 $\omega > 1$, S_4 equilibrium does not exist; in addition, according to the horizontal axis distribution, S_1 equilibrium only exists when the relative technical level t_{AB} is between $[0.5, 2]$, meets the condition of $\omega \geq max\{t_{AB}, 1/t_{AB}\}$, and there is no data leakage behavior, which is in line with the conclusion of proposition 1. In other cases, when ω satisfies $t_{AB} \leq \omega \leq 1/t_{AB}$ or $1/t_{AB} \leq \omega \leq t_{AB}$, it is the equilibrium that one party discloses data and the other party does not, and the leaking data behavior only occurs in the company with higher data technology level. This further verifies Proposition 2, proposed above.

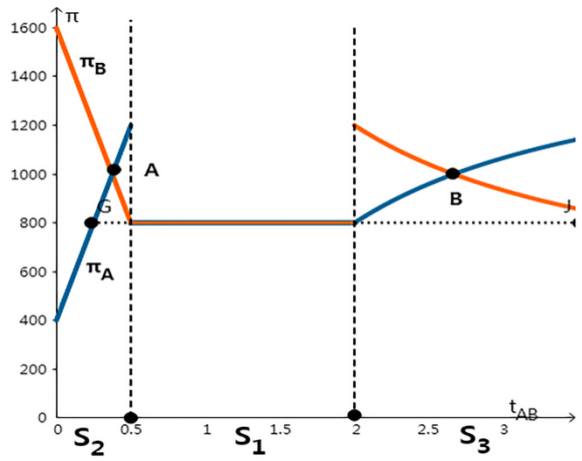

Figure 4. Three Kinds of Nash equilibrium under Severe Penalty.

When severe penalties are imposed, it is not possible for the two companies to leak data at the same time. The leaking party depends on the technical level. In the S_2/S_3 Nash equilibrium, shown in Figure 4, the two companies' earnings functions intersect at A and B. If the relative technical level of the two companies is in the S_2 Nash equilibrium and on the right side of G point, when company B leaks data, Company A can get higher earnings than the S_1 equilibrium even though Company A does not leak data; the same is also true for the S_3 Nash equilibrium. Therefore, under the control of severe supervision, even if one party with higher technical level may leak data, the weaker party will not be in a completely weak position; when the yield is higher than the S_1 equilibrium, there is even the possibility of the default party leaking data for a higher benefit.

Based on the above analysis, the simulation results under two different punishment levels verify the three propositions mentioned above, and also prove that the supervision

model and supervision mechanism proposed in this paper can influence the behavior of data sharing alliance participants. From the comparison of the two punishment levels, it can be seen that the greater the punishment level, the lower the risk of data leakage; meanwhile, in the same equilibrium, the benefit of the party who leaks data increases with the decrease of punishment level, while that of the party whose data is leaked decreases. Therefore, strict supervision can better protect the rights and interests of the leaked party and minimize the loss of data leakage.

5.2. Extension Discussion of "SF Express Company: Data War"

5.2.1. SF Express and Cainao Data Sharing Case Background

In this part of the study, we introduce the Harvard Business School case—"SF Express Company: Data War" to discuss the application of the model in practice and analyze how to use data sharing, leakage, supervision model to solve data leakage problems in data sharing and prevent data monopoly. SF Express Group Co. Ltd. (SF Express) was a leading express delivery and logistics solutions provider in China. In May 2017, SF Express became involved in a dispute with the logistics-tracking platform Cainiao Network Technology (Cainiao), which was controlled by Alibaba Group Holding Limited. The dispute, which involved an SF Express affiliated smart package locker company that declined a data-sharing request from Cainiao for protecting privacy data, caused SF Express and Cainiao to sever their ties over proprietary data and cyber security. This severance caused significant disruption to China's e-commerce sector. After regulatory intervention, both parties agreed to resume sharing data for the time being and had to negotiate a resolution to their data dispute [24].

