Notification No.: F.NO. COE/Ph.D./(Notification)/248/2023

Date of Award: 06/11/2023

Name of the Ph.D. Scholar:	**Shahnawaz Ahmad**
Name of the Supervisor:	Prof. Shabana Mehfuz
Department:	Department of Electrical Engineering, Faculty of Engineering and Technology, Jamia Millia Islamia, New Delhi-110025, India
Ph.D. Topic:	**Securing Cloud Based Encryption Key Management Platform**

Ph.D. Research Findings

To the best of our knowledge, the work presented in this thesis is the first attempt in which KMS has been intertwined with the cloud environment so that only authorized CSC can access sensitive data securely with the encryption mode of KMS. This thesis has presented solutions for the problem of KMS in a cloud environment. To accomplish this task, several KMS schemes have been presented here in this thesis. There are four main contributions in the present Thesis which are summarized as follows:

- Proposal of a Cloud security framework and key management services collectively for implementing DLP and IRM are proposed for enhancing Cloud Data Security. In this research work, policies for CSF for securing KMS have been proposed for enhancing Cloud Data Security.
- A Hybrid cryptographic approach to enhance the mode of key management system in a cloud environment has been proposed for enhancing Cloud Data Security. The proposed algorithm (HCA-KMS) has been able to overcome the issue of key exchange that plagues AES, simpler than ECC and more reliable than AES. As a result, KMS has been designed to provide high levels of security for healthcare information.
- An Efficient Time-Oriented Latency-Based Secure Data Encryption for Cloud has been implemented and the efficiency of this method has been estimated with the help of several performance metrics like QoS factors, Traffic-Throughput-Latency QoSV Estimation, Time-Oriented Latency (TLE) Approximation, latency ratio, throughput performance, Encryption Time and Decryption Time and accuracy.
- For ID, a novel DL-based Hyb EESCCNN has been proposed. SHA-512 is used for authenticating cloud users to store their information in the cloud server. The input dataset is pre-processed using an ordinal encoder and minimax scalar method. Features are extracted using Fast ICA. The important features are extracted, which reduces the training time while classifying the data. Finally, the malicious data is discarded and non-malicious data is securely stored in a cloud storage system using a novel ATBGVHE method.