Joint Pricing and Security Investment in Cloud Security Service Market With User Interdependency

Shaohan Feng, *Student Member, IEEE*, Zehui Xiong, *Student Member, IEEE*, Dusit Niyato, *Fellow, IEEE*, Ping Wang, *Senior Member, IEEE*, Shaun Shuxun Wang, and Sherman Xuemin Shen, *Fellow, IEEE*

Abstract—After several decades of development on cyber security techniques, one clear conclusion can be drawn: no cyber security solution can completely remove the risks faced by the users. In this regard, cyber-insurance has been introduced as a means to enable the users to alleviate the damage from the cyber threats by transferring the cyber risks to an insurer. In this article, we study a cloud security service market, which is composed of cloud users and cloud security service vendors (CSSVs). The CSSVs work as the insurers for selling the cloud security plan, which is consisted of cloud security service and cloud-insurance. The users in the cloud platform can purchase the cloud security plan from the CSSVs to secure their cloud service. If the cloud service is attacked and loss happens, the users will receive the claim from the CSSVs. To lower the successful attack probability, the CSSV has an incentive to invest in improving its cloud security service. Specifically, we model and study the cloud security service market in the framework of a two-stage Stackelberg game. On the upper stage, the CSSVs lead to decide on their own strategies, i.e., the price of the cloud security plan and the security investment to improve their offered cloud security service. On the lower stage, the users follow to decide on the purchase of the cloud security plan according to the price of the cloud security plan and the perceived cyber breach probability of the cloud security service. We analytically verify that the Stackelberg equilibrium exists and is unique. Extensive simulations have been conducted to evaluate the performance of the Stackelberg game. The performance evaluation shows some insightful results. For example, when the users have strong interdependency, the profits of the CSSVs become lower.

Index Terms—Security interdependency, security investment, cloud-insurance, cyber breach, and Stackelberg game

1 Introduction

Since the cloud services offer many benefits, e.g., improving efficiency and resource utilization, it has gained widespread use such as sensory data processing in vehicular networks [1] and storage services for overcoming the storage constraints of the mobile devices. However, like everything else of value operating online, cyber attacks in cloud services, e.g., unauthorized access and availability risks, are inevitable [2]. To address such security problems, many cloud security service vendors (CSSVs), e.g., IBM security [3] and Oracle [4], are providing security service to secure cloud for the users. Nevertheless, even though the cyber space in cloud is much more robust than before due to the significant improvements on cyber security techniques, e.g., cryptographic methods [5], completely securing the cyber space still remains as an open research field [6], [7]. Even worse, cyber attacks on organizations across all sectors remain rampant. The financial losses due to the cyber risks were estimated by McAfee to be between USD 300 billion and USD 1 trillion in 2014 [8]. There were 873 recorded breaches in the US with over 29 million records exposed for November 2016, indicated by the Identity Theft Resource Center's 2016 data breach category summary [9].

In this regard, an economic tool, i.e., cyber-insurance, has been introduced to enable effective cyber risk management [10], [11], [12]. Cloud-insurance, which is one of the cyber-insurance products, is a risk management technique via transferring the cyber risks faced by users to an insurance company with a fee, i.e., premium, in return [13]. Similar to the conventional insurance products, cloud-insurance can align the economic incentives of different parties. For example, the CSSVs can be regarded as cloud-insurers selling cloud security plan products consisted of cloud security service and cloud-insurance. This setting is well

- *S. Feng, Z. Xiong, and D. Niyato are with the School of Computer Science and Engineering, Nanyang Technological University, Singapore 639798. E-mail: {feng0089, ZXIONG002}@e.ntu.edu.sg, dniyato@ntu.edu.sg.*
- *P. Wang is with the Department of Electrical Engineering and Computer Science, Lassonde School of Engineering, York University, Toronto, ON M3J 1P3, Canada. E-mail: pingw@yorku.ca.*
- *S. Wang is with the Nanyang Business School, Nanyang Technological University, Singapore 639798. E-mail: wangsx@sustech.edu.cn.*
- *S. Shen is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada. E-mail: sshen@uwaterloo.ca.*

Manuscript received 2 Nov. 2019; revised 9 Apr. 2020; accepted 16 May 2020. Date of publication 21 May 2020; date of current version 15 June 2022. (Corresponding author: Shaohan Feng.) Recommended for acceptance by J. Liu. Digital Object Identifier no. 10.1109/TSC.2020.2996382

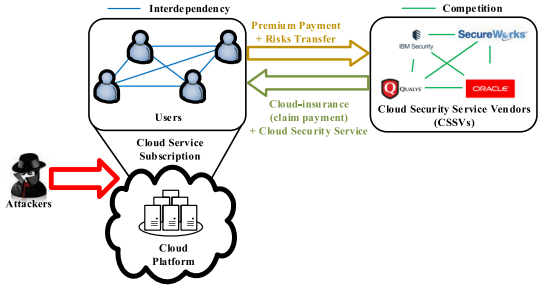


Fig. 1. System model for the cloud security service market.

adopted in the literature such as in [10]. In this way, the CSSVs can improve their profits by appropriately pricing cloud security plan and investing in improving their cloud security services. For the cloud users, they can buy the cloud security plan and use the cloud security service to secure their cloud service. Along with the cloud security service contained in the cloud security plan, the cloud-insurance can help the user to transfer their cyber risks to a third-party company, i.e., CSSV. For the security service consumption, the users are interdependent [10], [14], which will affect the decision-making of the CSSV and further the corresponding profit.

In this paper, we model and study a cloud security service market. As shown in Fig. 1, the CSSVs compete for selling substitutable security services, e.g., intrusion detection and virus scanning, to the users. The users who have the incentive to buy the security service are usually businesses due to their strict requirement of high-level service security. These security services protect the users' access to the cloud platform. For example, Oracle and IBM security offer substitutable cloud security services, e.g., Oracle CASB Cloud Service [4] and IBM Trusteer [3], respectively, to protect the cloud access. Similar to travel insurance in airline industry, the CSSVs can offer cloud-insurance to these security services and guarantee that the user will receive a financial compensation, i.e., claim, once a cyber attack, e.g., data loss, happens. The offer of cloud-insurance can ensure the competitiveness of the CSSVs in the cloud security service market and improves the users' confidence of using the cloud security service even when the attacks happen. Moreover, motivated by the desire to lower the probability of paying the claim, the CSSV has an incentive to invest in improving its own security service in order to reduce the cyber breach probability. As a representative example, IBM security can invest in IBM Trusteer to fight an identity fraud attack with a solution infused with layers of cognitive fraud detection and analytics. Otherwise, IBM security has a high probability of paying claim to the users. As such, if the users are attacked upon their access to the cloud platform, the users are less affected which helps the CSSV pay less claim accordingly. The cloud security service together with the cloud-insurance is named as "cloud security plan"[1]. This is well consistent with the policy of the real-world cyber insurer that not only the loss coverage service but also the vulnerability management programs are included in the products offered by the cyber-insurers, e.g., CyberEdge offered by AIG [15].

We consider particularly the interaction between the CSSVs and users as illustrated in Fig. 1. We propose a two-stage multi-leader-multi-follower game model based on the Stackelberg game framework. On the upper stage, the leaders, i.e., the CSSVs, strategize the price that they charge the users for their cloud security plan and the investment for improving their offered cloud security service. On the lower stage, the followers, i.e., the users, decide on the fraction of their money to spend on these cloud security plans. The major contributions of this paper are summarized as follows:

1) We investigate a joint pricing and security investment problem in the cloud security service market. Therein, we have proposed a two-stage game to model and study the interaction between the CSSVs and the users and the interplay among the users as well as the competition between the CSSVs.
2) We incorporate the security interdependency among the users, which is captured by an interdependency matrix. As such, the enhancement in the security level due to the interdependency among the users can be accordingly studied. Moreover, in the proposed model, we incorporate the relationship between the cyber breach probability and the CSSVs' security investments, where the effort that the CSSVs make to improve their offered cloud security service is modeled.
3) We evaluate our proposed model by conducting extensive simulation. The equilibrium strategies are obtained at different levels of security interdependency. Additionally, we investigate the performances under different number of threats and probabilities of breach.

The rest of the paper is organized as follows. Section 2 presents the related work, where the research gap in the literature has been highlighted. Section 3 describes the system model and Stackelberg game formulation. Section 4 provides the mathematical analysis of the existence and uniqueness of the Stackelberg equilibrium. Section 5 presents the numerical performance evaluation with some insightful results. Finally, Section 6 concludes the paper.

2 Related Works

Cyber-insurance is primarily concerned with the problem of risk transfer, where the cost from the risks is transferred to the insurers. An important aspect of risk transfer in cyber-insurance is the specification of the premium. The research in this area is mainly divided into independent and interdependent security [16]. Therein, the topic of interdependent security has gained a lot of attention from research communities due to the fact that the risks faced by any user also depend on those of all other users in an interdependent network [17]. The interdependent users face the possibility of being attacked either directly by attackers or indirectly from their malicious neighbors [18]. In this regard, the authors in [10] includes the network effect, i.e., interdependency, on security to measure the improvements in individual security of the users which are connected to the users investing in cyber-insurance. Thus, apart from investing in the security tools, e.g., firewalls, network intrusion

1. Note that the market under our consideration focuses on only the cloud security plan, which excludes the cloud service. This means that all the users in the market are subscribing to the cloud platform and hence cloud users.

detection tools, and incoming traffic monitoring, the users may also consider purchasing insurance to alleviate their financial losses in case they fall victim to successful attacks [19]. As such, on the premise of ensuring the optimal network robustness, the users can efficiently manage their risks through cyber-insurance.

In addition to the interdependent security, discriminative pricing of security products is an alternative for the users interacting via a network. Given a set of prices, a network game modeling the interaction of users has been developed in the recent works including [14], [20]. A key modeling assumption in [14], [20] is that the utility function of a user has a linear-quadratic functional form. The authors in [20] are the first to model a connection between Bonacich centrality and Nash equilibrium outcomes in a single stage game with local utility complementarities. However, it is necessary to model the pricing of security products with a multi-stage game, i.e., Stackelberg game, by considering the fact that there are other types of players, e.g., security vendors and insurers. Accordingly, the authors in [14] proposed a two-stage discriminative pricing game to investigate the interplay between the security vendors and the network users. The network effect, i.e., interdependency among the end-users, and discriminative pricing in a security service market were jointly considered. Moreover, the Internet service provider acts as a cyber-insurance agency and forms a symbiotic relationship with the security vendors [14].