Based on the simulation analysis results and Harvard Business School case "SF Express Company: Data War," we get the following management implications.

5.2.2. If There Is No Data Supervision on Company Sharing, It Is Difficult to Avoid Data Leakage

When the two companies share data, if they do not adopt supervision measures, data leakage will be difficult to avoid, which is also the key reason for the data dispute between SF Express and Cainiao platform. To obtain more data, enterprises need to share their data. However, without supervision, enterprises may lose more than their profits gain, which is also the factor of "information island" and "data monopoly." To avoid the recurrence of SF Express and Cainiao events, it is necessary to design a data supervision mechanism before data sharing, to prevent the company's data leakage behavior and ensure a good data market environment.

5.2.3. According to the Data Sharing Needs, the Company Can Choose the Punishment Level and Supervise the Data Sharing Process

SF Express and Cainiao are leading enterprises in China. Once data leakage occurs, the operation of China's E-commerce transactions will be affected. The data war is also due to the fear that the other party will leak data, which will cause an unpredictable impact. Therefore, SF Express and Cainiao companies need to establish an effective data sharing alliance and adopt a severe punishment supervision mechanism to protect their data.

5.2.4. Under the Mutual Supervision Mechanism of Data Sharing, the Company Allows Members of the Sharing Alliance to Leak Data

The technical level of SF Express and Cainiao platforms is similar, and only the severe punishment can avoid data leakage. However, if the two companies with different technical levels share data and the leakage data has no serious impact on the company, even if the punishment is increased, there is also the possibility of unilateral leakage of S_2 and S_3 data. As a result, both parties may choose to control the level of penalties and default to the other party's data disclosure, rather than just consider banning it entirely.

6. Conclusions

Aiming at the problems of data sharing, leakage, and supervision, our paper established a model of data sharing, leakage, and supervision based on game theory, and discussed the effective strategies of data sharing, leakage, and data supervision. This paper makes a simulation analysis of the model, discusses the influence of different supervision levels on the behavior of participants, and discusses the influence of data supervision mechanism on the game decision-making of Data Sharing Alliance Based on the data dispute of SF express company. The main conclusions are as follows:

6.1. S_1 Strategy Equilibrium Is the Best Sharing Strategy for Data Alliance

Data sharing alliance members all have the motivation to leak data. If the data supervision penalty level condition does not meet $\omega \geq max\{t_{AB}, 1/t_{AB}\}$, data sharing alliance will deviate from the S_1 strategy equilibrium, resulting in the risk of customer data leakage.

6.2. S_2 or S_3 Nash Equilibrium Needs to Meet $t_{AB} \leq \omega \leq 1/t_{AB}$ or $1/t_{AB} \leq \omega \leq t_{AB}$

Due to the unequal technical level of the members of the data sharing alliance, the technical weak party is forced to accept the sub-strategy of "sharing and not leaking data." In fact, this is an unfair data sharing alliance. When the weak party improves its own technical level, the data sharing alliance will fail.

6.3. S_4 Nash Equilibrium Needs to Meet $\omega \leq min\{t_{AB}, 1/t_{AB}\}$, Company A and B Choose the "Sharing and Leaking Data" Sub-Strategy

At this time, due to the unreasonable design of the regulatory mechanism, if the amount of data leakage penalty is set low enough, companies A and B will choose to leak customer data, which infringes on the interests of customer data privacy.

The results of simulation analysis show that the company sharing and leaking behavior is affected by both the level of data supervision fines and the relative technical level. The data supervision mechanism proposed in this paper can effectively control the company data leaking behavior. The data supervision strategy with severe penalties can especially make up for the technical weakness of the company and achieve the stability of the data sharing alliance.

