Management of Symmetric Cryptographic Keys in Cloud Based Environment

Faiza Fakhar*, Muhammad Awais Shilibi*

**Department of Computing, School of Electrical Engineering and Computer Science, NUST, Islamabad, Pakistan*

10msitffakhar@seecs.edu.pk , awais.shibli@seecs.edu.pk

Abstract— Although, cloud computing provides innumerable benefits to its customers but it fails to solve information security concerns especially in public cloud. Symmetric Cryptographic Key is sensitive data and it is required to be stored at cloud platform to solve several problems of encrypted data such as searching/manipulation on encrypted data. This paper presents a technique that will manage symmetric cryptographic keys on cloud-based environment. Proposed technique is based on secret splitting technique enhanced Shamir's algorithm. Proposed technique is implemented in OpenStack private cloud environment for performance analysis and it is found out that the technique works efficiently. Furthermore, it is fulfilling the best practices metrics, given by National Institute of Standard and Technology.

***Keyword*— Public Key Cryptographic Standard (PKCS7),Public Key Infrastructure (PKI); Cryptographic Key Management (CKM), National Institute of Standard &Technology (NIST), Secure Shell (SSH).**

F. Fakhar is doing graduate from School of Electrical Engineering and Computer Science, NUST, Pakistan. Her field of research is information security in cloud computing.

M. A. Shibli finished his PhD from Department of Communication Systems (COS) KTH Sweden. During and before his PhD studies he authored in fifteen publications in the area of security for distributed systems published in international conferences and journals, such as IEEE. He is currently working as Assistant Professor at School of Electrical Engineering and Computer Sciences (SEECS-NUST). His current area of research is security in open distributed systems.