To date, there have been several cyber-insurance products available in the market. For example, CyberEdge from AIG not only provides the loss coverage approaches but also helps the insured organization develop effective cyber risk management programs [15]. Therein, the cyber risk management programs include internet facing system examination and cyber security maturity assessment. A cyber-insurance product named "Cyber Enterprise Risk Management (ERM) Insurance" is provided by Chubb [21]. The ERM insurance mainly focuses on covering the business losses due to the cyber failures or attacks. Both loss coverage and reputation safeguard service are included in Beazley Breach Response (BBR) service [22].

Cyber-insurance introduces a number of unique issues compared to classical insurance. Information asymmetry is the situation where companies are reluctant to share full details of their security provisioning with insurers [23]. For example, the companies may act in a more insecure manner by investing in less security after the acquisition of insurance because they now know that the insurer will bear some of the negative consequences. Furthermore, the frequency of breaches is difficult to be predicted [24]. Also, security systems are often interdependent which makes it difficult to assess the system vulnerability [25]. Moreover, unlike other fields of insurance, it is even more challenging to determine when an attack has actually taken place, since many are lengthy and leave liability unclear [26]. For the sake of this problem, in this paper, we make assumptions that the cyber breach probability is associated with the cyber security spending [27].

We consider the security service vendors as the insurers, which is similar to that in [10], [14]. Particularly, the security service vendors sell security plans consisted of security service and insurance. The security service vendors will invest in improving its security service to reduce the cyber breach probability and accordingly decrease its claim payment [28]. Therefore, to improve the payoff, it's necessary to establish the quantitative relation between the security service vendors' investment and the cyber breach probability of its security service.

In [29], the authors presented an economic model to analyze the effect of information security investment in addressing the vulnerability of an organization's information and communication system. They considered some classes of cyber breach probability functions in the analysis. Additionally, a benchmark proportional hazard model was proposed for quantifying the effect of cyber security spending on the vulnerability by using the concept of hazard rate [27]. For any information and communication system, the vulnerability depends on the size of cyber security spending. This means that the increase in security spending will correspondingly reduce the vulnerability.

To the best of our knowledge, none of the works in the literature jointly study the security investment, pricing, and interdependency among users, which play important roles in a security service market. Thus, this is the main contribution of this paper.

3 System Description

We investigate the joint pricing and security investment problem in the competitive cloud security service market as shown in Fig. 1. In the market under our consideration, there are CSSVs competing to sell their substitutable cloud security plans. The plan is composed of cloud security service and cloud-insurance. The cloud security service is used to protect the basic cloud service enjoyed by users, and the cloud-insurance provides the users with the claim payment if the cloud security service cannot prevent an attack from happening. The CSSVs are able to set prices and invest to improve their offered cloud security service. The users make their decisions to purchase a cloud security plan by considering the prices, the perceived cyber breach probability of the offered security service as well as the interaction with other users. The notations have been summarized in Table 1.

3.1 Preliminaries

Motivated by [27], we quantify the effectiveness of information security spending in addressing the vulnerability of an organization's information and communication system with a family of security breach probability functions. In particular, let $v(z)$ denote the cyber breach probability of the cloud security service when the corresponding investment is z. Accordingly, $q = 1 - v(z)$ is the probability of that the cloud security service is not breached corresponding to the security investment of z, which is named as "security level". [27] introduced a family of security breach probability functions, i.e., $v(\cdot)$, with tractably mathematical expression including

1) The Exponential Power Class of cyber breach probability function, i.e.,

$$v_{\mathrm{EP}}(z) = v(1)^{z^{\alpha}}; \tag{1}$$

TABLE 1
Notations

Symbol	Description
i, j	Users i, j
A, B	Cloud security service vendors (CSSVs)
$\mathcal{N}$	A set of users
$x_i, 1-x_i$	Demand from user i to the CSSV-A and CSSV-B, respectively
$\mathbf{x}_{-i}$	Demands to the CSSV-A without user i
$\mathbf{G}$, g_{ij}	Security interdependency matrix and its elements, respectively
a_i, b_i	Parameters of concave utility functions [32]
d^{A}, d^{B}	Coefficient of congestion of the CSSV-A and CSSV-B, respectively
p_i^{A}, p_i^{B}	Prices of the cloud security plan for user i from the CSSV-A and CSSV-B, respectively
q^{A}, q^{B}	Security levels of the cloud security service from the CSSV-A and CSSV-B, respectively
z^{A}, z^{B}	Investments of the CSSV-A and CSSV-B, respectively
$v(\cdot)$	Probability of being breached for the cloud service
α	$\alpha > 0$ is the parameter for the family of security breach probability functions

2) The Proportional Hazard Class of cyber breach probability function, i.e.,

$$v_{\mathrm{PH}}(z) = 1 - [1 - v(1)]^{z^{-\alpha}}; \tag{2}$$

3) The Wang Transform Class of cyber breach probability function, i.e.,

$$v_{\mathrm{WT}}(z) = \Phi\left[\Phi^{-1}(v(1)) - \alpha \ln(z)\right]; \tag{3}$$

where Φ is the cumulative distribution function for the standard normal distribution, $v(1)$ is the cyber breach probability when investment is 1, i.e., $z = 1$, and $\alpha > 0$. Therein, α quantifies the effect of the historical information of the cloud security service on the security level, and $v(1)$ captures the effect of the efficiency of the investment on the improvement of the cyber breach probability. For example, if the security solution is highly effective and well developed as shown in the historical data, the value of α should be large while that of $v(1)$ should be small. Note that although the cyber breach probability depends on many factors such as type of attack, the number of attackers, the techniques used in the attack and prevention, for tractability reason, we consider only these two parameters, i.e., α and $v(1)$. The more sophisticated function with more degrees of freedom will be considered in the future work. Note also that the above family of security breach probability functions is applicable to the analytical results presented in Section 4.2 due to their monotonic decreasing and convex properties.

To illustrate the quantitative effect of the investment on the improvement of the cyber breach probability and hence interpret the physical meaning of (1), (2), and (3), Fig. 2 plots the cyber breach probability and the security level against the investment for $v(1) = 0.5$ and $\alpha = 0.5$. As shown in Fig. 2a, all the curves are monotonic decreasing and convex. This means that the cyber breach probability decreases as the investment increases, which results in higher security level and hence more reliable cloud security service. Moreover, the decreasing

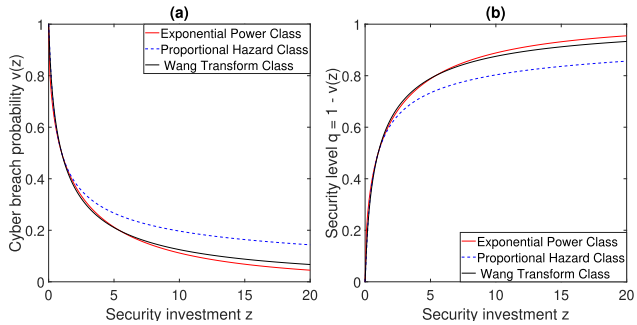


Fig. 2. (a) The relationship between the cyber breach probability $v(z)$ and the investment z and (b) the relationship between the security level $q = 1 - v(z)$ and the investment z.

rate of the cyber breach probability becomes smaller when it is close to its minimum value, i.e., 0. This implies the fact that achieving a perfect cloud security solution is impossible. We observe that there are some differences among these three curves with respect to the convexity. These differences on convexity can be used to investigate the differences among the specific techniques adopted in the cloud security services provided by the CSSVs. For example, IBM Trusteer uses its patented analytics and machine learning for real-time risk level evaluation [30] while Oracle uses LORIC's machine learning [4]. Consider the investment to be on computation resource for training machine learning algorithms. The more investment allows CSSV to adopt more sophisticated models, e.g., more number of hidden nodes in deep learning, which leads to higher security level, e.g., higher accuracy of intrusion detection. Many studies such as [31] experimented and showed such relationship which is consistent with our proposed functions. It is worth noting that the model parameters $v(1)$ and α can be estimated and set according to the real experimental results, e.g., from [31].

Additionally, due to the bijection in the family of security breach probability functions, i.e., (1), (2), and (3), shown in Fig. 2, the investment can be defined as a function of the cyber breach probability and further the security level as follows:

$$v\,(z) = 1 - q \Leftrightarrow z(q) = v^{-1}(1-q). \tag{4}$$

Accordingly, the investment determination problem of the CSSVs is transformed into a security level determination problem of the CSSVs.

3.2 System Model

For ease of presentation, we study a cloud security service market, where two CSSVs, i.e., CSSV-A and CSSV-B, are competing to sell their cloud security plans to users as shown in Fig. 1. The set of the users is denoted by $\mathcal{N}$. Each user $i \in \mathcal{N}$ will buy one cloud security plan. Let $x_i \in [0, 1]$ denote user i's demand of the cloud security plan to CSSV-A. Correspondingly, user i's demand of the cloud security plan to CSSV-B is $1 - x_i$. The strategies of the user i are therefore x_i and $1 - x_i$. Note that the demand fraction x_i can indicate the probability that user i buys from the CSSV-A. Note also that we consider a unit demand that the user "will definitely purchase" the cloud security plan. Hence, the scenario that the user decides not to buy is not under our consideration.

The security levels of cloud security service provided by the CSSV-A and CSSV-B are denoted by q^{A} and q^{B}, respectively. The security levels have an impact on the users' purchasing demand. For example, the better security level can attract more demand. Furthermore, the security levels q^{A} and q^{B} depend on the investments by the CSSVs, which are denoted by z^{A} and z^{B}, respectively.

