

299. HOMOMORPHIC ENCRYPTION USED IN REAL TIME APPLICATION-MEDICAL INDUSTRY

R.Krithiga¹, S.MohamedSaleem.S², Celin Sindhya³, P.Nirmala Deve⁴

Department of Computer Science and Engineering, Valliammai Engineering College

Kattankulathur, Chennai, India

¹rkritthigarajesh@gmail.com, ²mohamedsaleem25@gmail.com, ³sidhyacelin@gmail.com,

⁴nirmalasp@gmail.com

Abstract—Homomorphic encryption is the encryption techniques, which operates on the encrypted data in the computing domain, particularly in cloud computing. Homomorphic encryption can be applied in any pattern by using various public key algorithms and it provides a means for information across in a computing domain. The aim of the paper is focus on the concepts and various principles of homomorphic encryption. We have developed a proof of algorithm that demonstrates a practical use for a homomorphic encryption technique, the results of our algorithm are provided, such as RSA, Paillier, Benaloh's scheme, Damgared-jurile, EL-Gamal are explored.

Index Terms—Cryptography, Homomorphic Encryption, Paillier algorithm, RSA, Benaloh's, Damgared-jurile.

Journal of Science and Innovative Engineering & Technology