JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Robust Data Integrity and Privacy Model for IoT-Integrated Smart Grids

Saranya A
Assistant Professor
Department of Computer science
Bharathi Women's Arts and Science College, Kallakurichi, Tamilnadu, India

Abstract : Smart grid environments continuously generate time-varying power consumption data, which must be transmitted to a central server for processing. In such systems, the failure of a single sensor node can disrupt the entire aggregation process. Earlier approaches address this issue using fault-tolerant aggregation mechanisms that continue to operate even when certain nodes fail. However, ensuring the integrity of aggregated data remains a major challenge, as transmitted readings may be altered or corrupted. To overcome this limitation, a recoverable-data strategy is adopted, enabling restoration of accurate data even when corruption occurs. This is achieved by comparing aggregated values with sensor-generated information. The proposed model strengthens integrity and privacy preservation while supporting secure data aggregation in smart grids.

Keywords: Data integrity, homomorphic encryption, Signature Aggregation, Data Integrity Verification,wireless sensor networks.

I. INTRODUCTION

A Wireless Sensor Network (WSN) consists of multiple distributed sensor devices deployed across a region to observe environmental conditions and transmit collected information to a central authority. In smart grid systems, these sensors help optimize energy distribution—from generation and transmission to consumer-level usage. Smart meters play a vital role by recording power consumption periodically and enabling two-way communication with the control center (CC). These meters deliver detailed real-time operational information, supporting dynamic load adjustments, fault monitoring, and system resilience.

Because smart meters record user-specific consumption data at frequent intervals, privacy protection becomes crucial. Numerous schemes have been developed to preserve consumer privacy, especially through homomorphic encryption, which allows data aggregation without exposing individual readings. Existing methods safeguard privacy against curious aggregators but often assume all meters strictly follow the protocol and are honest. They do not effectively handle accidental faults, cyber-attacks, or cases where adversaries tamper with data during aggregation. To address integrity concerns, an end-to-end authentication mechanism compatible with homomorphic encryption is incorporated. Homomorphic signatures are generated along aggregation paths, allowing the CC to verify aggregated results efficiently. Additionally, a hop-by-hop incremental verification scheme is applied to detect forged or altered data, ensuring accountability and quick isolation of compromised nodes

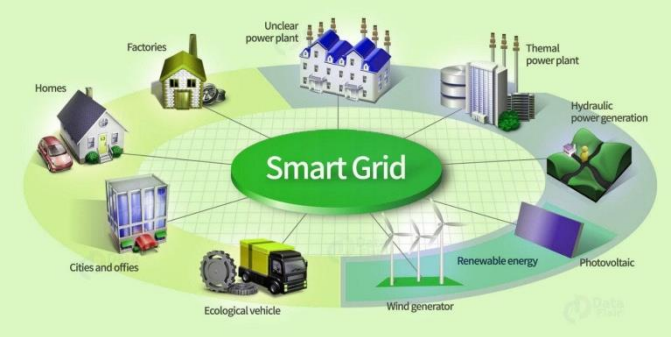

Fig1.smart grid system architecture

I. RELATED WORK

Rather than depending on expensive trusted third parties for anonymizing meter data, researchers have explored aggregation-based privacy preservation using homomorphic encryption. Some protocols support partial-share aggregation but encounter scalability issues due to heavy communication requirements Several privacy-preserving in-network data aggregation schemes have been proposed for smart metering. While these solutions protect confidentiality from malicious nodes, they often overlook authentication, leaving systems vulnerable to data manipulation. Simple digital signature or MAC-based integrity mechanisms have been suggested, but they either lack compatibility or impose high verification costs.

Homomorphic signature schemes have emerged as a promising solution because they allow intermediate nodes to update signatures along with aggregated values while still supporting efficient batch verification at the collector.

III PROBLEM FORMALIZATION

In this section we sanctify system model,security supplies and the propose goal.

3.1 System model

The focus of the system model is secure transmission of residential consumption data to the CC in a privacy-preserving manner. A typical residential area (RA) includes a gateway linked to the smart grid control center and numerous household users. The system incorporates a trusted authority (TA), the control center, a residential gateway, and many smart meters deployed at consumer premises.

3.2Security Requirements

Smart grid communication must ensure confidentiality and integrity. Adversaries may eavesdrop on communication channels or compromise the gateway or CC to obtain sensitive information.

