Joint Pricing and Security Investment for Cloud-Insurance A Security Interdependency Perspective

Marcharla Prudhvi

Department of Computer Science, Sri Venkateswara University, Tirupati

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 paper, 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. Specially, 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 cloud security service vendors become lower.*

I. INTRODUCTION

1.1 Cloud Computing

Cloud computing is the on-demand availability of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the user. The term is generally used to describe data centres available to many users over the Internet. A simple definition of cloud computing involves delivering different types of services over the Internet. From software and analytics to secure and safe data storage and networking resources, everything can be delivered via the cloud. You can access it from just about any computer that has internet access. cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale. Cloud computing is the delivery of different services through the Internet. These resources include tools and applications like data storage, servers, databases, networking, and software. ... As long as an electronic device has access to the web, it has access to the data and the software programs to run it.

1.2 Types of Cloud Computing

Cloud computing is a broad term which refers to a collection of services that offer businesses a cost-effective solution to increase their IT capacity and functionality. There are three main types of cloud environment, also known as cloud deployment models. The models are.

- *Public cloud*

A public cloud is a type of computing in which a service provider makes resources available to the public via the internet. Some public cloud providers offer resources for free, while clients pay for other resources by subscription or a pay-per-usage model. Public clouds are the most common type of cloud computing deployment. Microsoft Azure is an example of a public cloud. In a public cloud, you share the same hardware, storage and network devices with other organisations or cloud "tenants," and you access services and manage your account using a web browser.

- *Private cloud*

The private cloud is defined as computing services offered either over the Internet or a private internal network and only to select users instead of the general public. Also called an internal or corporate cloud, private cloud computing gives businesses many of the benefits of a public cloud - including self-service, scalability and elasticity - with the additional control and

customisation available from dedicated resources over a computing infrastructure hosted on-premises. In addition, private clouds deliver a higher level of security and privacy through both company firewalls and internal hosting to ensure operations and sensitive data are not accessible to third-party providers.

- *Hybrid cloud*

Hybrid cloud is a solution that combines a private cloud with one or more public cloud services, with proprietary software enabling communication between each distinct service. A hybrid cloud strategy provides businesses with greater flexibility by moving workloads between cloud solutions as needs and costs fluctuate. Hybrid cloud refers to a mixed computing, storage, and services environment made up of on-premises infrastructure, private cloud services, and a public cloud—such as Amazon Web Services (AWS) or Microsoft Azure—with orchestration among the various platforms

There are three main service models of cloud computing. They are

- *IaaS (Infrastructure as Service)*

This is the most common service model of cloud computing as it offers the fundamental infrastructure of virtual servers, network, operating systems and data storage drives. It allows for the flexibility, reliability and scalability that many businesses seek with the cloud, and removes the need for hardware in the office. This makes it ideal for small and medium sized organisations looking for a cost-effective IT solution to support business growth. IaaS is a fully outsourced pay-for-use service and is available as a public, private or hybrid infrastructure.

- *PaaS (Platform-as-a-Service)*

This is where cloud computing providers deploy the infrastructure and software framework, but businesses can develop and run their own applications. Web applications can be created quickly and easily via PaaS, and the service is flexible and robust enough to support them. PaaS solutions are scalable and ideal for business environments where multiple developers are working on a single project. It is also handy for situations where an existing data source (such as CRM tool) needs to be leveraged.

- *SaaS (Software as a Service)*

This cloud computing solution involves the deployment of software over the internet to various businesses who pay via subscription or a pay-per-use model. It is a valuable tool for CRM and for applications that need a lot of web or mobile access – such as mobile sales management software. SaaS is managed from a central location so businesses don't have to worry about maintaining it themselves, and is ideal for short-term projects.

1.3 Cloud Services Benefits

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 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. To address such security problems, many cloud security service vendors (cssvs), e.g., ibm security and oracle, 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, completely securing the cyber space still remains as an open research field.

1.4 Problem Analysis in Investment

The financial losses due to the cyber risks were estimated by McAfee to be between USD 300 billion and USD 1 trillion in 2014. There were 873 recorded breaches in the US with over 29 million records exposed for November 2016, indicated by the Identity Theft Resource Centre's 2016 data breach category summary.

In this regard, an economic tool, i.e., cyber-insurance, has been introduced to enable effective cyber risk management. 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. 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 adopted in the literature such as. 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, which will affect the decision making of the CSSV and further the corresponding profit.

