Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.881 – 888

RESEARCH ARTICLE

CONCEALED CLIENT DATA AGGREGATION FOR DATABASE-AS-SERVICE (DAS)

JEBARANJANI.B
M.E/CSE
V.S.B Engineering College
Karur, TamilNadu
jebaranjani@gmail.com

SANGEETHA.S
AP/CSE
V.S.B Engineering College
Karur, TamilNadu
sangi.vs@gmail.com

Abstract---Data aggregation scheme reduces the large amount of transmission in Wireless Sensor Networks (WSN). Concealed Data Aggregation schemes that are extended from homomorphic public encryption system are designed for a multi-application environment. The drawbacks of existing work include address aggregation security for Database As Service (DAS) Model. Client query aggregation increases the computation cost. Compromised secret keys affect the sensor node aggregations that are loosed. In DAS client stores database are on an entrusted service provider. The proposed work presented Concealed Data Aggregation for Database-AS-Service. It establishes the trusted database server for the client data storage. The aggregation of client queries for multiple applications is made with private homomorphic encryption standards. The client query responsive data are extracted from trusted data server with authenticated concealment. PH scheme contains utilizable properties to conceal data of respective clients. It minimizes the computation cost due to the client query aggregates. The uncompromised secret key improves the client query response for multiple groups.

Index Terms---Concealed data aggregation, elliptic curve cryptography, homomorphic encryption, wireless sensor networks.

Full Text: http://www.ijcsmc.com/docs/papers/February2014/V3I2201424.pdf