- **Confidentiality:** All user readings must remain private during transmission and storage. Only authorized entities should access the operational responses sent by the CC.
- **Data Integrity:** The CC must be able to verify that each encrypted reading originates from a legitimate user and has not been altered en route. Attackers—including compromised gateways, curious users, or malicious meters—must not be able to forge, modify, or impersonate data.

3.3 Design goal

The main objective is to create an aggregation protocol that supports both privacy and integrity. The scheme should allow aggregation of encrypted data without requiring decryption at intermediate nodes.
Additionally, the CC must be able to validate authenticity, detect corruption, and recover original readings if needed.

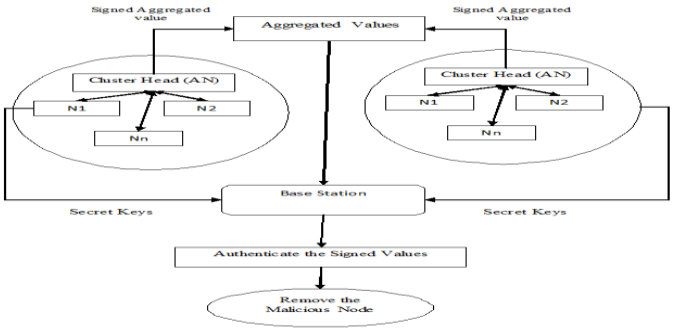

Fig 2 Architecture diagram

IV. PRELEMINARIES

4.1.Homomorphic Encryption

Homomorphic encryption enables computations on ciphertexts without revealing plaintext values. Although effective for privacy preservation, traditional homomorphic schemes do not support verifiable integrity due to their malleability. Therefore, additional mechanisms such as homomorphic signatures are required to validate aggregated outputs without compromising confidentiality.

1) A simplified overview of the cryptosystem is presented, including:

- **Key Generation:** Producing public and private keys for encryption and verification.
- **Encryption:** Sensors encrypt their readings using randomness.
- **Decryption:** The CC decrypts aggregated results through discrete logarithm computation.
- **Homomorphic Addition:** Ciphertexts can be multiplied to represent aggregated values.

4.2 Signing:

Each sensor signs its encrypted output using a homomorphic signature, enabling aggregation of signatures without decryption. Verifiers later check consistency between aggregated values and aggregated signatures, ensuring integrity.

Table 1. Performance Metrics of the Proposed RCDI Model

Parameter	Value
Encryption Time	0.52 ms
Aggregation Delay	1.24 ms
Verification Time	0.89 ms
Communication Overhead	Low

V. PROPOSED METHOD

. The proposed system introduces **Recoverable Data Integrity (RCDI)**, enabling the CC to recover each sensor's individual reading even after intermediate aggregation. Two schemes are proposed

5.1 Proposed RCDI-schemes

This scheme operates through four stages:

- **Setup:** Installation of cryptographic parameters.
- **Encrypt-Sign:** Sensors encrypt and sign readings before transmission.
- **Aggregate:** Cluster heads combine ciphertexts and corresponding signatures.
- **Verify:** The CC decrypts aggregated values, extracts individual readings, and validatesthem using aggregated signatures.

This design leverages powerful H-Sensors to handle computational tasks, reducing the load on low-end L-Sensors. The scheme includes:

- Intracluster encryption for L-Sensors
- Intercluster encryption and signing by H-Sensors
- Aggregation by H-Sensors along forwarding paths
- Final verification at the CC

5.2 Recovery Property

The recovery mechanism allows the CC to authenticate all data and perform additional aggregation functions, such as maximum selection or sum computation, without needing retransmissions. In RCDI-HETE, each H-Sensor verifies integrity using MACs and performs computations as instructed by the CC, maintaining flexibility and robustness.

VI .SECURITY AND SCALABILITY ANALYSIS

The proposed schemes provide strong security under the assumed threat model. Since all messages are encrypted and signed, adversaries cannot forge, alter, or insert fake data without detection. Even if sensors or cluster heads are compromised, attackers lack the keys required for generating valid signatures

Selective forwarding attacks can be mitigated using existing defensive methods. The architecture scales well because computationally heavy tasks are delegated to capable nodes in the heterogeneous model.

VII. PERFORMANCE AND COST EVALUATION

The performance and cost evaluation of the proposed model is essential to determine its feasibility, scalability, and practical deployment capability within real-world smart grid environments. Performance evaluation focuses on measuring computational overhead, communication efficiency, latency, memory consumption, and verification time under varying network conditions. These metrics help quantify the operational impact of integrating homomorphic encryption, signature aggregation, and recoverability mechanisms into smart-meter data workflows.