Based on the research conclusions above, we put forward some policy suggestions for data sharing, leakage, and supervision: (1) the government should encourage enterprises to establish data sharing alliances, improve relevant supervisions and policies, and increase support for enterprise data sharing. (2) Because a large part of the data sharing between companies comes from individual users, if the data is leaked, it will threaten the privacy and security of users, which is not conducive to the stable operation of the data market; in addition, there is the situation that members of data sharing alliance allow each other to leak data. Therefore, in addition to the mutual supervision between companies, the government should also supervise the data leakage behaviors. (3) When the government supervises the data sharing alliance, it should pay attention to the punishment level of the supervision mechanism of both sides and the data leakage behavior of high-tech companies to ensure the data market.

6.4. Further Research

This paper focuses on the behavior of data leakage of participants in the process of data sharing, and provides a regulatory approach to solve such data leakage. However, the research of this paper still has some limitations. First of all, on the technical level, the disadvantage of this article is to use the theory of complete information game to build a supervision model, but considering that it is difficult to know all the information of each other in the actual company data sharing. In the next study, we will consider the data sharing, leakage, and supervision in non-complete information situations. In the future research direction, the model proposed in this paper requires both parties to supervise

each other, which is also the reason for the imbalance of supervision in the conclusion. We also find that most enterprises' data sharing is based on the third-party data platform. Therefore, we can consider that further study on data supervision mechanism should be based on the third-party data platform in the future research.

Author Contributions: H.Y. and X.H. have contributed equally and substantially to the work reported, which was based on X.H.'s Master thesis. H.Y. has acted as the supervisor of the original work and has contributed to writing, reviewing, and editing the present manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Social Science Fund of China [No. 20BGL107].

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This work was supported by the National Social Science Fund of China [No. 20BGL107].

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Gruschka, N.; Mavroeidis, V.; Vishi, K.; Jensen, M. Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018; pp. 5027–5033.
2. Kim, J.H. Overview of disciplinary data sharing practices and promotion of open data in science. *Sci. Ed.* **2019**, *6*, 3–9. [CrossRef]
3. Zuiderwijk, A.; Janssen, M.; Susha, I. Improving the speed and ease of open data use through metadata, interaction mechanisms, and quality indicators. *J. Organ. Comp. Electron. Commer* **2016**, *26*, 116–146. [CrossRef]
4. Zhu, Q.; Krikke, H.; Caniels, M.C. Supply chain integration: Value creation through management inter-organizational learning. *Int. J. Oper. Prod. Manag.* **2018**, *38*, 211–229. [CrossRef]
5. Simeng, W.; Jing, R.; Yunfei, S. Study on the impact mechanism of alliance conventions on the dual innovation capability of enterprises. *Manage* **2019**, *32*, 19–32.
6. Van Der Klerj, R.; Wijn, R.; Hof, T. An application and empirical test of the Capability Opportunity Motivation-Behaviour model to data leakage prevention in financial organizations. *Comput. Secur.* **2020**, *97*, 101970. [CrossRef]
7. Goode, S.; Hoehle, H.; Venkatesh, V.; Brown, S.A. User compensation as a data breach recovery action: An investigation of the Sony PlayStation network breach. *MIS Q.* **2017**, *41*, 703–727. [CrossRef]
8. Chen, H.S.; Jai, T.M. Trust fall: Data breach perceptions from loyalty and non-loyalty customers. *Serv. Ind. J.* **2019**, *4*, 1–17. [CrossRef]
9. Cheng, L.; Liu, F.; Yao, D. Enterprise data breach: Causes, challenges, prevention, and future directions: Enterprise data breach. *Wiley Interdiscip. Rev. Data Min. Knowl. Discov.* **2017**, *7*, e1211. [CrossRef]
10. Srinivasan, S.; Pitcher, Q. Harvard Business Review. Data Breach at Equifax. 2018. Available online: https://store.hbr.org/product/data-breach-at-equifax/118031?sku=118031-PDF-ENG (accessed on 21 October 2017).
11. Cuinan, M.J.; Williams, C.C. How ethics can enhance organizational privacy: Lessons from the Choice Point and TJX data breaches. *Mis Q.* **2009**, *33*, 673–687.
12. Goel, S.; Shawky, H.A. Management. Estimating the market impact of security breach announcements on firm values. *Inf. Manag.* **2009**, *46*, 404–410. [CrossRef]
13. Gerlach, J.P.; Eling, N.; Wessels, N.; Buxmann, P. Flamingos on a slackline: Companies' challenges of balancing the competing demands of handling customer information and privacy. *Inf. Syst. J.* **2019**, *29*, 548–575. [CrossRef]
14. Zafar, H.K.; Ko, M.; Osei-Bryson, K.M. Financial Impact of Information Security Breaches on Breached Firms and their Non-Breached Competitors. *Inf. Resour. Manag. J.* **2012**, *25*, 21–37. [CrossRef]
15. Sen, R.; Borle, S. Estimating the Contextual Risk of Data Breach: An Empirical Approach. *J. Manag. Inform. Syst.* **2015**, *32*, 314–341. [CrossRef]
16. Johnson, M.E. Information Risk of Inadvertent Disclosure: An Analysis of File-Sharing Risk in the Financial Supply Chain. *J. Manag. Inform. Syst.* **2008**, *25*, 97–124. [CrossRef]
17. Bromiley, P.; McShane, M.; Nair, A.; Rustambekov, E. Enterprise Risk Management: Review, Critique, and Research Directions. *Long Range Plan.* **2015**, *48*, 265–276. [CrossRef]
18. Yeung, A.K.W.; Hall, G.B. Spatial Data Sharing, Data Warehousing and Database Federation. Available online: https://www.buecher.de/shop/geoinformationssystem/spatial-database-systems-ebook-pdf/ebook-pdf/products_products/detail/prod_id/37353573/ (accessed on 23 May 2007).

