International Journal of Advanced Science and Technology
Vol. 29, No. 05, (2020), pp. 10520 - 10530

A Study on Light-Weight Cryptographic Methods Providing High Data Security in Cloud

Nagababu Garigipati[1], Dr. V. Krishna Reddy[2]

[1]*Research Scholar,* [2]*Professor*

[1,2]*Department of Computer Science and Engineering, KoneruLakshmaiah Educational Foundation, Vaddeswaram, AP, India*

[1]*nag.garigipati@gmail.com,*[2]*vkrishnareddy@kluniversity.in*

Abstract

With the emergence of cloud computing, organizations changed their strategy in data storage and computations. Instead of investing on the computing resources, they prefer outsourcing their data to cloud. However, they are concerned about data security in the untrusted area. Thus data security in cloud has become an important research area due to its wide usage and the sources from which it is generated. Traditional cryptographic methods like RSA are heavy weight and not desirable for protecting data in the wake of quantum computers. Therefore, it is essential to explore cryptographic primitives that are lightweight yet provide stronger security. Data is often outsourced to Infrastructure as a Service (IaaS) layer of public cloud. There is need for protecting the data when it is at rest, when it is in transit and also when it is being processed in distributed environments. In this paper, we reviewed the present state of the art pertaining to data security and particularly focused on lightweight security primitives. It provides useful insights on different aspects of data security including methods used to secure data, lightweight cryptographic methods, hash based methods, hybrid approaches. It also provides research gap found the existing cryptographic methods used for data security in cloud computing.

Keywords *–Data security, cryptography, lightweight cryptography, cloud computing*

1. INTRODUCTION

Enterprises in the real world are giving much importance to maintaining data of every aspect related to business. This data is growing faster in volume and needed outsourced to public cloud.Data is asset to an organisation and it needs to be protected. Providing security to such data is challenging as it is originated from different sources and generally outsourced to cloud which is untrusted environment. Many researchers contributed in using and building security schemes. Traditional encryption schemes like DES and RSA are found to be heavy weight and not appropriate for the bulk of data [6]. Many lightweight cryptographic primitives came into existence as explored in [1], [5], [7], [8], [10]. Lightweight hash functions are also used in studied in [13], [14]. There are latest security frameworks on data security [53], [54], [55], [56], [57]. In [53], the focus is on securing data when it is being processed. In [54], stream security classification is made pertaining to IoT applications. In [55] and [56] lightweight security is discussed for IoT environments while [57] provides an overview of data privacy and security. Elliptic Curve Cryptography (ECC) is found to be a lightweight security solution to protect large volumes of data [46]. It is also found that the combination of ECC and Diffie-Hellman (EC-DH) [52] provides more lightweight alternative for data security where the data is originated by resource constrained IoT devices. This paper provides the current academic thinking on the security to data focusing more on the lightweight cryptographic solutions. It also provides research gaps identified besides giving valuable insights on data security.

Our contribution in this paper is the survey of literature on cryptographic techniques used to secure data outsourced to cloud including their utility and research gaps. The remainder of the paper is structured as follows. Section provides review on lightweight cryptographic primitives. Section 3 presents security mechanisms used to protect data. Section 4 reviews on the cryptographic techniques for cloud storage security. Section 5 provides hash function based security for cloud data. Section 6 presents a hybrid approach for data security. Section 7 provide valuable insights on research gaps while section 7 concludes the paper and provides directions for future work.

ISSN: 2005-4238 IJAST