UNIVERSITY of RWANDA

ACEIoT

Lightweight Privacy-Preserving Data Aggregation Scheme Based on Elliptic Curve for Smart Grid Communications

Thokozani Vallent Felix
University of Rwanda
PhD Student ,ACEIOT

Abstract:

Smart grid(SG) is a modern electricity grid based on bi-directional flow of electricity and information for effiicient energy management. Due to dependence on information communication, the system is prone to potential cyber-security attacks such as, user identity theft and data privacy breach. Addressing these cyber-security issues with optimal efficiency in smart grid is an open research problem. From this perspective this paper proposes a lightweight scheme for robust information security and privacy-preservation in data aggregation in SG. The proposed scheme utilizes elliptic curve variant of El Gamal encryption cryptosystem and signcryption techniques to achieve user anonymity with greater efficiency. The scheme satisfes the standard security requirements proven in the random oracle model and does not need a trusted third-party or certifcate issuance during scheme run. Performance evaluation analysis shows that the proposed scheme has a better overall performance to most relevant comparable schemes, since it does not use heavy computation operations such as bilinear pairings, map-to-point hash operations, exponentiation among others. Furthermore, the proposed scheme does not depend on trusted authority (TA) neither suffers from coalition attack nor insider attacks.

Seminar date:	Time:	Venue:
17th June 2022	10:00-11:00 am	Virtual