# DDoS attacks detection in the cloud using K-medoids algorithm

SeongHo Yoon, Miyoung Kang

School of Cybersecurity, Korea University, Seoul 02841, Korea

**shyoon17@korea.ac.kr, dasuni@korea.ac.kr**

*Abstract*— **A denial of service (DoS) attack means that users cannot use a device or access server or network resources due to malicious cyber threats by an attacker, and Distributed Denial of Service (DDoS) attack is that several zombie PCs attack in the form of DoS. DDoS attacks are increasing daily, and DDoS attacks on the cloud are also growing. In this paper, since IDS/IPS operating outside the cloud does not recognize the inside, we propose a model to detect DDoS attacks by checking network traffic using the K-medoids algorithm, one of the clustering algorithms.**

*Keyword*— **DDoS, Clustering, Cloud Computing, Security, TCP/IP**

**Seong Ho Yoon** received B.S. degree from the School of Computer Engineering, Dongguk University, Korea in 2020. He is currently an M.S. candidate in the School of Cybersecurity, Korea University. His current research interests are in Network Security and secure software engineering.

**Miyoung Kang** received the M.S. degree in the Department of Computer Science and Engineering at Dongguk University and the Ph.D. degree in the Department of Computer Science and Engineering at Korea University, Seoul, Korea. She is a research professor at the graduate school of Sybersecurity at Korea University, Seoul, Korea. Her research interests are Formal Methods, process algebras, software-defined networking (SDN), and security in networks.