The marginal cost for each the CSSV is decomposed into two parts, i.e., the investment for improving the security level of the cloud security service and the claim paid to the users if the cloud security service cannot prevent the attack from happening. Note that the investments are part of the CSSVs' running costs while they are independent of the users' demands. However, the costs incurred by the claims paid to the users are dependent on the users' demand. In this case, the marginal cost of providing cloud security plan by the CSSV-A is decomposed into two part as follows [27]:

$$z^{\mathrm{A}}\big(q^{\mathrm{A}}\big) \text{ and } \big(1-q^{\mathrm{A}}\big)n\lambda, \tag{5}$$

where n and λ represent the number of threats and the monetary value of the insured asset, respectively. Here, the terms $z^{\mathrm{A}}\big(q^{\mathrm{A}}\big)$ and $\big(1-q^{\mathrm{A}}\big)n\lambda$ account for the costs incurred by the investment and the claim paid to the users if the cloud security service provided by the CSSV-A cannot prevent the attack from happening, respectively. The cost for providing service is fixed and hence is not accounted. The marginal cost for the CSSV-B can be decomposed and expressed similarly, i.e., $z^{\mathrm{B}}\big(q^{\mathrm{B}}\big)$ and $\big(1-q^{\mathrm{B}}\big)n\lambda$.

We denote the strategies of the users on the CSSV-A by $\mathbf{x} \triangleq \big[x_1,\ldots,x_{|\mathcal{N}|}\big]^{\top}$, where x_i for all $i \in \mathcal{N}$ is the demand of user i. Moreover, we define $\mathbf{x}_{-i} \triangleq [x_1,\ldots,x_{i-1},x_{i+1}\ldots, x_{|\mathcal{N}|}]^{\top}$. Then, by applying the strategy of x_i, user i can achieve the utility of [14]:

$$\begin{aligned} &u_i\big(x_i,\mathbf{x}_{-i},p_i^{\mathrm{A}},p_i^{\mathrm{B}},q^{\mathrm{A}},q^{\mathrm{B}}\big)\\ &= q^{\mathrm{A}}a_ix_i - b_i{x_i}^2 + q^{\mathrm{B}}a_i(1-x_i) - b_i(1-x_i)^2\\ &\quad + \sum_{j\in\mathcal{N}} g_{ij}x_ix_j + \sum_{j\in\mathcal{N}} g_{ij}(1-x_i)\big(1-x_j\big) - p_i^{\mathrm{A}}x_i\\ &\quad - p_i^{\mathrm{B}}(1-x_i) - \frac{d^{\mathrm{A}}}{2}\left(\sum_{j\in\mathcal{N}} x_j\right)^2 - \frac{d^{\mathrm{B}}}{2}\left(\sum_{j\in\mathcal{N}}\big(1-x_j\big)\right)^2. \end{aligned} \tag{6}$$

In (6), we use the linear-quadratic functional from, i.e., $a_ix_i - b_i{x_i}^2$ and $a_i(1-x_i) - b_i(1-x_i)^2$, to capture the marginal decreasing gains of the user's utility. The reason is that the quadratic property not only allows for a tractable analysis and a good second order approximation of concave payoffs but also hints at the essence of the risk-averse users. Specifically, the coefficient $a_i \geq 0$ is the maximum intrinsic demand rate capturing a linear own-effort effect from the investment on the cloud security plan and hence is strongly dependent on the security level of products. The coefficient $b_i \geq 0$ is the intrinsic demand elasticity factor reflecting the convex cost in own-effort [33]. Moreover, if user i is highly risk-averse, the value of a_i should be large while that of b_i should be small. Regarding the terms $\sum_{j\in\mathcal{N}} g_{ij}x_ix_j$ and $\sum_{j\in\mathcal{N}} g_{ij}(1-x_i)\big(1-x_j\big)$, they measure the security interdependency among the users. Here, $g_{ij} \geq 0$, $\forall i,j \in \mathcal{N}$, i.e., the element of the interdependency matrix $\mathbf{G}$ on ith row and jth column, quantifies the security interdependency on user i from user j. The element of $\mathbf{G}$ on ith row and ith column, i.e., g_{ii}, $\forall i \in \mathcal{N}$, is assumed to be 0. The security interdependency among users comes from the users' security spending on the cloud security plan. Like the network externality in cloud services market [34], the users can exchange information on other channels, e.g., social networks, of what they buy for the security service plan and construct the interdependency with each other. To purchase x_i unit of cloud security plan from the CSSV-A, user i needs to pay $p_i^{\mathrm{A}}x_i$ to the CSSV-A. Similarly, $p_i^{\mathrm{B}}(1-x_i)$ is the payment that the CSSV-B receives from user i. The terms $\frac{d^{\mathrm{A}}}{2}\big(\sum_{j\in\mathcal{N}} x_j\big)^2$ and $\frac{d^{\mathrm{B}}}{2}\big(\sum_{j\in\mathcal{N}}(1-x_j)\big)^2$ describe the congestion of the cloud security service [35]. Again, we take Oracle CASB Cloud Service [4] as a representative example. Since Oracle CASB Cloud Service dynamically evaluate the users' risks in real-time due to LORIC's machine learning capabilities, the service delay appears when there exists a large number of users. This will decrease the users' utility.

The CSSV-A and CSSV-B aim at maximizing their own profits. The profits of the CSSV-A and CSSV-B are

$$\Pi^{\mathrm{A}} = \sum_{i\in N}\big[p_i^{\mathrm{A}} - \big(1-q^{\mathrm{A}}\big)n\lambda\big]x_i - z^{\mathrm{A}}\big(q^{\mathrm{A}}\big), \tag{7}$$

and

$$\Pi^{\mathrm{B}} = \sum_{i\in N}\big[p_i^{\mathrm{B}} - \big(1-q^{\mathrm{B}}\big)n\lambda\big](1-x_i) - z^{\mathrm{B}}\big(q^{\mathrm{B}}\big), \tag{8}$$

respectively. Note that the investments, $z^{\mathrm{A}}\big(q^{\mathrm{A}}\big)$ and $z^{\mathrm{B}}\big(q^{\mathrm{B}}\big)$, are used to improve the security level of cloud security service. Again, the investments are part of the CSSVs' operating costs while they are independent of the users' demands. However, the costs $\big(1-q^{\mathrm{A}}\big)n\lambda$ and $\big(1-q^{\mathrm{B}}\big)n\lambda$ are due to the claims paid to the users and hence are dependent on the users' demand. Therefore, recall from (5), the cost of each CSSV is divided into two parts based on the fact whether they are dependent on the users' demand or not, e.g., $z^{\mathrm{A}}(q^{\mathrm{A}})$ and $(1-q^{\mathrm{A}})n\lambda$ for the CSSV-A. By pricing the cloud security plan, the CSSV-A receives the revenue of $p_i^{\mathrm{A}}x_i$ from user i while needs to pay the claim of $\big(1-q^{\mathrm{A}}\big)n\lambda x_i$ to user i when the cloud security service of the CSSV-A is breached. Therefore, the profit excluding the cost incurred by the security investment of CSSV-A is $\sum_{i\in N}\big[p_i^{\mathrm{A}} - \big(1-q^{\mathrm{A}}\big)n\lambda\big]x_i$. After including the cost incurred by the investment, the total profit of CSSV-A is shown in (7). The total profit of CSSV-B as shown in (8) can be derived similarly.

3.3 Stackelberg Game Formulation

The CSSVs are the sellers making offers of their services to the market, and the users are the customers. The sellers typically make their decisions before the buyers. Based on the utility and profit functions given in (6), (7), and (8), it is intuitive to model the cloud security market as a two-stage Stackelberg game. Also, this Stackelberg setting is commonly adopted in a similar market situation [14]. Specically, we consider the users to be the followers and they decide on the demand of the cloud security plan based on the price and the security levels. The interaction among the users is studied by formulating

a noncooperative follower subgame. We model the interplay, i.e., competition, between the CSSV-A and CSSV-B as a noncooperative leader subgame on the upper stage. The CSSVs lead to make decision on their strategies, i.e., the prices of cloud security plans for every user and their investments for improving the security level of the cloud security service. The two-stage Stackelberg game is defined as follows:

- Given the strategies of the CSSVs, the noncooperative follower subgame for the users can be defined as a user-level noncooperative game $\mathcal{G}_{\mathrm{u}} = \{\mathcal{N}, \mathbf{x}, \mathcal{X}, \mathbf{u}\}$. Therein, $\mathcal{N}$ denote the set of the users, and $\mathbf{x} = \left[x_1, \ldots, x_{|\mathcal{N}|}\right]^\top$ is the demands of all the user i to the CSSV-A. $\mathcal{X} \subset \mathbb{R}^{|\mathcal{N}|}$ denotes the domain of definition for $\mathbf{x}$. $\mathbf{u} = \left[u_1, \ldots, u_{|\mathcal{N}|}\right]^\top$ is the utility vector of the users, and the element of which is defined in (6);
- Given the strategies of the users, i.e., $\mathbf{x}$, the noncooperative leader subgame for the CSSV-A and CSSV-B can be defined as a CSSV-level noncooperative game $\mathcal{G}_{\mathrm{C}} = \{[\mathbf{p}^{\mathrm{A}\top}, q^{\mathrm{A}}]^\top, \mathcal{D}^{\mathrm{A}}, [\mathbf{p}^{\mathrm{B}\top}, q^{\mathrm{B}}]^\top, \mathcal{D}^{\mathrm{B}}, \mathbf{\Pi}\}$. Here, $[\mathbf{p}^{\mathrm{A}\top}, q^{\mathrm{A}}]^\top = [p_1^{\mathrm{A}}, \ldots, p_{|\mathcal{N}|}^{\mathrm{A}}, q^{\mathrm{A}}]^\top$ is the vector of the prices and security level for the CSSV-A, and $\mathcal{D}^{\mathrm{A}} = \{.[\mathbf{p}^{\mathrm{A}\top}, q^{\mathrm{A}}]^\top | p_i^{\mathrm{A}} \in [0, p^{\mathrm{u}}], \forall i \in \mathcal{N}, q^{\mathrm{A}} \in [0, 1]\}$ is the domain of definition for the prices and security level of the CSSV-A. $[\mathbf{p}^{\mathrm{B}\top}, q^{\mathrm{B}}]^\top$ and $\mathcal{D}^{\mathrm{B}}$ are defined in a similar way. $\mathbf{\Pi} = \left[\Pi^{\mathrm{A}}, \Pi^{\mathrm{B}}\right]^\top$ is the profit vector for the CSSVs.

In the next section, we analyze the equilibrium of the above game.

