NVLC: New Variant Lightweight Cryptography Algorithm for Internet of Things

Seddiq Q. Abd Al-Rahman
College of Computer
Sciences and Information Technology
University Of Anbar
Anbar, Iraq
co.sedeikaldossary@uoanbar.edu.iq
ORCID: 0000-0002-6917-7352

Ali Makki Sagheer
Al-Qalam University College
Kirkuk, Iraq
prof.ali@alqalam.edu.iq

Omar A. Dawood
Computer Science Department
College of Computer
Sciences and Information Technology
University Of Anbar
Anbar, Iraq
the_lionofclub@yahoo.com
Omar-Abdulrahman@uoanbar.edu.iq
ORCID: 0000-0003-3276-602X

***Abstract*—The rapid industrial and technological development along with the continues need to improve lifestyle have led to the emergence of the Internet of Things (IoT) as a service. Due to its nature, there are a huge amount of data been transmitted over IoT in every minute. Considering security aspects of such a huge data, with limited resources including bandwidth and energy, requires an innovative way of securing such as data driven environment. This study aims to propose a low-cost encryption algorithm (NVLC) to handle a low-cost Radio-frequency Identification (RFID) tags and sensors within IoT environment. NVLC is a symmetric block cipher with a 64-bit block size data and 80-bit/128-bit for the secret key. Although 6 rounds of NVLC is enough to maintain data security, however, we are applying 20 rounds to increase data security and complexity of decryption. This paper uses a substitution-permutation network within NVLC as a uniform architecture of cryptography. NVLC has been designed and implemented using a combination of mathematical and logical and methods considering the requirement of IoT lightweight devices and infrastructure. The proposed cipher was shown the security evaluation, software, and hardware experiments to it, and**

things act as bridges between the physical and computing worlds, and (2) the nature of objects makes the scope of attacks greater [3]. The attention of security and privacy are the main concern to trust the devices as they are connected to the Internet. Hackers could access many devices and data knowledge, which requires companies to focus on electronic security devices [4]. Researchers have sought ways to secure data within their industrial boundaries in a lightweight and safe manner. Lightweight encryption is a junction of two terms "Light and weight". Lightweight encryption is a sector of a classical cryptographic algorithm that is pertinent for resource-constrained devices in IoT. In addition, lightweight encryption and decryption are implemented on platforms as well as hardware and software [5].

Lightweight cryptographic model was an algorithm tailored for implementation in limited environments as RFID tags, sensors, smart cards, health-care devices and so on. However, the aim of applied lightweight cryptography is to