A Lightweight Block Cipher Algorithm for Secure SDN Environment

Jungha Jin
Dept. of Computer Engineering
KONKUK University
Seoul, 05029, Korea
drake75@konkuk.ac.kr

Yewon Oh
Dept. of IT Convergence Information Security
KONKUK University
Seoul, 05029, Korea
iamoyw@konkuk.ac.kr

Keecheon Kim
Dept. of Computer Engineering
KONKUK University
Seoul, 05029, Korea
kckim@konkuk.ac.kr

***Abstract*— Software Defined Network is a next-generation networking technology that transforms a closed network environment based on existing network vendors into a flexible, software-based, centralized management environment that can be simplified by abstracting and programming. Although these advantages can be applied to some security problems rather than existing networks, most of the security problems and vulnerabilities of existing networks are present and various attacks are taking place. In this paper, we propose a structure to enhance the security function of SDN by checking how to implement the network security function using SDN technology and lightening the existing block cipher algorithm for this security problem. Lightweight-AES algorithm, which is a lightweight block cipher algorithm based on the AES-256 algorithm, which can simultaneously satisfy the quality of high level of security. In the case of simply reducing the number of round operations of the AES algorithm, the difference diffusion effect of the KeySchedule function generating the round key is reduced, and the security of the encryption algorithm is degraded due to the related key attack using the related key difference characteristic. The Lightweight-AES algorithm proposed in this paper improves the rate of cancellation and decryption by reducing the number of round operations, and the round internal function is supplemented to increase the differential diffusion effect of the KeySchedule function. In order to evaluate the performance of the Lightweight-AES algorithm proposed in this paper, a comparison simulation is performed with the existing AES algorithm. As a result, we confirmed that the Lightweight-AES algorithm can provide SDN content security equal to the encryption / decryption rate and algorithm security strength of the AES-128 algorithm. Therefore, it is considered that the proposed Lightweight-AES algorithm can provide better security service in SDN environment quality and security than the existing AES-128 algorithm.**

***Index Terms*—SDN, Block cipher algorithm, AES-256, Related Key Attack, Avalanche Effect**