4 Stackelberg Equilibrium Analysis

$$\begin{aligned}\frac{\partial u_i}{\partial x_i} &= q^{\mathrm{A}}a_i - 2b_i x_i - q^{\mathrm{B}}a_i + 2b_i(1-x_i) + \sum_{j\in N} g_{ij}x_j + g_{ii}x_i \\ &\quad - \sum_{j\in N} g_{ij}(1-x_j) - g_{ii}(1-x_i) - d^{\mathrm{A}}\sum_j x_j \\ &\quad + d^{\mathrm{B}}\sum_j (1-x_j) - p_i^{\mathrm{A}} + p_i^{\mathrm{B}} \\ &= \left(q^{\mathrm{A}} - q^{\mathrm{B}}\right)a_i - 4b_i x_i + 2b_i + 2\sum_{j\in N} g_{ij}x_j - \sum_{j\in N} g_{ij} \\ &\quad - \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)\sum_j x_j + |\mathcal{N}|d^{\mathrm{B}} - p_i^{\mathrm{A}} + p_i^{\mathrm{B}}, \quad \forall i \in \mathcal{N} \end{aligned} \tag{9}$$

$$\begin{aligned}\frac{\partial \mathbf{u}}{\partial \mathbf{x}} &= \left(q^{\mathrm{A}} - q^{\mathrm{B}}\right)\mathbf{a} - 2\mathbf{B}\mathbf{x} + \mathbf{B}\mathbf{1} + 2\mathbf{G}\mathbf{x} - \mathbf{G}\mathbf{1} \\ &\quad - \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)\mathbf{I}\mathbf{x} + |\mathcal{N}|d^{\mathrm{B}}\mathbf{1} - \mathbf{p}^{\mathrm{A}} + \mathbf{p}^{\mathrm{B}}. \end{aligned} \tag{10}$$

$$\begin{aligned}&\left(q^{\mathrm{A}} - q^{\mathrm{B}}\right)\mathbf{a} - 2\mathbf{B}\mathbf{x}^* + \mathbf{B}\mathbf{1} + 2\mathbf{G}\mathbf{x}^* - \mathbf{G}\mathbf{1} \\ &- \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)\mathbf{I}\mathbf{x}^* + |\mathcal{N}|d^{\mathrm{B}}\mathbf{1} - \mathbf{p}^{\mathbf{A}} + \mathbf{p}^{\mathbf{B}} = \mathbf{0} \\ &\Leftrightarrow \quad \left(q^{\mathrm{A}} - q^{\mathrm{B}}\right)\mathbf{a} + (\mathbf{B} - \mathbf{G})\mathbf{1} + |\mathcal{N}|d^{\mathrm{B}}\mathbf{1} - \mathbf{p}^{\mathbf{A}} + \mathbf{p}^{\mathbf{B}} \\ &= \left[2\mathbf{B} - 2\mathbf{G} + \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)\mathbf{I}\right]\mathbf{x}^* \end{aligned} \tag{11}$$

$$\begin{aligned}\mathbf{x}^* = [2\mathbf{B} - 2\mathbf{G} + (d^{\mathrm{A}} + d^{\mathrm{B}})\mathbf{I}]^{-1}[(q^{\mathrm{A}} - q^{\mathrm{B}})\mathbf{a} \\ + (\mathbf{B} - \mathbf{G})\mathbf{1} + |\mathcal{N}|\lceil^{\mathrm{B}}\mathbf{1} - \mathbf{p}^{\mathbf{A}} + \mathbf{p}^{\mathbf{B}}]\end{aligned} \tag{12}$$

$$\begin{aligned}&\left\{\left[2\mathbf{B} - 2\mathbf{G} + \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)\mathbf{I}\right]\right\}_{ii} = 4b_i + \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right) > \sum_{j\neq i}\left[2g_{ij} - \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)\right] \\ &= \sum_{j\neq i}\left|2g_{ij} - \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)\right| = \sum_{j\neq i}\left|\left\{\left[2\mathbf{B} - 2\mathbf{G} + \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)\mathbf{I}\right]\right\}_{ij}\right|. \end{aligned} \tag{13}$$

Following the backward induction, we first obtain the Nash Equilibrium (NE) of the user-level game $\mathcal{G}_{\mathrm{u}}$ by using the first order optimality condition. The concavity of the utility functions indicates the existence of the NE in the user-level game $\mathcal{G}_{\mathrm{u}}$. This NE is proven to be unique by showing that the Jacobian matrix of the utility functions of the user-level game $\mathcal{G}_{\mathrm{u}}$ satisfies the dominance solvability condition.[2] Then, we substitute the NE of the user-level game $\mathcal{G}_{\mathrm{u}}$ into the CSSV-level game $\mathcal{G}_{\mathrm{C}}$ and prove that the Jacobian matrix of the profit functions of the CSSV-level game $\mathcal{G}_{\mathrm{C}}$ is negative definite. This demonstrates the existence and uniqueness of the NE to the CSSV-level game $\mathcal{G}_{\mathrm{C}}$ exists and is unique. The Stackelberg equilibrium therefore exists and is unique.

4.1 Equilibrium Analysis for the User-Level Game

To obtain the optimal solution for the user-level game $\mathcal{G}_{\mathrm{u}}$, we take the partial derivative of (6) with respect to x_i, which has been shown in (9).

Let $\mathbf{a} = \left[a_1, a_2, \ldots, a_{|\mathcal{N}|}\right]^\top$, $\mathbf{p}^{\mathrm{A}} = \left[p_1^{\mathrm{A}}, p_2^{\mathrm{A}}, \ldots, p_{|\mathcal{N}|}^{\mathrm{A}}\right]^\top$, $\mathbf{p}^{\mathrm{B}} = [p_1^{\mathrm{B}}, p_2^{\mathrm{B}}, \ldots, p_{|\mathcal{N}|}^{\mathrm{B}}]^\top$, $\mathbf{1} = ones \quad (|\mathcal{N}|, 1)$, $\mathbf{B} = diag([2b_1, 2b_2, \ldots, 2b_{|\mathcal{N}|}])$, and $\mathbf{I} = ones(|\mathcal{N}|, |\mathcal{N}|)$, $\frac{\partial u_i}{\partial x_i}$, $\forall i \in \mathcal{N}$ can be rewritten in a matrix form, i.e., (10).

Let $\frac{\partial u_i}{\partial x_i} = 0$, $\forall i \in \mathcal{N}$, we have $\mathbf{x}^*$, i.e., the best responses of the users, as shown in (11).

Lemma 1. *The invertibility and positive definiteness of the matrix* $\left[2\mathbf{B} - 2\mathbf{G} + \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)\mathbf{I}\right]$ *are guaranteed if* $\frac{\sum_{j\neq i}\left[2g_{ij} - \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)\right]}{4b_i + \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)} < 1$, $\forall i \in \mathcal{N}$.

Proof. We have $\frac{2g_{ij} - \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)}{4b_i + \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)} \geq 0$, $\left(d^{\mathrm{A}} + d^{\mathrm{B}}\right) > 0$, and $b_i > 0$. Moreover, we also have $2g_{ij} - \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right) \geq 0$ and $4b_i + \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right) > \sum_{j\neq i}\left[2g_{ij} - \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)\right] = \sum_{j\neq i}\left|2g_{ij} - \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)\right|$. Therefore, the inequality (13) is certainly satisfied, where $\{\cdot\}_{ij}$ denotes the ijth element of a matrix. This implies the strictly diagonal dominance of the matrix $\left[2\mathbf{B} - 2\mathbf{G} + \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)\mathbf{I}\right]$. Moreover, according to Gershgorin circle theorem [36], every eigenvalue λ of the matrix $\left[2\mathbf{B} - 2\mathbf{G} + \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)\mathbf{I}\right]$ satisfies

$$\begin{aligned}&\left|\left\{\left[2\mathbf{B} - 2\mathbf{G} + \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)\mathbf{I}\right]\right\}_{ii} - \lambda\right| \\ &\leq \sum_{j\neq i}\left|\left\{\left[2\mathbf{B} - 2\mathbf{G} + \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)\mathbf{I}\right]\right\}_{ij}\right|. \end{aligned} \tag{14}$$

Due to the strictly diagonal dominance of $[2\mathbf{B} - 2\mathbf{G} + \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)\mathbf{I}]$ and, moreover, $\{[2\mathbf{B} - 2\mathbf{G} + \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)\mathbf{I}]\}_{ii} = 4b_i + \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)$ is larger than 0, we can conclude that λ is positive. Consequently, $\left[2\mathbf{B} - 2\mathbf{G} + \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)\mathbf{I}\right]$ is positive definite due to the fact that all its eigenvalues are larger than 0. In addition, $\left[2\mathbf{B} - 2\mathbf{G} + \left(d^{\mathrm{A}} + d^{\mathrm{B}}\right)\mathbf{I}\right]$ is invertible because of its positive definiteness.

2. The dominance solvability condition for a concave game is $-\frac{\partial^2 u_i}{\partial x_i^2} \geq \sum_j |\frac{\partial^2 u_i}{\partial x_i \partial x_j}|$, where u_i and x_i are the utility function and strategy for user i, respectively.