II. EXISTING SYSTEM

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. 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. The users are interdependent in which they can take advantage of the positive security effects generated by other users' investments in security. We assume that the cloud provider and cloud-insurer are the business partners. Therefore, the cloud-insurers can invest in the cloud platform to improve the security level of the cloud service.

Disadvantages:

- To protect from the damage, the users can buy a cloud-insurance product from the cloud-insurers which will pay a claim to the users if an attack happens to the cloud service.
- Security and the performance is low.
- There is no cyber security solution can completely remove the risks faced by the users

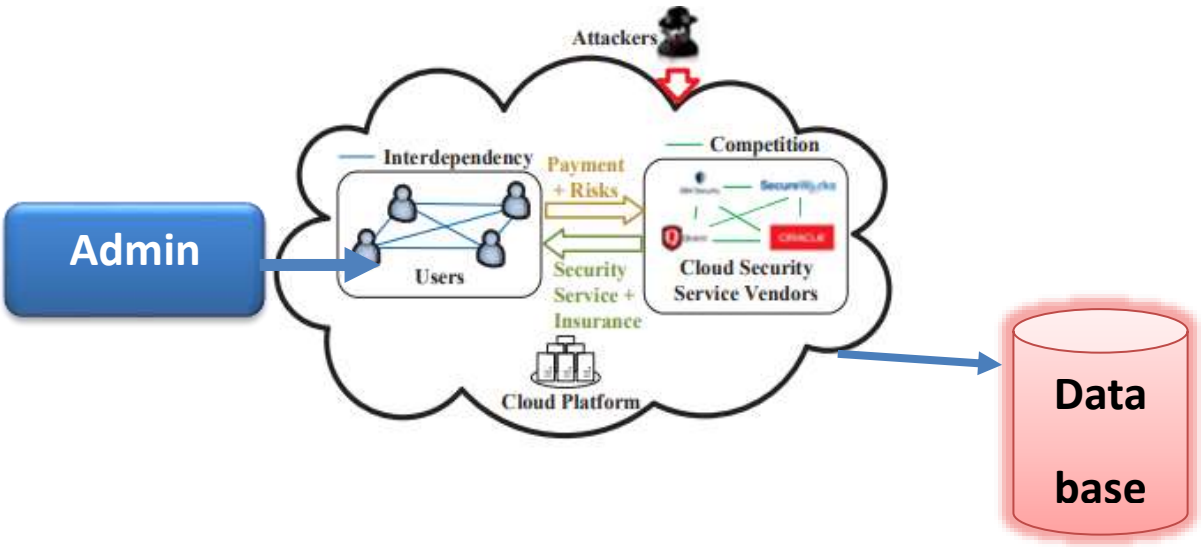
III. PROPOSED SYSTEM

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. Identified and authorized for data access based on their recognizable identities, which avoids complicated certificate management in usual secure distributed systems. More importantly, IBET provides a transformation mechanism that converts an IBE ciphertext into an IBBE ciphertext so that a new group of users not specified during the IBE encryption can access the underlying data. Thorough theoretical and experimental analyses demonstrate the high efficiency and practicability of the proposed scheme.

Advantages:

- They can take advantage of the positive security effects generated by other users' investments in security.
- High security and more effective.
- The performance of the cloud should be high and the user friendly.

IV. SYSTEM ARCHITECTURE



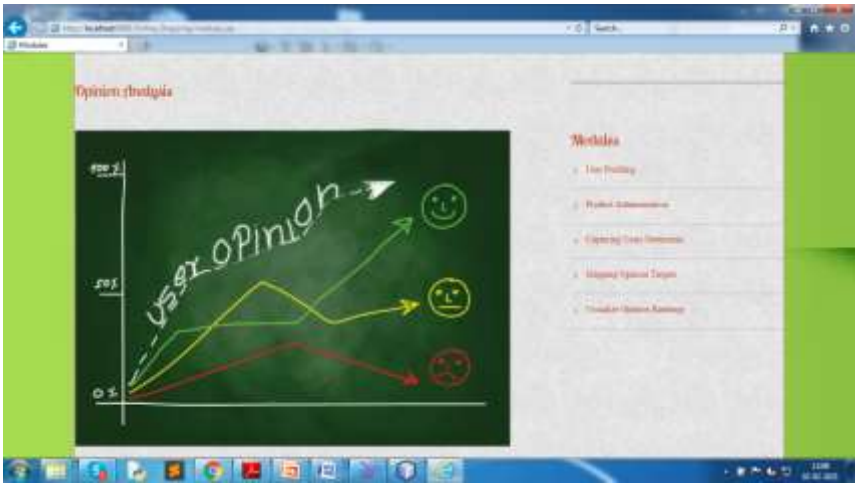
Applications:

This security plan has implemented in android application. this method is also implemented to the bank Health Insurance, Medical insurance also use this method to make the plans, EMI, loans etc.