19. Shin, S.; Kim, J.Y.; Le, M.; Shin, Y.H.; Kim, M.K. Implementation of Research Data Platform: In the Perspective of Data Transfer. In Proceedings of the 2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN), Zagreb, Croatia, 2–5 July 2019; pp. 735–737.
20. Lu, Y.; Huang, X.; Li, D.; Zhang, Y. Collaborative Graph-Based Mechanism for Distributed Big Data Leakage Prevention. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, UAE, 9–13 December 2018; pp. 1–7.
21. Xu, H.; He, Q.; Li, X.; Jiang, B.; Qin, K. BDSS-FA: A Blockchain-Based Data Security Sharing Platform with Fine-Grained Access Control. *IEEE Access* **2020**, *8*, 87552–87561. [CrossRef]
22. Saatc, C.; Gunal, E.S. Preserving Privacy in Personal Data Processing. In Proceedings of the 2019 1st International Informatics and Software Engineering Conference (UBMYK), Ankara, Turkey, 6–7 November 2019; pp. 1–4.
23. Karafili, E.; Lupu, E.C.; Cullen, A.; Williams, B.; Arunkumar, S.; Calo, S. Improving data sharing in data rich environments. In Proceedings of the 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA, 11–14 December 2017; pp. 2998–3005.
24. Harvard Business Review: SF Express: Data wars. Ivey Publishing. 2018. Available online: https://store.hbr.org/product/sf-express-data-wars/w18544?sku=W18544-HCB-ENG# (accessed on 24 September 2018).
25. Katz, G.; Elovici, Y.; Shapira, B. CoBAn: A context-based model for data breach prevention. *Inf. Sci.* **2014**, *262*, 137–158. [CrossRef]
26. Hauer, B. Data and Information Leakage Prevention within the Scope of Information Security. *IEEE Access* **2015**, *3*, 2554–2565. [CrossRef]
27. Guevara, C.; Santos, M.; Lopez, V. Data breach detection algorithm based on task sequences and probabilities. *IEEE Trans. Knowl. Data Eng.* **2011**, *23*, 51–63.
28. Al-Zaben, N.; Onik, M.M.H.; Yang, J.; Lee, N.; Kim, C. General Data Protection Regulation Complied Blockchain Architecture for Personally Identifiable Information Management. In Proceedings of the 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE), Southend, UK, 16–17 August 2018; pp. 77–82.
29. Gwebu, K.L.; Jing, W.; Li, W. The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management. *J. Manage. Inform. Syst.* **2018**, *35*, 683–714. [CrossRef]
30. Ghouse, M.; Nene, M.J.; VembuSelvi, C. Data Leakage Prevention for Data in Transit using Artificial Intelligence and Encryption Techniques. In Proceedings of the 2019 International Conference on Advances in Computing, Communication and Control (ICAC3), Mumbai, India, 20–21 December 2019; pp. 1–6.