$$[\nabla_{i,j}u_i(\mathbf{x})]_{\forall i,j\in\mathcal{N}} + [\nabla_{i,j}u_i(\mathbf{x})]^{\top}_{\forall i,j\in\mathcal{N}}$$
$$= \begin{bmatrix} \nabla_{1,1}u_1(\mathbf{x}) & \nabla_{1,2}u_1(\mathbf{x}) & \cdots & \nabla_{1,|\mathcal{N}|}u_1(\mathbf{x}) \\ \nabla_{2,1}u_2(\mathbf{x}) & \nabla_{2,2}u_2(\mathbf{x}) & \cdots & \nabla_{2,|\mathcal{N}|}u_2(\mathbf{x}) \\ \vdots & \vdots & \ddots & \vdots \\ \nabla_{|\mathcal{N}|,1}u_{|\mathcal{N}|}(\mathbf{x}) & \nabla_{|\mathcal{N}|,2}u_{|\mathcal{N}|}(\mathbf{x}) & \cdots & \nabla_{|\mathcal{N}|,|\mathcal{N}|}u_{|\mathcal{N}|}(\mathbf{x}) \end{bmatrix} + \begin{bmatrix} \nabla_{1,1}u_1(\mathbf{x}) & \nabla_{1,2}u_1(\mathbf{x}) & \cdots & \nabla_{1,|\mathcal{N}|}u_1(\mathbf{x}) \\ \nabla_{2,1}u_2(\mathbf{x}) & \nabla_{2,2}u_2(\mathbf{x}) & \cdots & \nabla_{2,|\mathcal{N}|}u_2(\mathbf{x}) \\ \vdots & \vdots & \ddots & \vdots \\ \nabla_{|\mathcal{N}|,1}u_{|\mathcal{N}|}(\mathbf{x}) & \nabla_{|\mathcal{N}|,2}u_{|\mathcal{N}|}(\mathbf{x}) & \cdots & \nabla_{|\mathcal{N}|,|\mathcal{N}|}u_{|\mathcal{N}|}(\mathbf{x}) \end{bmatrix}^{\top} \tag{15}$$

$$= 2\begin{bmatrix} -4b_1 - \left(d^{\mathrm{A}}+d^{\mathrm{B}}\right) & 2g_{12} - \left(d^{\mathrm{A}}+d^{\mathrm{B}}\right) & \cdots & 2g_{1|\mathcal{N}|} - \left(d^{\mathrm{A}}+d^{\mathrm{B}}\right) \\ 2g_{21} - \left(d^{\mathrm{A}}+d^{\mathrm{B}}\right) & -4b_2 - \left(d^{\mathrm{A}}+d^{\mathrm{B}}\right) & \cdots & 2g_{2|\mathcal{N}|} - \left(d^{\mathrm{A}}+d^{\mathrm{B}}\right) \\ \vdots & \vdots & \ddots & \vdots \\ 2g_{|\mathcal{N}|1} - \left(d^{\mathrm{A}}+d^{\mathrm{B}}\right) & 2g_{|\mathcal{N}|2} - \left(d^{\mathrm{A}}+d^{\mathrm{B}}\right) & \cdots & -4b_{|\mathcal{N}|} - \left(d^{\mathrm{A}}+d^{\mathrm{B}}\right) \end{bmatrix} = -2\left[2\mathbf{B} - 2\mathbf{G} + \left(d^{\mathrm{A}}+d^{\mathrm{B}}\right)\mathbf{I}\right] \tag{16}$$

$$\begin{aligned} \Pi^{\mathrm{A}} &= \sum_{i\in\mathcal{N}} (p_i^{\mathrm{A}} - (1-q^{\mathrm{A}})n\lambda)x_i - z^{\mathrm{A}}(q^{\mathrm{A}}) \\ &= [\mathbf{p}^{\mathrm{A}} - (1-q^{\mathrm{A}})n\lambda\mathbf{1}]^{\top}\mathbf{x} - z^{\mathrm{A}}(q^{\mathrm{A}}) \\ &= [\mathbf{p}^{\mathrm{A}} - (1-q^{\mathrm{A}})n\lambda\mathbf{1}]^{\top}\mathbf{K}[(q^{\mathrm{A}}-q^{\mathrm{B}})\mathbf{a} + (\mathbf{B}-\mathbf{G})\mathbf{1} \\ &\quad + |\mathcal{N}|d^{\mathrm{B}}\mathbf{1} - \mathbf{p}^{\mathbf{A}} + \mathbf{p}^{\mathbf{B}}] - z^{\mathrm{A}}(q^{\mathrm{A}}) \end{aligned} \tag{17}$$

$$\begin{aligned} \Pi^{\mathrm{B}} &= \sum_{i\in\mathcal{N}} (p_i^{\mathrm{B}} - (1-q^{\mathrm{B}})n\lambda)(1-x_i) - z^{\mathrm{B}}(q^{\mathrm{B}}) \\ &= [\mathbf{p}^{\mathrm{B}} - (1-q^{\mathrm{B}})n\lambda\mathbf{1}]^{\top}(\mathbf{1}-\mathbf{x}) - z^{\mathrm{B}}(q^{\mathrm{B}}) \\ &= [\mathbf{p}^{\mathrm{B}} - (1-q^{\mathrm{B}})n\lambda\mathbf{1}]^{\top} \\ &\quad \times \{\mathbf{1} - \mathbf{K}[(q^{\mathrm{A}}-q^{\mathrm{B}})\mathbf{a} + (\mathbf{B}-\mathbf{G})\mathbf{1} + |\mathcal{N}|d^{\mathrm{B}}\mathbf{1} - \mathbf{p}^{\mathbf{A}} \\ &\quad + \mathbf{p}^{\mathbf{B}}]\} - z^{\mathrm{B}}(q^{\mathrm{B}}). \end{aligned} \tag{18}$$

□

Since $[2\mathbf{B} - 2\mathbf{G} + (d^{\mathrm{A}}+d^{\mathrm{B}})\mathbf{I}]$ is invertible as proven in Lemma 1, we can left multiply both the sides of (11) by its inverse matrix and obtain the optimal solution to $\mathcal{G}_{\mathrm{u}}$ as shown in (12). Moreover, we can have

$$\mathbf{x}^* = \mathbf{K}[(q^{\mathrm{A}}-q^{\mathrm{B}})\mathbf{a} + (\mathbf{B}-\mathbf{G})\mathbf{1} + |\mathcal{N}|^{\mathrm{B}}\mathbf{1} - \mathbf{p}^{\mathbf{A}} + \mathbf{p}^{\mathbf{B}}], \tag{19}$$

where $\mathbf{K} = [2\mathbf{B} - 2\mathbf{G} + (d^{\mathrm{A}}+d^{\mathrm{B}})\mathbf{I}]^{-1}$ is positive definite thanks to the positive definiteness of its inverse matrix as proven in Lemma 1.

Proposition 1. *If the game $\mathcal{G}_{\mathrm{u}}$ can satisfy: 1) $\mathcal{X} \subset \mathbb{R}^{|\mathcal{N}|}$ is nonempty, convex, and compact; 2) $\mathbf{u}$ is continuous with respect to $\mathbf{x}$, and u_i is concave with respect to x_i, there exists one NE.*

Theorem 1. *There exists NE in the user-level noncooperative game $\mathcal{G}_{\mathrm{u}} = \{\mathcal{N}, \mathbf{x}, \mathcal{X}, \mathbf{u}\}$.*

Proof. Based on (6), we can have

$$\frac{\partial^2 u_i}{\partial {x_i}^2} = -4b_i + 2g_{ii} - \left(d^{\mathrm{A}}+d^{\mathrm{B}}\right) = -4b_i - \left(d^{\mathrm{A}}+d^{\mathrm{B}}\right) \le 0, \tag{20}$$

which implies that $u_i\left(x_i, \mathbf{x}_{-i}, \mathbf{p}^{\mathrm{A}}, \mathbf{p}^{\mathrm{B}}, q^{\mathrm{A}}, q^{\mathrm{B}}\right)$ is concave with respect to x_i, $\forall i \in \mathcal{N}$. Moreover, as $\mathcal{X} = \{[x_1, \ldots, x_{|\mathcal{N}|}] | x_i \in [0,1], \forall i \in \mathcal{N}\}$ satisfies the first condition of Proposition 1, there exists one NE in the user-level noncooperative game $\mathcal{G}_{\mathrm{u}} = \{\mathcal{N}, \mathbf{x}, \mathcal{X}, \mathbf{u}\}$. □

Theorem 2. *According to Lemma 1, if the Jacobian matrix of $\mathbf{u}(\mathbf{x}) = \left[u_1(\mathbf{x}), \ldots, u_{|\mathcal{N}|}(\mathbf{x})\right]^{\top}$ can satisfy the dominance solvability condition, there exists one unique NE for the user-level noncooperative game $\mathcal{G}_{\mathrm{u}} = \{\mathcal{N}, \mathbf{x}, \mathcal{X}, \mathbf{u}\}$.*

Proof. We will prove that the Jacobian matrix of the utility functions of $\mathcal{G}_{\mathrm{u}}$ satisfies the dominance solvability condition in the following. The Jacobian matrix of $\mathbf{u}(\mathbf{x}) = [u_1(\mathbf{x}), \ldots, u_{|\mathcal{N}|}(\mathbf{x})]^{\top}$ is shown in (15), where $\nabla_{i,j}u_i(\mathbf{x})$ is the second partial derivative of $u_i(\mathbf{x})$ with respect to x_i first and x_j second, i.e., $\frac{\partial^2 u_i}{\partial x_i \partial x_j}$, $\forall i, j \in \mathcal{N}$. Then, based on (15), we can obtain (16).

Based on Lemma 1 and the strictly diagonally dominance of $-\left[\nabla_{i,j}u_i(\mathbf{x})\right]_{\forall i,j\in\mathcal{N}} - \left[\nabla_{i,j}u_i(\mathbf{x})\right]^{\top}_{\forall i,j\in\mathcal{N}}$, the specifical Jacobian matrix (16) satisfies the dominance solvability condition. Therefore, $\left[\nabla_{i,j}u_i(\mathbf{x})\right]_{\forall i,j\in\mathcal{N}} + \left[\nabla_{i,j}u_i(\mathbf{x})\right]^{\top}_{\forall i,j\in\mathcal{N}}$, i.e., the Jacobian matrix, satisfies the dominance solvability condition [37]. This implies that the user-level noncooperative game $\mathcal{G}_{\mathrm{u}} = \{\mathcal{N}, \mathbf{X}, \mathcal{X}, \mathbf{u}\}$ admits an unique NE. The proof is completed. □

4.2 Equilibrium Analysis for the CSSV-Level Game

Given the users' strategies, for the CSSV-A and CSSV-B in the competitive market, the profit of each CSSV is affected not only by its own price and security level, but also by the price and security level offered by the other CSSV. Therefore, the price and security level determination between the CSSVs is a noncooperative game $\mathcal{G}_{\mathrm{C}}$. The NE of the CSSV-level game is a strategy that no CSSV can increase its profit by choosing a different strategy with the other players' strategies unchanged [38]. In this case, we first prove that the CSSV-level noncooperative game $\mathcal{G}_{\mathrm{C}}$ admits one NE, and the uniqueness of which will be proven later.

Given the users' strategies in (12), we can rewrite the profit functions for the CSSVs in a matrix form as shown in (17) and (18). In (17) and (18), the investments z^{A} and z^{B} are in the functional form as shown in (4), in which security levels q^{A} and q^{B} are their independent variables, respectively. Then, we calculate the second partial derivatives of (17) with respect to $\mathbf{p}^{\mathrm{A}}$ and q^{A} as well as that of (18) with respect to $\mathbf{p}^{\mathrm{B}}$ and q^{B} as shown in (23), where $z^{\mathrm{A}''} = \frac{\partial^2 z^{\mathrm{A}}}{\partial {q^{\mathrm{A}}}^2}$ and $z^{\mathrm{B}''} = \frac{\partial^2 z^{\mathrm{B}}}{\partial {q^{\mathrm{B}}}^2}$.