V. FUTURE ENHANCEMENT:

In this cloud plan, security services and the insurance may have future plans. We will incorporate the reinsurance in the cloud security service market as the future work. The user can make the opportunity to make the reinsurance.

HOME:

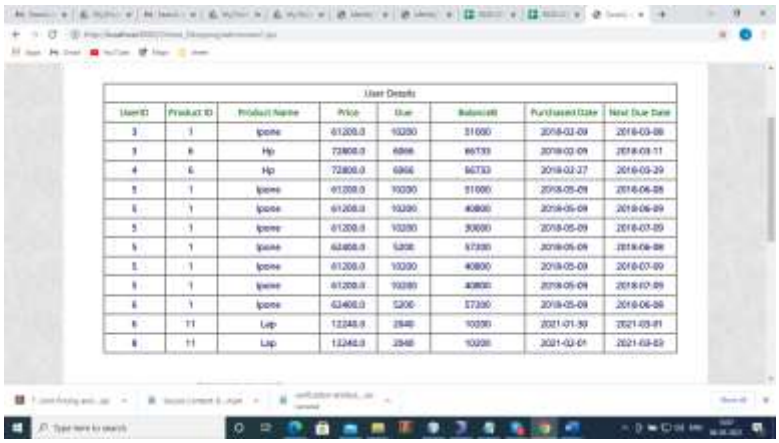


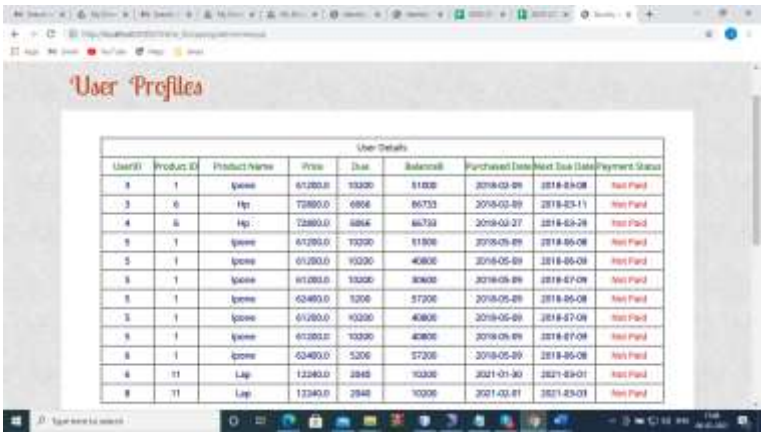

Welcome
BUSINESS
ADMINISTRATION
functions
performance
organizations
directing
elements
derived
goals
admin
man


Product Category
Laptop
Product Name
Price
Product Model
Date of Deploy
Choose file

