Student Name: **Adesh Kumari**
Supervisor Name: Dr. M. Yahya Abbasi
Department: Department of Mathematics, Faculty of Natural Sciences
Jamia Millia Islamia, New Delhi-110025

Topic: Design and Analysis of Authentication Protocols using Elliptic Curve Cryptography

Keywords: Authentication, Smartcard, Signature, Cloud computing, Elliptic curve cryptography, Healthcare system, Security and privacy

FAINDINGS

In Chapter 1, some basic definitions and security objectives for authentication schemes such as security goals and summary of attacks for communication network have been stated. Further, we have discussed cryptographic prerequisites such as general principles, symmetric-key vs public-key cryptography, one-way collision- resistant hash function, basic concepts of elliptic curve cryptosystem, signcryption, biometric, fuzzy extractor and random oracle model.

Chapter 2 is devoted to a new ECC based mutual authentication framework for secure communication, in which users authenticate each other and established a session key. With the help of session key, users can be connected securely over the public communication channel. Further, the proposed protocol does not require the calculation of bilinear pairing which makes this protocol more efficient in communication environment. Finally, we have evaluated the security attributes of the presented framework and proved that the proposed protocol is more protected in established secure networks over the insecure public communication channel. The content of this Chapter is published in **Journal of Discrete Mathematical Sciences and Cryptography (Scopus & ESCI Indexed Journal).**

In Chapter 3, we have demonstrated the various security drawbacks of Wang et al. [1] scheme such as off-line password guessing attack, stolen-verifier attack, no protection for session key and impersonation attack. Here, we have provided a solution of these attacks by designing an ECC based secure and efficient mutual authentication protocol using smartcard. Further, we have proved that the suggested framework provides better security attributes and functionality features than related schemes, which is based on random oracle model. The presented protocol is also more efficient in terms of computation and communication cost in comparison to other protocols in the same environment. Therefore, the proposed protocol is a real-life application in communication system. The content of this Chapter is published in **Journal of Information Security and Applications (SCIE Indexed Journal).**

Chapter 4 deals with the smartcard based mutual authenticated framework for cloud networking using ECC, which shows the better security and efficiency in cloud computing

domain. Further, we have proved that in terms of communication and computation, it is overhead with relevant frameworks in cloud environment. The proposed protocol may be useful in post quantum cryptography, and is a real-life application for network system. The content of this Chapter is published in **proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2021) (Scopus Indexed).**

In Chapter 5, we have proposed a new ECC based anonymous efficient authentication framework for cloud-assisted healthcare system. The proposed framework is having healthcare center upload phase, patient data upload phase, treatment phase and checkup phase in cloud environment. Each phase provides mutual authentication property. The proposed scheme is more secure against many attacks and satisfied different attributes in cloud-based healthcare system. The computation and communication of the proposed framework is less in comparison to different frameworks in cloud-based healthcare environment. Therefore, the proposed work is the real-life application in cloud-based healthcare system. The content of this Chapter is published in **International Journal of Computers and Applications (Scopus & ESCI Indexed Journal).**

Chapter 6 deals with cloud-based authentication framework for smart medical system. Security and privacy are two essential concerns to establish a secure authentication framework in smart medical system. Here, we have described an ECC based suitable framework for smart medical system in cloud environment. In this Chapter, we have discussed six different phases such as registration phase, healthcare center upload phase, patient data upload phase, treatment phase, checkup phase and emergency phase. Further, we have demonstrated that the proposed framework manages better security and privacy features and attributes compared to related frameworks in the similar environment. Also, we have shown that the proposed framework is more efficient in term of computation and communication expenditure compared with related protocols in smart medical system. Therefore, the proposed work is the real-life application in cloud-based smart medical system. The content of this Chapter is published in **IEEE Access (SCIE Indexed Journal).**