Theorem 3. *The CSSV-level noncooperative game $\mathcal{G}_{\mathrm{C}}$ admits one NE if $z^{\mathrm{A}''} = \frac{\partial^2 z^{\mathrm{A}}}{\partial {q^{\mathrm{A}}}^2} > (\mathbf{a} + n\lambda\mathbf{1})^{\top}\mathbf{K}(\mathbf{a} + n\lambda\mathbf{1})$ and $z^{\mathrm{B}''}$*

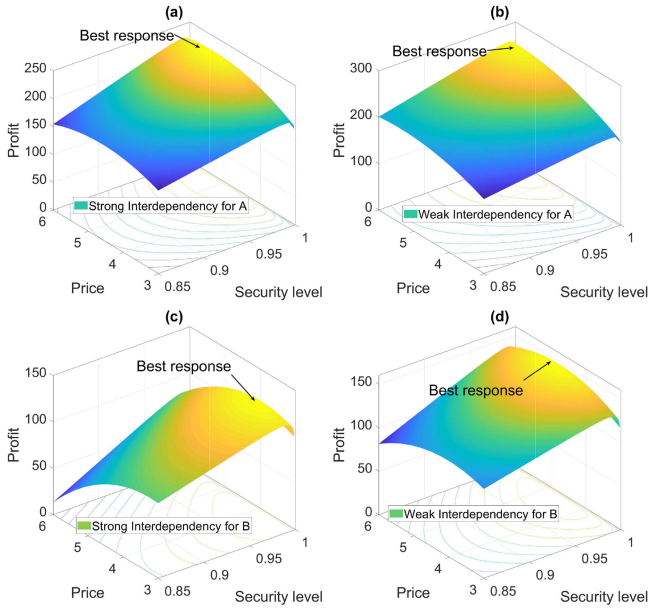


Fig. 3. Best response of the CSSV-A under (a) strong and (b) weak interdependency as well as that of the CSSV-B under (c) strong and (d) weak interdependency.

$= \frac{\partial^2 z^{\mathrm{B}}}{\partial q^{\mathrm{B}2}} > (\mathbf{a}+n\lambda\mathbf{1})^{\top}\mathbf{K}(\mathbf{a}+n\lambda\mathbf{1})$. *Then, the Stackbelberg equilibrium of the market game exists.*

Proof. Please refer to Appendix A, which can be found on the Computer Society Digital Library at http://doi.ieeecomputersociety.org/10.1109/TSC.2020.2996382. □

Theorem 4. *The CSSV-level noncooperative game $\mathcal{G}_{\mathrm{C}}$ admits one unique NE if $z^{\mathrm{A}''} = \frac{\partial^2 z^{\mathrm{A}}}{\partial q^{\mathrm{A}2}} > (\mathbf{a}+n\lambda\mathbf{1})^{\top}\mathbf{K}(\mathbf{a}+n\lambda\mathbf{1})$ and $z^{\mathrm{B}''} = \frac{\partial^2 z^{\mathrm{B}}}{\partial q^{\mathrm{B}2}} > (\mathbf{a}+n\lambda\mathbf{1})^{\top}\mathbf{K}(\mathbf{a}+n\lambda\mathbf{1})$. Then, the Stackbelberg equilibrium of the market game is unique.*

Proof. Please refer to Appendix B, available in the online supplemental material. □

As Theorems 3 and 4 have respectively guaranteed the existence and uniqueness of the Stackelberg equilibrium, the iterative best response algorithm in [39] can be adopted to search for the equilibrium according to Theorem 10 in [39].

5 Performance Evaluation

5.1 Parameters Setting

In this section, we present the numerical results to study the behaviours of the players in the cloud security service market. The number of the users in the cloud security service market is $|\mathcal{N}|$. The parameter setting for the users are $a_i \sim N(\mu_a, \sigma)$ and $b_i \sim N(\mu_b, \sigma)$ with $\mu_a = 10$, $\mu_b = 2.3$, and $\sigma = 1/3$. Due to the diversity of the CSSVs, we set the intrinsic parameters for the congestion of the CSSVs as $d^{\mathrm{A}} \sim N(\mu_d, \sigma)$ and $d^{\mathrm{B}} = d^{\mathrm{A}} + d$, where $\mu_d = 0.1$ and $d = 0.05$. The off-diagonal elements of interdependency matrix $\mathbf{G}$, i.e., g_{ij}, $\forall i \neq j$, is generated following $N(\mu_g, \sigma)$, where $\mu_g = 0.13$ for strong interdependency and 0.12 for weak interdependency. The diagonal elements of interdependency matrix $\mathbf{G}$, i.e., g_{ii}, $\forall i \in \mathcal{N}$, equal 0 [14]. The other default coefficients are set as follows: $v(1) = 0.5$, $n = 1$, $\lambda = 1$, $p^{\mathrm{u}} = 10$, and $\alpha = 2$. Without loss of generality, we choose the functional form for the Proportional Hazard Class of security breach probability as expressed in (2), as the specific formulation for $v(z)$. However, similar results are expected for the other classes of security breach probability. Note that the price shown in the following figures is the mean of the discriminative prices.

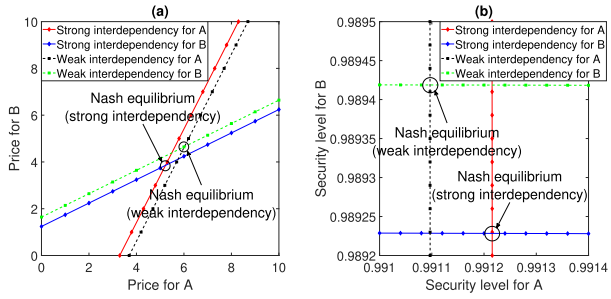


Fig. 4. NE for (a) price and (b) security level.

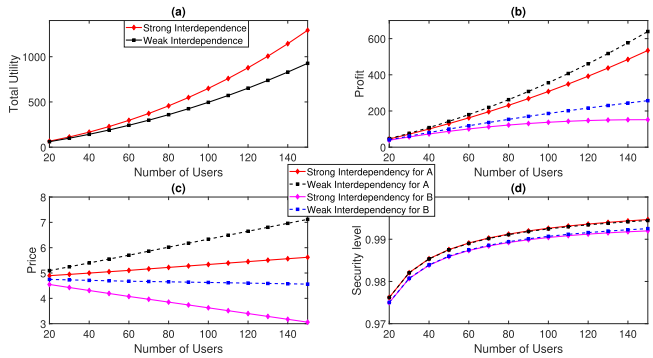


Fig. 5. (a) Total users' utilities, (b) profit, (c) price and (d) security level with increasing users and different levels of interdependency.

5.2 Numerical Results

Figs. 3 and 4 show the best response and NE, respectively. We first evaluate the profit of the CSSV. In Fig. 3, the CSSVs serve 80 users. The profit of the CSSV-A changes due to the different prices charging the users and different investments to improve the security level of cloud security service. From Fig. 3a, there is a point where the profit of the CSSV-A is maximized, which is pointed by the arrowhead of "Best response". This point constitutes the Stackelberg equilibrium for the CSSV-A. As is evident from Fig. 3a, this profit, which is a function of price and security level, is unimodal, and the optimal solution can be obtained analytically.

Fig. 4 illustrates the NEs of the price and security level for the CSSV-A and CSSV-B under different levels of interdependency. The NE is the point at which the best responses for the CSSV-A and CSSV-B intersect. Under different levels of interdependency among the users, different NEs are observed. As expected, when the level of interdependency is strong, the prices of cloud security plans provided by the CSSV-A and CSSV-B decrease, which can be observed in Fig. 4a. Furthermore, when the level of interdependency is strong, the security level of the cloud security service for the CSSV-A increases slightly while that for the CSSV-B

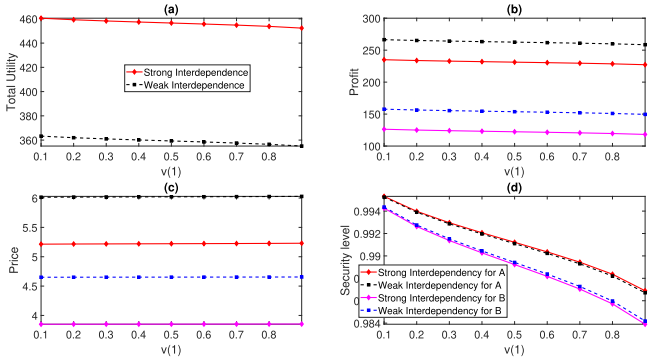


Fig. 6. (a) Total users' utilities, (b) profit, (c) price and (d) security level with increasing probability of being breached $v(1)$.

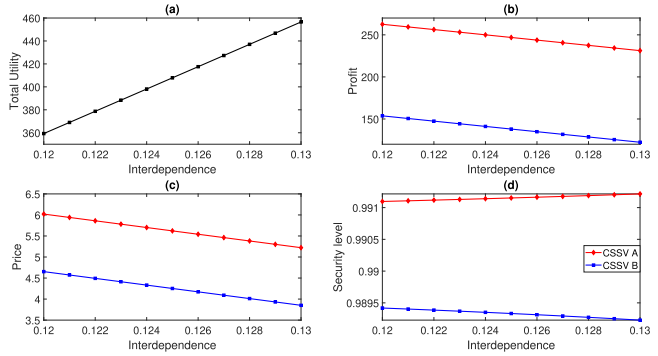


Fig. 7. (a) Total utilities, (b) profit, (c) price, and (d) security level with varying interdependency.

decreases slightly, as shown in Fig. 4b. The reason for this phenomenon is explained in the subsequent discussions.