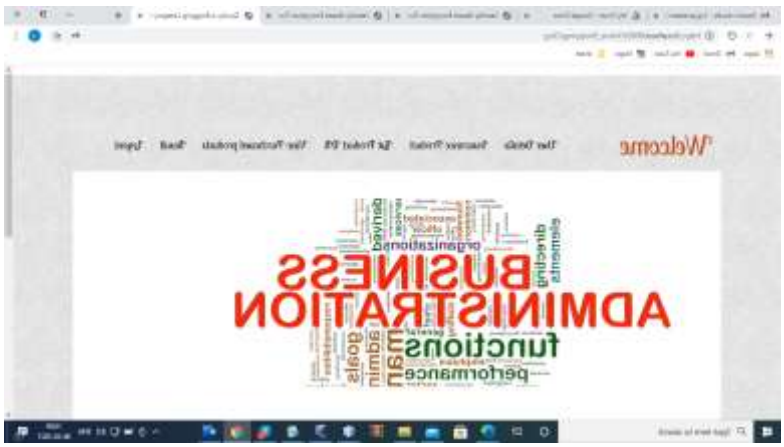

Product DB


User Profiles
User Details



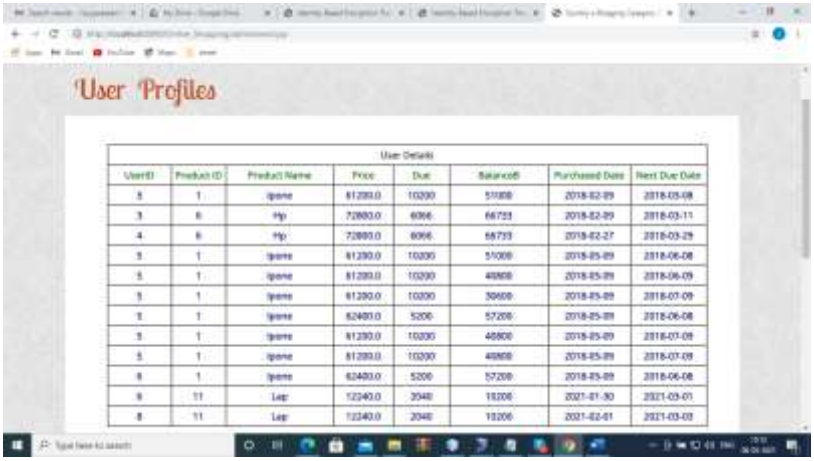

User Profiles

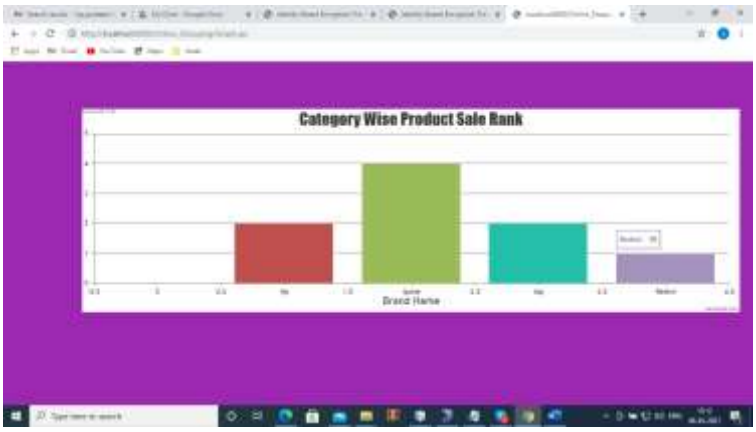
Cloud:


Welcome
BUSINESS
ADMINISTRATION
functions
performance


Insurance Products

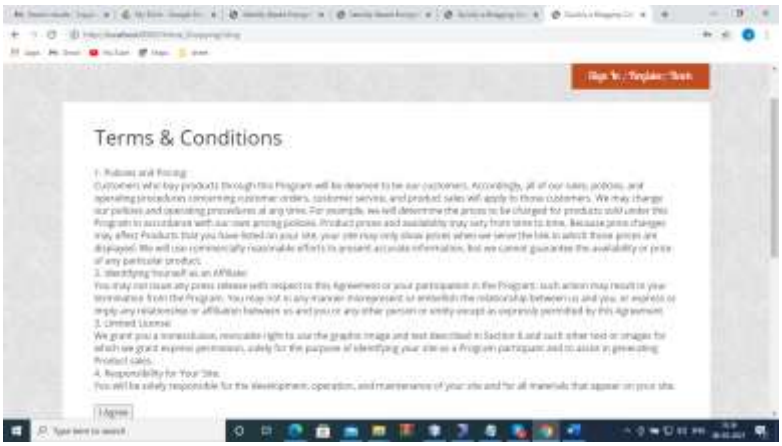

Insurance Products

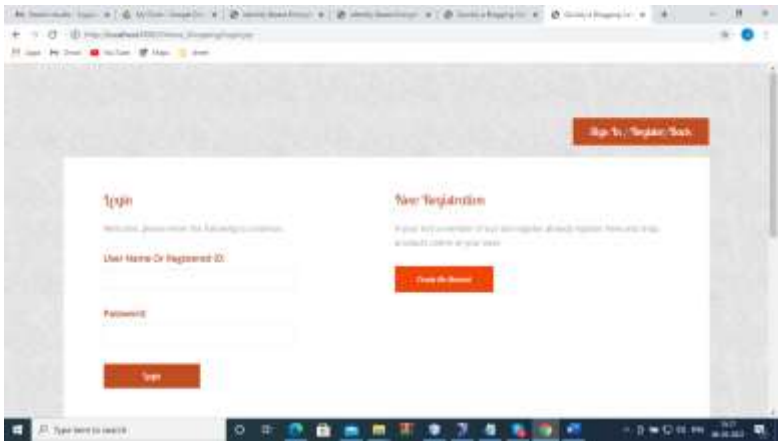

User Profiles
User Details



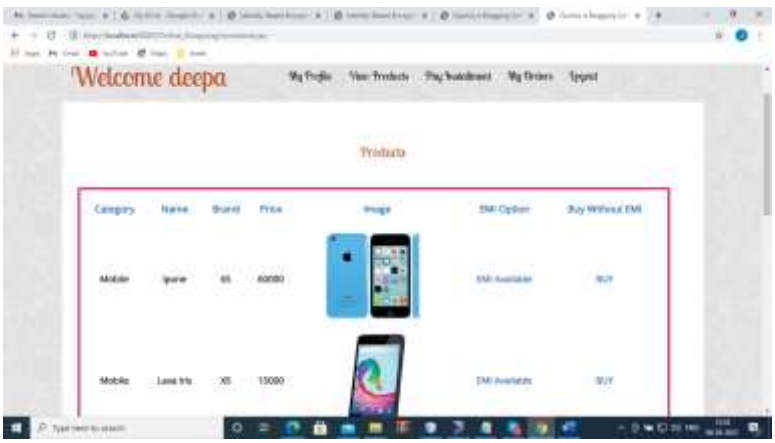
Attacker:

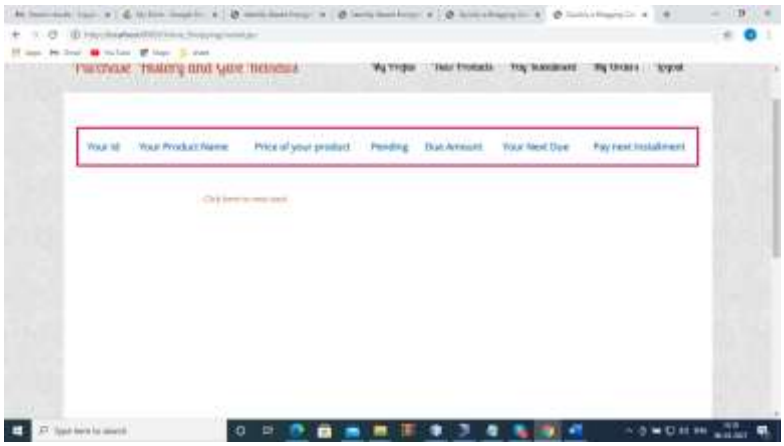
User:






Welcome DEEPA
Categories
New Chatharam


Welcome deepa
Products
Category
Name
Brand
Price
Image
EMI Option
Buy Without EMI



VI. CONCLUSION

Finally, 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 modelled 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.

REFERENCES

[1] R. Pal, L. Golubchik, K. Psounis and P. Hui, "On a way to improve cyber-insurer profits when a security vendor becomes the cyberinsurer," in IFIP Networking Conference. IEEE, May 2013, USA, pp. 1–9.

[2] S. Yu, C. Wang, K. Ren, and W. Lou, ''Achieving secure, scalable, and fine-grained data access control in cloud computing,'' in Proc. IEEE INFOCOM, Mar. 2010, pp. 525–533.

[3] B. Ferreira, J. Rodrigues, J. Leitao, and H. Domingos, ''Privacy-preserving content-based image retrieval in the cloud,'' in Proc. IEEE 34th Symp. Reliable Distrib. Syst. (SRDS), Sep. 2015, pp. 11–20.

[4] K. Liu, C. Giannella, and H. Kargupta, ''An attacker's view of distance preserving maps for privacy preserving data mining,'' in Proc. PKDD, Berlin, Germany, 2006, pp. 297–308

[5] 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 Transactions on Dependable and Secure Computing, 2017

[6] B. Filkins, "Quantifying risk: Closing the chasm between cybersecurity and cyber insurance," SANS Institute, available via https://www. sans. org/readingroom/whitepapers/leadership/quantifying-risk-closing-chasmcybersecurity-cyber-insurance-36770 on, vol. 3, no. 01, pp. 2017, 2016.

[7] R. Anderson, R. Bohme, R. Clayton and T. Moore, "Security ¨ economics and the internal market," Study commissioned by ENISA, 2008.

[8] Y. Zhang, Z. Xiong, D. Niyato, P. Wang and J. Jin, "A gametheoretic analysis of complementarity, substitutability and externalities in cloud services," in GLOBECOM 2017-2017 IEEE Global Communications Conference. IEEE, 2017, pp. 1–6.