31. Yue, L.; Junqin, H.; Shengzhi, Q.; Ruijin, W. Big Data Model of Security Sharing Based on Blockchain. In Proceedings of the 2017 3rd International Conference on Big Data Computing and Communications (BIGCOM), Chengdu, China, 10–11 August 2017; pp. 117–121.
32. Shen, J.; Zhou, T.; He, D.; Zhang, Y.; Sun, X.; Xiang, Y. Block Design-Based Key Agreement for Group Data Sharing in Cloud Computing. *IEEE Trans. Dependable Secur. Comput.* **2019**, *16*, 996–1010. [CrossRef]
33. Nicholson, J.; Tasker, I. Data Exchange: Privacy by design for data sharing in education. In Proceedings of the 2017 International Conference on the Frontiers and Advances in Data Science (FADS), Xi'an, China, 23–25 October 2017; pp. 92–97.
34. Acquisti, A.; Brandimarte, L.; Loewenstein, G. Privacy and human behavior in the age of information. *Science* **2015**, *347*, 509–514. [CrossRef] [PubMed]
35. Ouyang, Q.; Chao, W.U. Study on influencing factors of safety big data sharing and its model construction. *J. Saf. Sci. Technol.* **2017**, *13*, 27–32.
36. Zhen, J.; Xie, Z.; Dong, K. Information security pressure and employee violation willingness: Regulated intermediary effect. *Manage* **2018**, *31*, 01–102.
37. Dong, X.; Li, R.; He, H. Secure sensitive data sharing on a large data platform. *Tsinghua Sci. Technol.* **2015**, *20*, 72–80. [CrossRef]
38. Truong, N.B.; Sun, K.; Lee, G.M.; Guo, Y. GDPR-Compliant Personal Data Management: A Blockchain-Based Solution. *IEEE Trans. Inf. Forensic Secur* **2020**, *15*, 1746–1761. [CrossRef]
39. Fengmei, Y.; Anying, W.; Jun, W. Research on E-commerce credit supervision mechanism under C2B2C mode based on game theory. *Syst. Eng. Theory Pract.* **2017**, *37*, 2102–2110.
40. Susha, I.; Janssen, M.; Verhulst, S.; Pardo, T. Data collaboratives: How to create value from data for public problem solving? In Proceedings of the 18th Annual International Conference on Digital Government Research, Staten Island, NY, USA, June 2017; pp. 604–606.
41. Newman, A.L. What the "right to be forgotten" means for privacy in a digital age. *Science* **2015**, *347*, 507–508. [CrossRef]
42. Sooksatra, K.; Li, W.; Mei, B.; Alrawais, A.; Wang, S.; Yu, J. Solving data trading dilemma with asymmetric incomplete information using zero-determinant strategy. Proceedings of International Conference on Wireless Algorithms, Systems, and Applications, Tianjin, China, 20–22 June, 2018; Springer: Cham, Switzerland, 2018; pp. 425–437.
43. DeBeck, C. 3 Biggest Factors in Data Breach Costs and How to Reduce Them. September 25; Security Intelligence. Available online: https://securityintelligence.com/posts/data-breach-three-biggest-factors-in-cost/ (accessed on 25 September 2020).