We evaluate the impact of number of users in Fig. 5. From Fig. 5a, the total utilities in the cloud security service market under strong interdependency are always higher than those under weak interdependency. The reason is that the users will become safer if many of other users also buy the same cloud security plan. In other words, the security level of user j is enhanced if its associated neighbor user i also buys the same cloud security plan. Clearly, this enhancement in the users' security level under strong interdependency is larger than that under weak interdependency. This is also consistent with the results that the increasing rate of the users' total utilities under strong interdependency is faster than that under weak interdependency. As shown in Fig. 5b, the profits of both the CSSV-A and CSSV-B decrease as the interdependency becomes stronger. The main reason is that when the users are strongly interdependent, the CSSVs need to remain competitive by improving the security level of the cloud security service. However, this requires much more investment as the increasing rate of the security level becomes smaller when it is close to the maximum level as shown in Fig. 2. Thus, the CSSVs may not want to invest too much in improving the near perfect security level. From Fig. 5d, the security level is therefore not affected much by the changes in the level of interdependency. As a result, the CSSVs have to adjust their prices appropriately, which can be observed from the numerical results in Fig. 5c.

We evaluate the impact of the parameter $v(1)$ (i.e., the probability of being breached when investment is 1). We set the number of users to be 80 and $v(1)$ is varied from 0.1 to 0.9. As shown in Fig. 6d, the security level of cloud security service decreases as $v(1)$ increases, which leads to the increase of the probability of being breached. Correspondingly, this further leads to the decrease in the users' total utilities as shown in Fig. 6a. The reason is that the users may become unsafer as the probability of being breached increases, even when they are covered by the cloud-insurance. Additionally, the decrease in the security level of cloud security service has an impact on the profits of the CSSVs. The decrease in the security level of cloud security service leads to the increase of the probability of paying claims. In this case, even when the prices of the cloud security plan do not change simultaneously, the profits of both the CSSVs decrease as $v(1)$ increases.

Fig. 7 shows the impact of user's interdependency. The number of users is 80 in the market, and μ_g is increased. As expected, the users' total utilities increase as the level of interdependency becomes stronger while both the profits and prices of the CSSVs decrease, as shown in Figs. 7a, 7b, and 7c. From Fig. 7d, the security level for the CSSV-A increases slightly as the level of interdependency becomes stronger for the purpose of remaining competitive. In contrast, the security level of cloud security service for the CSSV-B decreases. This is due to the fact that the CSSV-B may not be capable of maintaining such a high security level for the cloud security service when both its price of cloud security plan and profit are much lower than that of the CSSV-A. Furthermore, as aforementioned, the investment becomes larger since the increasing rate of the security level becomes smaller, when the security level is close to the maximum level. This means even a slight decrease in the security level will reduce substantial amount of investment. Therefore, the security level of cloud security service for the CSSV-B decreases slightly as the level of interdependency becomes stronger, which reduces much investment while maintaining a similar security level.

We compare the performance of the proposed competitive market with that of the cooperative market in Fig. 8. In the cooperative market, the CSSV-A and CSSV-B jointly optimize their total profit, i.e., sum of individual profits. From Fig. 8c, in the cooperative market, the price of cloud security plan is always at the maximum level, i.e., p^{u}. Thus, the total profit in the cooperative market under strong interdependency is exactly the same as that under weak interdependency, as shown in Fig. 8b. Furthermore, we observe that the total profit in the cooperative market is always higher than that in the competitive market. This result is not only from the changes in the price but also from the changes in the security level of the cloud security service. First, the prices of cloud security plan in the cooperative market is higher than those in the competitive market, which leads to the increase in the CSSVs' revenue from the users. Second, as shown in Fig. 8d, the security levels of cloud security service in the cooperative market is lower than that in the competitive market. As a result, the CSSVs can reduce their investment. However, in Fig. 8a, compared with the competitive market, the higher price of cloud security plan and lower security level of cloud security service in the cooperative market result in a negative value for the users' total utilities. The reason is that the cooperative market

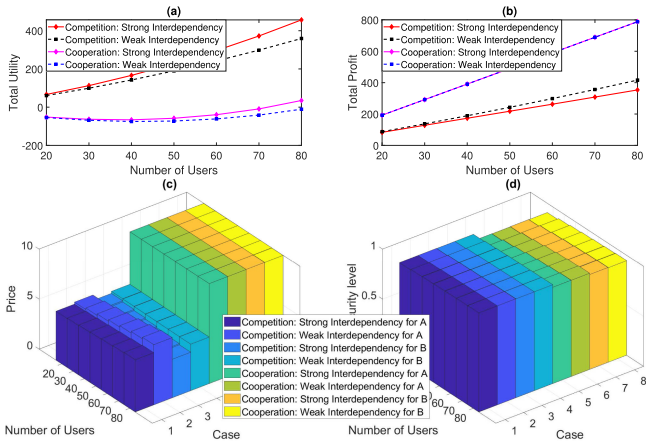


Fig. 8. (a) Total users' utilities, (b) profit, (c) price and (d) security level under competition and cooperation.

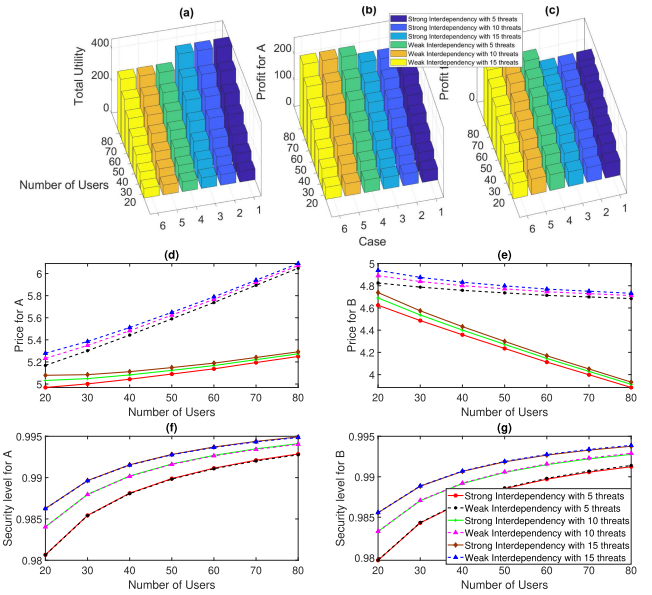


Fig. 9. (a) Total users' utilities, (b) & (c) profit for the CSSVs A & B, (d) & (e) price for the CSSVs A & B, and (f) & (g) security level for the CSSVs A & B with increasing number of the users and increasing numbers of threats.

enables the existing CSSVs to collude and extensively exploit the users. This is consistent with the real-world example about omena, i.e., a small fish, that the fish brokers, i.e., leaders, collude and exploit the fish traders, i.e., followers [40]. The future work on the collusive cloud security service market can be studied.

Fig. 9 shows the impact of n, i.e., the number of threats, on the users' total utilities, the CSSVs' profits, the prices of cloud security plan, and the security level of cloud security service. The security level of cloud security service is improved by the CSSVs through raising the investment when the number of threats increases from 5 to 15, as shown in Figs. 9f and 9g. In this case, we observe that the users' total utilities do not change much accordingly. Furthermore, we observe that the CSSVs' profits are not affected by the increase in the number of threats, even when the investment is increased due to the improvement in the security level of the cloud security service. This due to the fact that the improvement in the security level of cloud security service not only results in the decrease in the probability of paying the claims to the users, but also makes the cloud security plan more attractive to the users. Accordingly, the price of cloud security plan increases as the number of threats increases as shown in Figs. 9d and 9e. This increase in the price of cloud security plan can help to compensate for the cost incurred by the more investment for improving the security level. Additionally, the different levels of interdependency still have an impact on these metrics. However, as observed in Figs. 9f and 9g, the impact of interdependency on the security level of cloud security service is smaller than that of the number of threats. For example, in Fig. 9f, the improvement in the security level between the curves of "Weak Interdependency with 15 threats" and "Weak Interdependency with 10 threats" is larger than that between the curves of "Strong Interdependency with 10 threats" and "Weak Interdependency with 10 threats" for the CSSV-A. The reason is that the number of threats has stronger impact than the interdependency on the users.

In summary, we have evaluated the impact of the number of the users on the performance of the market under our consideration. Therein, the increasing number of the users intensifies the competition between the CSSVs. This results in the lower plan price for CSSV-B while higher plan price for CSSV-A. Moreover, we study the cloud security service market under different security interdependencies. An interesting results can be found that the increasing security interdependency results in different decision behaviors on the security level of the cloud security service for different CSSVs. Furthermore, we compare the performance of the parties in the competitive market with that of the cooperative market. The results imply that in a seller dominant market, the cooperative market can significantly improve the sellers' revenue while extensively exploit the buyers, which is consistent the the real-world scenario.

6 Conclusion

In this paper, we have studied the cloud security service market, where a joint pricing and security investment problem has been investigated. In particular, this problem has been investigated in the framework of a two-stage Stackelberg game. The CSSVs offer the cloud security plan, which is constituted of cloud-insurance and cloud security service, to the users and act as the leaders on the upper stage. The CSSVs lead to decide on their strategies, i.e., the price and the security investment, and the competition between which has been model as a CSSV-level noncooperative subgame on the upper stage. The interaction among the users has been modeled as a user-level noncooperative subgame on the lower stage. Therein, the security interdependency among the users has been incorporated. The equilibrium of the proposed Stackelberg game has been proven to be existence and unique. We have presented extensive numerical results of the proposed game. We will incorporate the reinsurance in the cloud security service market as the future work.

Acknowledgments

This research/project was supported by the National Research Foundation (NRF), Singapore, under Singapore

Energy Market Authority (EMA), Energy Resilience, NRF2017EWT-EP003-041, Singapore NRF2015-NRF-ISF001-2277, Singapore NRF National Satellite of Excellence, Design Science and Technology for Secure Critical Infrastructure NSoE DeST-SCI2019-0007, A*STAR-NTU-SUTD Joint Research Grant on Artificial Intelligence for the Future of Manufacturing RGANS1906, Wallenberg AI, Autonomous Systems and Software Program and Nanyang Technological University (WASP/NTU) under Grant M4082187 (4080), Singapore MOE Tier 2 MOE2014-T2-2-015 ARC4/15, and MOE Tier 1 2017-T1-002-007 RG122/17.

REFERENCES

[1] G. Xu, H. Li, S. Liu, M. Wen, and R. Lu, "Efficient and privacy-preserving truth discovery in mobile crowd sensing systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 3854–3865, Apr. 2019.