Cost evaluation, on the other hand, examines the economic implications of the system. This includes the computational cost for sensors and gateway nodes, storage costs at the control center, bandwidth usage, and the cost of deploying and maintaining cryptographic operations across large-scale Wireless Sensor Networks (WSNs). Since smart grids involve millions of reporting nodes, even small increases in overhead may translate into significant long-term operational expenses.

Evaluating performance and cost together allows decision-makers to determine whether the proposed scheme provides an optimal balance between security and resource consumption. A high-security model that is too computationally expensive may not be feasible for resource-constrained sensors, while a low-cost system with insufficient security may expose the grid to data manipulation attacks. The combined analysis therefore ensures that the proposed RCDI-HOMO and RCDI-HETE frameworks deliver robust security, verifiable integrity, and scalability without imposing prohibitive operational costs..

VIII.CONCLUSION

This study presented recoverable privacy-preserving data aggregation mechanisms suitable for both homogeneous and heterogeneous WSN environments. A distinguishing capability of the proposed schemes is that the CC can retrieve all sensor readings securely rather than only aggregated outputs. Although signature operations introduce additional overhead, the overall cost remains feasible. Simulation results demonstrate the efficiency and security of the proposed frameworks for large-scale WSN deployments..

IX.REFERENCES

[1] S. Ozdemir and Y. Xiao, “Secure data aggregation in wireless sensor networks: A comprehensive overview,” Comput. Netw., vol. 53, no. 12, pp. 2022–2037, Aug. 2009.

[2] L. Wasserman, All of statistics : a concise course in statistical inference. New York: Springer.

[3] C. T. Chou, A. Ignatovic, and W. Hu, “Efficient computation of robust average of compressive sensing data in wireless sensor networks in the presence of sensor faults,” Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 8, pp. 1525–1534, Aug 2013

[4] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen,“EPPA: An efficient andprivacy-preserving aggregation scheme for secure smart grid communications,”*IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1621–1631,Sep. 2012.

[5] M. Hashmi, S. Hanninen, and K. Maki, “Survey of smart grid concepts,architectures, and technological demonstrations worldwide,” in IEEE PES Conference on Innovative Smart Grid Technologies, 2011.

[6] X. Li *et al.*, “Securing smart grid: Cyber attacks, countermeasures, and challenges,” *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 38–45, Aug. 2012

[7] L. Chen, R. Lu, and Z. Cao, “PDAFT: A privacy-preserving data aggregation scheme with fault tolerance for smart grid communications,”*Peer-to-Peer Netw. Appl.*, to be published.

[8] F. Li, B. Luo, and P. Liu, “Secure information aggregation for smart gridsusing homomorphic encryption,” in *Proc. 1st IEEE Int. Conf. Smart GridCommun. (SmartGridComm)*, 2010, pp. 327–332.

[9] A. Metke and R. Ekl, “Smart grid security technology,” in *Innovative Smart Grid Technologies*, Jan. 2010, pp. 1–7.

[10] Efthymiou C, Kalogridis G (2010) Smart grid privacy via anonymization of smart metering data. In: SmartGridComm, pp 238–243

[11] Jia W, Zhu H, Cao Z, Dong X, Xiao C Human-factor-awareprivacy preserving aggregation in smart grid. IEEE Syst J (toappear)

[12] T.-H. Chan, E. Shi, and D. Song, “Privacy-preserving stream aggregationwith fault tolerance,” in *Financial Cryptography and Data Security*,A. Keromytis, Ed. Berlin Heidelberg: Springer, 2012,LectureNotes in Computer Science, vol. 7397, pp. 200–214.

[13].HULL, B., BYCHKOVSKY, V., ZHANG, Y., CHEN, K., GORACZKO,M., MIU, A., SHIH, E., BALAKRISHNAN, H., AND MADDEN, S.Cartel: a distributed mobile sensor computing system

[14]. A. Wander, N. Gura, H. Eberle, V. Gupta, and S. Shantz, “Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks,” Proc. IEEE Third Int’l Conf. Pervasive Computing and Comm. (PERCOM ’06), 2005.

[15] G. De Meulenaer, F. Gosset, F.X. Standaert, and L. Vandendorpe, “On the Energy Cost of Communication and Cryptography in Wireless Sensor Networks,” Proc. IEEE Int’l Conf. Wireless and Mobile Computing, Networking and Comm., pp. 580-585, 2008.