A Game Theory Method to Cyber-threat Information Sharing in Cloud Computing Technology

L. M. Muthulakshmi

Department of Computer Science,Auxilium College of Arts and Science for Women, Pudukkottai, India

*Corresponding author: ramamoorthy260679@gmail.com

ABSTRACT

Industry, academic, and government institutions place a high importance on cyber security, and information exchange regarding cyber threats among them has the potential to maximize vulnerability identification while reducing cost. The likelihood that an attacker will use the same vulnerability to launch multiple attacks on various organizations can be decreased by sharing information about cyber threats. It can also reduce the possibility that an attacker will compromise an organization and gather information to launch attacks on other organizations. Due to their own self-interests, businesses may not disclose information honestly in this strategic context. Additionally, if all participants use the same approach, some businesses may reduce their investment in cyber security and rely on information supplied by others, leading to underinvestment in the field. This essay investigates the using game theory. In order to investigate the conditions under which several self-interested businesses can invest in vulnerability discovery and share their cyber-threat information, this research applies game theory. We use a public cloud computing platform, one of the cyberspace sectors that is expanding the fastest, to implement our method.

Keywords: Game Theory, Information Sharing, Innovation Adoption

DOI: 10.21467/abstracts.158 ISBN: 978-81-965621-0-6 (eBook)