The Effect of Consumer Portfolio on the Risk Profile of Cloud Provider

Muhammad Yasir Muzayan Haq
University of Twente
The Netherlands
m.y.m.haq@utwente.nl

Abhishta Abhishta
University of Twente
The Netherlands
s.abhishta@utwente.nl

Lambert J.M. Nieuwenhuis
University of Twente
The Netherlands
l.j.m.nieuwenhuis@utwente.nl

ABSTRACT

The economies-of-scale model of Cloud services has brought many financial and technical benefits for organizations. However, recent events like the attack on Dyn and GitHub have shown that successful attacks on big Cloud providers can cause a massive impact on a major portion of the Internet ecosystem. In this project, we will study how the consumer portfolio of a Cloud provider may affect its risk profile. We will use the result to develop a recommender system for choosing a Cloud provider based on consumer security and business requirements. Insights from our research can be used to simulate an alternative more secure market structure for the Cloud ecosystem. We invite fellow researchers to further discuss this idea and possible collaboration.

CCS CONCEPTS

• **Security and privacy** → **Distributed systems security**; • **Computer systems organization** → **Cloud computing**; • **Social and professional topics** → **Offshoring**.

KEYWORDS

Cloud, Security, Oligopoly, Cyber Attacks, Decision Support System

1 INTRODUCTION

In recent years, Cloud outsourcing has been the go-to option for many organizations due to its economic and technical benefits, such as, cost efficiency, scalability, and flexibility [4]. Cloud services are based on a massive computing infrastructure which is rented as smaller chunks to the consumers. They can be categorized into several types based on provided services and deployment models. Each type has a different price scheme, privacy, and security level. More secure and privacy preserving Cloud services are usually more expensive. But, is Cloud outsourcing always the most secure option?

Many people believe that moving to Cloud is beneficial for several reasons. However, recent internet outages have shown that distributed systems are not immune to cyber attacks [2]. The likelihood of attack on the Cloud is also a consequence of its economies-of-scale model i.e., sharing a single infrastructure to multiple consumers. Intuitively, the more consumers use the same infrastructure, the more resources does a Cloud provider has to invest in protection, however, also bigger is the impact, once an attack is successful. Therefore, we require a more systematic way for organizations to choose a Cloud service that is suitable for a specific need while maintaining/decreasing the risk posed by cyber attacks. We present a model that will be used to develop a recommender system based on empirical analysis on attack data to help organizations make this decision. We consider both consumer security and business requirements to suggest the appropriate profile of the Cloud provider. Furthermore, we want to study different market scenarios for Cloud ecosystem to propose a more secure Cloud market structure.

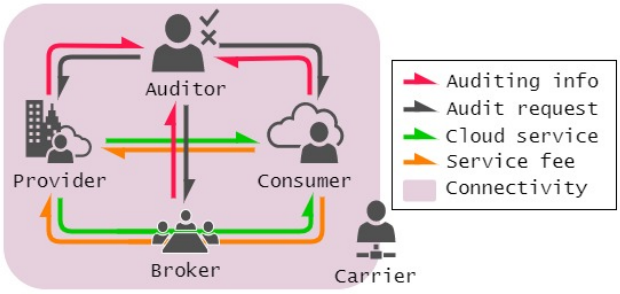

Figure 1: Key stakeholders in Cloud ecosystem.

The aim of this poster is to invite further discussion from the fellow researchers and to initiate collaboration. In the next sections, we discuss the methodology chosen by us to develop the proposed recommender system and expected outcomes of our research. We do this by identifying the key stakeholders involved in the Cloud ecosystem, the risks in Cloud, and its contributing factors.

There are five **key stakeholders** in the Cloud ecosystem [8]. Figure 1 depicts the business relationship between these stakeholders. Cloud consumers and providers can use service from a Cloud broker as an intermediary to manage, sell, and negotiate service agreements. A Cloud auditor is responsible to conduct auditing activity in Cloud operation and keep a check over the involved parties. Meanwhile, a Cloud carrier provides connectivity to enable communication and service exchange between the parties.