[2] CALYPTIX, "Top 5 risks of cloud computing," [Online]. Available: https://www.calyptix.com/research-2/top-5-risks-of-cloud-computing/

[3] I. security, "Cloud security," [Online]. Available: https://www.ibm.com/security/saas

[4] O. C. Security, "Cloud security: A reason to move to cloud," [Online]. Available: https://www.oracle.com/security/index.html

[5] A. Piva, F. Bartolini, and M. Barni, "IEEE internet computing: Issue addendum - managing copyright: Watermark and cryptography algorithms," *IEEE Distrib. Syst. Online*, vol. 3, no. 5, Jan. 2002.

[6] R. Anderson and T. Moore, "Information security economics–and beyond," in *Poc. Annu. Int. Cryptology Conf.*, 2007, pp. 68–91.

[7] M. Lelarge and J. Bolot, "Economic incentives to increase security in the internet: The case for insurance," in *Proc. INFOCOM*, 2009, pp. 1494–1502.

[8] McAfee, "Net losses: Estimating the global cost of cybercrime," Center for Strategic and International Studies, Economic Impact of Cybercrime II, 2014. [Online]. Available: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_McAfee_PDF.pdf

[9] I. T. R. Center and CyberScout, "Identity theft resource center data breach reports," http://www.idtheftcenter.org/2016databreaches.html.

[10] R. Pal, L. Golubchik, K. Psounis, and P. Hui, "On a way to improve cyber-insurer profits when a security vendor becomes the cyber-insurer," in *Proc. IFIP Netw. Conf.*, 2013, pp. 1–9.

[11] P. Naghizadeh and M. Liu, "Opting out of incentive mechanisms: A study of security as a non-excludable public good," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 12, pp. 2790–2803, Dec. 2016.

[12] X. Lu, D. Niyato, H. Jiang, P. Wang, and H. V. Poor, "Cyber insurance for heterogeneous wireless networks," *IEEE Commun. Magazine*, vol. 56, no. 6, pp. 21–27, 2018.

[13] TechTarget, "cloud insurance," 2013. [Online]. Available: http://searchcloudstorage.techtarget.com/definition/cloud-insurance

[14] R. Pal, L. Golubchik, K. Psounis, and P. Hui, "Security pricing as enabler of cyber-insurance a first look at differentiated pricing markets," *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 2, pp. 358–372, Mar. 2019.

[15] AIG, "Cyberedge," 2020. [Online]. Available: https://www.aig.com/business/insurance/cyber-insurance

[16] J. Chase, D. Niyato, P. Wang, S. Chaisiri, and R. Ko, "A scalable approach to joint cyber insurance and security-as-a-service provisioning in cloud computing," *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 4, pp. 565–579, Jul./Aug. 2017.

[17] G. Heal and H. Kunreuther, "Interdependent security: A general model," National Bureau of Economic Research, 2004. [Online]. Available: https://www.nber.org/papers/w10706

[18] S. L. Pfleeger, J. B. Predd, J. Hunker, and C. Bulford, "Insiders behaving badly: Addressing bad actors and their actions," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 169–179, Mar. 2010.

[19] R. J. La, "Interdependent security with strategic agents and cascades of infection," *Biol. Cybern.*, vol. 24, no. 3, pp. 1378–1391, 2016.

[20] C. Ballester, A. Calvó-Armengol, and Y. Zenou, "Who's who in networks. wanted: The key player," *Econometrica*, vol. 74, no. 5, pp. 1403–1417, 2006.

[21] CHUBB, "Cyber enterprise risk management," 2020. [Online]. Available: https://www2.chubb.com/uk-en/business/by-category-computer-risks-cyber-enterprise-risk-management.aspx

[22] Beazley, "Beazley breach response (BBR)," 2020. [Online]. Available: https://www.beazley.com/usa/specialty_lines/professional_liability/technology_media_and_business_services/beazley_breach_response.html

[23] ENISA, "Incentives and barriers of the cyber insurance market in Europe," 2012. [Online]. Available: https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe

[24] B. Filkins, "Quantifying risk: Closing the chasm between cybersecurity and cyber insurance," *SANS Institute*, vol. 3, no. 01, 2016. [Online]. Available: https://www.sans.org/reading-room/whitepapers/leadership/quantifying-risk-closing-chasm-cybersecurity-cyber-insurance-36770

[25] R. Anderson, R. Böhme, R. Clayton, and T. Moore, "Security economics and the internal market," *Study Commissioned ENISA*, 2008. [Online]. Available: https://www.enisa.europa.eu/publications/archive/economics-sec/

[26] T. Bandyopadhyay, "Organizational adoption of cyber insurance instruments in IT security risk management: A modeling approach," in *Proc. Paper*, 2012, vol. 5. [Online]. Available: https://aisel.aisnet.org/sais2012/5/

[27] S. Wang, "Optimal level and allocation of cybersecurity spending: Model and formula," Jul. 2017. [Online]. Available: https://ssrn.com/abstract=3010029

[28] C. Tang and J. Liu, "Selecting a trusted cloud service provider for your SaaS program," *Comput. Secur.*, vol. 50, pp. 60–73, 2015.

[29] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 438–457, 2002.

[30] I. Trusteer, "IBM trusteer fraud protection suite," 2020. [Online]. Available: https://www.ibm.com/sg-en/marketplace/trusteer-fraud-protection-suite/details#product-header-top

[31] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017.

[32] A. Fazeli and A. Jadbabaie, "Duopoly pricing game in networks with local coordination effects," in *Proc. IEEE 51st Annu. Conf. Decis. Control*, 2012, pp. 2684–2689.

[33] X. Gong, L. Duan, X. Chen, and J. Zhang, "When social network effect meets congestion effect in wireless networks: Data usage equilibrium and optimal pricing," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 2, pp. 449–462, Jan. 2017.

[34] Y. Zhang, Z. Xiong, D. Niyato, P. Wang, and J. Jin, "A game-theoretic analysis of complementarity, substitutability and externalities in cloud services," in *Proc. IEEE Global Commun. Conf.*, 2017, pp. 1–6.

[35] X. Gong, L. Duan, and X. Chen, "When network effect meets congestion effect: Leveraging social services for wireless services," in *Proc. 16th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2015, pp. 147–156.

[36] S. A. Gershgorin, "Gershgorin circle theorem," 2020. [Online]. Available: https://en.wikipedia.org/wiki/Gershgorin_circle_theorem

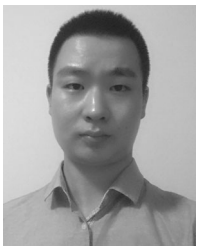
[37] J. B. Rosen, "Existence and uniqueness of equilibrium points for concave n-person games," *Econometrica: J. Econometric Soc.*, vol. 33, pp. 520–534, Jul. 1965.

[38] M. J. Osborne, *An Introduction to Game Theory*, vol. 3, New York, NY, USA, Oxford Univ. Press, Nov. 2004.

[39] G. Scutari, F. Facchinei, J.-S. Pang, and D. P. Palomar, "Real and complex monotone communication games," *IEEE Trans. Inf. Theory*, vol. 60, no. 7, pp. 4197–4231, Jul. 2014.

[40] C. AFRICA, "Cooperative enterprises build a better world," 2012. [Online]. Available: http://www.ilo.org/wcmsp5/groups/public/—ed_protect/—protrav/—ilo_aids/documents/publication/wcms_188624.pdf

[41] G. Debreu, "A social equilibrium existence theorem," in *Proc. Nat. Acad. Sci. United States America*, vol. 38, no. 10, pp. 886–893, 1952.



Shaohan Feng (Student Member, IEEE) received the BS degree from the School of Mathematics and Systems Science, Beihang University, Beijing, China, in 2014, and the MS degree from the School of Mathematical Sciences, Zhejiang University, Hangzhou, China, in 2016. He is currently working toward the PhD degree with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His current research interest includes resource management in cloud computing and communication networks.

Zehui Xiong (Student Member, IEEE) received the BEng degree with honors in telecommunication engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2016. He is currently working towards the PhD degree with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His research interests include network economics, game theory for resource management, market models and pricing.

Dusit Niyato (Fellow, IEEE) received the BEng degree from the King Mongkuts Institute of Technology Ladkrabang (KMITL), Thailand, in 1999, and the PhD degree in electrical and computer engineering from the University of Manitoba, Canada, in 2008. He is currently a professor with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His research interests include the area of Internet of Things (IoT) and network resource pricing.

Ping Wang (Senior Member, IEEE) received the PhD degree in electrical engineering from the University of Waterloo, Canada, in 2008. She is currently an associate professor with the Department of Electrical Engineering and Computer Science, York University, Canada. Before that, she was with Nanyang Technological University, Singapore. Her current research interests include resource allocation in multimedia wireless networks, cloud computing, and smart grid. She was a co-recipient of the best paper awards from the IEEE International Conference on Communications in 2007, from the IEEE Wireless Communications and Networking Conference in 2012, and from IEEE Communications Society (ComSoc) Green Communications & Computing Technical Committee (TCGCC) in 2018. She has been serving as an associate editor for several journals including the *IEEE Transactions on Wireless Communications*, the *EURASIP Journal on Wireless Communications and Networking*, and the *International Journal of Ultra Wideband Communications and Systems*.

Shaun Shuxun Wang received the BS degree from Peking University, China, in 1986, and the PhD degree from the University of Waterloo, Canada, in 1993. He is currently a professor and chair of Finance Department, Southern University of Science and Technology, China. His research interests include financial risk management, economics of information security and data integrity.

Xuemin (Sherman) Shen (Fellow, IEEE) received the BSc degree from Dalian Maritime University, China, in 1982, and the MSc and PhD degrees in electrical engineering from Rutgers University, New Brunswick, NJ, in 1987 and 1990, respectively He is currently a University professor with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. His research focuses on resource management in interconnected wireless/wired networks, wireless network security, social networks, smart grid, and vehicular ad hoc and sensor networks. He was the recipient of the James Evans Avant Garde Award in 2018 from the IEEE Vehicular Technology Society, Joseph LoCicero Award in 2015, and Education Award in 2017 from the IEEE Communications Society. He is a Registered Professional Engineer of Ontario, Canada, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, a Royal Society of Canada fellow, and a distinguished lecturer of the *IEEE Vehicular Technology Society and Communications Society*. He is the editor-in-chief for the *IEEE Internet of Things Journal* and the vice president on publications of the IEEE Communications Society.