Like other IT systems, Cloud outsourcing also brings along several risks, including security risk. In our research we define risk as the expected loss due to a successful cyber attack. According to

SIGCOMM '21 Demos and Posters, August 23–27, 2021, Virtual Event, USA

ACM ISBN 978-1-4503-8629-6/21/08.
https://doi.org/10.1145/3472716.3472851

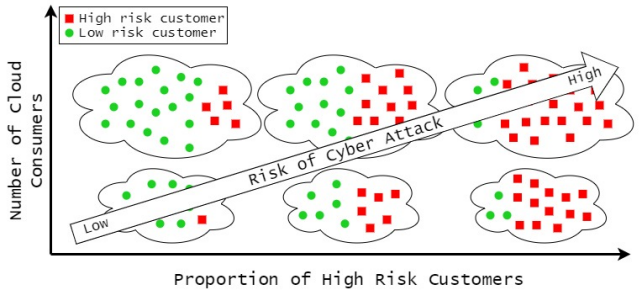

Figure 2: Riskiness of Cloud service providers based on their consumer portfolio.

Gordon and Loeb [6] expected loss can be quantified as shown in Equation (1), where v is the probability of success of an attempted attack, t is the probability of an attempted attack to a specific target, and λ is the potential loss in terms of value of the information set if no security measures are in place.

In our research, we focus on helping organizations in minimizing the threat (t) of a cyber attack by improving the Cloud outsourcing process using a recommender system. **Probability of attack (t) on a Cloud** is dependent on its resource pooling characteristic which is closely related to the consumer portfolio of a Cloud provider, i.e., who are its consumers, how many of them and how often do they get attacked as shown in Figure 2.

$$L = v \times \underbrace{t}_{\text{probability of attack}} \times \lambda \quad (1)$$

Geer et.al. [5] showed that Cloud market concentration influences all three aspects in security risk (i.e., threat, vulnerability, and impact). Studies have also shown that organizations in some industry sectors are subject to more cyber attacks than the others [10]. This implies, a Cloud consumer might possess a higher probability of becoming a collateral damage when they use a service from a Cloud provider that is a vendor for organizations with a greater likelihood of attacks. Consequences of such a scenario were faced by customers of DNS service provider, Dyn, which was originally aimed to take down Sony PlayStation Network's gaming platform [2, 3, 7].

Therefore, we hypothesize that both number and profile of Cloud consumers contribute to the level of cyber threat of a Cloud provider [10]. To test this hypothesis, we will use measurement based empirical approach to study attack incidents data with industry sector information of the attacked targets. In addition, we will use the results to develop a recommender system and conduct a simulation study of different Cloud market scenarios that would decrease the riskiness of the entire market.

2 ANALYSIS AND RESEARCH OUTPUTS

In order to quantify threat we will analyze the following two parameters in this research: 1) *the distribution of attacks across different consumer sectors*, and 2) *the distribution of attacks across different sizes of Cloud provider*. Using both parameters, we aim to quantify

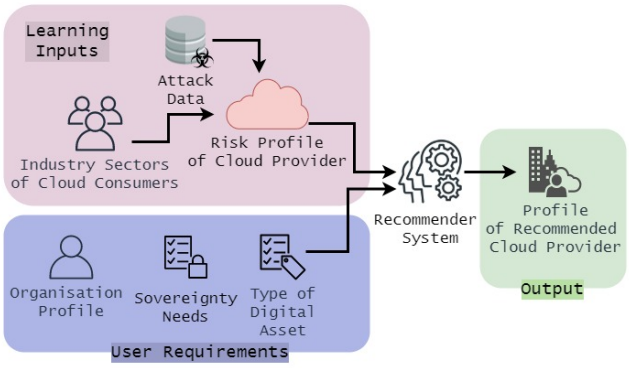

Figure 3: A model for a Cloud service provider recommender system.

the level of threat of a certain Cloud service provider based on its consumer portfolio. For this purpose, we will use a dataset of attack events (e.g.,[1], [7]) which includes the domain names [11] and the URL categories [9] of the attacked targets.

Using conclusions from the empirical analysis on attack data, we will develop a **recommender system** prototype for Cloud consumers to help them choose the best Cloud provider for their digital assets. The system will analyze user requirements (e.g., organization profile, sovereignty needs, and types of digital asset) and suggest characteristics (e.g., size and consumer portfolio) of appropriate Cloud provider for them as shown in Figure 3.

Using the quantified levels of threat for various consumer portfolios we will study how different Cloud market scenarios affect the cyber threat distribution. We will use this information to build a simulation model of Cloud market which can be used to propose a Cloud market structure with lower security risk.

3 CONCLUSION

In this poster, we present a methodology to analyze the effect of consumer portfolio on risk profile of a Cloud provider. Using a measurement based empirical approach, we aim to develop a recommender system and later simulate alternative market scenarios for a more secure Cloud ecosystem. The purpose of this poster is to invite fellow researchers to discuss possible collaboration.

ACKNOWLEDGMENTS

This work is funded by the Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) MeAsuring Security in Cloud OuTsourcing (MASCOT) project.

REFERENCES

[1] Abhishta Abhishta. 2019. *The Blind Man and The Elephant: Measuring Economic Impacts of DDoS Attacks.* Ph.D. Dissertation. University of Twente, Netherlands. https://doi.org/10.3990/1.9789036549127

[2] A. Abhishta, R. Van Rijswijk-Deij, and L.J.M. Nieuwenhuis. 2018. Measuring the impact of a successful DDoS attack on the customer behaviour of managed DNS service providers. *Computer Communication Review* 48, 5 (2018), 70–76. https://doi.org/10.1145/3310165.3310175 cited By 0.

[3] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis Kallitsis, et al. 2017. Understanding the mirai botnet. In *26th {USENIX} security symposium ({USENIX} Security 17).* 1093–1110.

[4] M. Carroll, A. Van Der Merwe, and P. Kotzé. 2011. Secure cloud computing: Benefits, risks and controls. https://doi.org/10.1109/ISSA.2011.6027519

[5] Dan Geer, Eric Jardine, and Eireann Leverett. 2020. On market concentration and cybersecurity risk. *Journal of Cyber Policy* 5, 1 (Jan. 2020), 9–29. https://doi.org/10.1080/23738871.2020.1728355 Publisher: Routledge _eprint: https://doi.org/10.1080/23738871.2020.1728355.

[6] Lawrence A. Gordon and Martin P. Loeb. 2002. The economics of information security investment. *ACM Transactions on Information and System Security* 5, 4 (Nov. 2002), 438–457. https://doi.org/10.1145/581271.581274

[7] Mattijs Jonker, Alistair King, Johannes Krupp, Christian Rossow, Anna Sperotto, and Alberto Dainotti. 2017. Millions of targets under attack: a macroscopic characterization of the DoS ecosystem. In *Proceedings of the 2017 Internet Measurement Conference (IMC '17)*. Association for Computing Machinery, New York, NY, USA, 100–113. https://doi.org/10.1145/3131365.3131383

[8] Fang Liu, Jin Tong, Jian Mao, Robert B. Bohn, John V. Messina, Mark L. Badger, and Dawn M. Leaf. 2011. NIST Cloud Computing Reference Architecture. (Sept. 2011). https://www.nist.gov/publications/nist-cloud-computing-reference-architecture Last Modified: 2018-11-10T10:11-05:00.

[9] Srdjan Matic, Costas Iordanou, Georgios Smaragdakis, and Nikolaos Laoutaris. 2020. Identifying Sensitive URLs at Web-Scale. In *Proceedings of the ACM Internet Measurement Conference (IMC '20)*. Association for Computing Machinery, New York, NY, USA, 619–633. https://doi.org/10.1145/3419394.3423653

[10] Arman Noroozian, Maciej Korczyński, Carlos Hernandez Gañan, Daisuke Makita, Katsunari Yoshioka, and Michel Van Eeten. 2016. Who gets the boot? analyzing victimization by ddos-as-a-service. In *International Symposium on Research in Attacks, Intrusions, and Defenses*. Springer, 368–389.

[11] Roland van Rijswijk-Deij, Mattijs Jonker, Anna Sperotto, and Aiko Pras. 2016. A High-Performance, Scalable Infrastructure for Large-Scale Active DNS Measurements. *IEEE Journal on Selected Areas in Communications* 34, 6 (June 2016), 1877–1888. https://doi.org/10.1109/JSAC.2016.2558918 Conference Name: IEEE Journal on Selected Areas in Communications.