IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 09, Issue 2 (February. 2019), ||V (I) || PP 56-59

An Overview of Privacy-Preserving Data Aggregation in IoT

Manas Ranjan Mohapatra[1], Dr. Jitendra Sheetlani[2], Dr. Rasmi Ranjan Patra[3]
[1]*Research Scholar, SOCA, SSSUTMS, Sehore, M.P., India*
[2]*Associate Professor, SOCA, SSSUTMS, Sehore, M.P., India*
[3]*Assistant Professor, Dept. of CSA, CPGS, OUAT, Bhubaneswar, India*
Corresponding Author: Manas Ranjan Mohapatra

Abstract: Internet of Things (IoT) is a system of interrelated connected physical objects that are accessible through the internet. Internet of Things offers the most flexibility and convenience in our daily applications as the IoT devices can improve productivity, accuracy and financial benefit in addition to reduced human intrusion. Security, privacy and communication overhead Problems are also arising in IoT. To address this problem, many privacy-preserving data aggregation schemes have been proposed in the past years. Privacy-preserving data aggregation is one application in IoT. Privacy-preserving data aggregation is a main building block that can protect user's privacy.

In this paper, we present an overview of privacy-preserving data aggregation scheme for IoT to preserve privacy and to reduce communication overhead. There are many Privacy-Preserving Data Aggregation (PPDA) approaches have been proposed to ensure data privacy during data aggregation in resource-constrained sensor nodes. We provide an overview and analysis of the state of the art PPDA approaches in this paper. We have evaluated the most recent approachesand provide in-depth analysis of the minute steps involved in these approaches. In addition, this overview gives very analysis of each mathematical operation involve in different PPDA schemes. This study will help the researchers to design energy efficient and computationally feasible solution to ensure user's privacy in IoT applications.

Keywords: Privacy, Internet of Things, Computing, Network, Sensor, Grouping, Security, Data Aggregation, Communication Overhead.

Date of Submission: 21-01-2019 Date of acceptance:05-02-2019

I. INTRODUCTION

The 'Internet of Things' is the most significant technology in new era of computation. Internet of Things is an interaction of smart objects that are connected to the Internet. It is a system of related computing devices, mechanical and digital machines, objects, people or animals that are provided with unique identifiers and also the potential to transmission of data over a network without requiring human-to-human or human-to-device interaction. IoT System transmit data over wireless networks may contain the private data or the secret data, then this type of system includes security problems such as cyber-attacks, private privacy and planned crimes. To solve these problems, it should have some features such as Privacy-Preserving and data aggregation.

Privacy of one individual remains one of the important aspects in society. Privacy is one of the main problem to relate the wireless sensor networks in IoT to civilian applications, where curious individuals may attempt to determine more detailed information by eavesdropping on the communications of their neighbors. Data aggregation is an approach, which is proposed to substantially reduce the communication overhead and energy spending of sensor node during the development of data collection in IoT. However, privacy preservation is more challenging in data aggregation, where the aggregators need to perform some aggregation operations on sensing data it received. Efficient data aggregation method can raise the life of sensor nodes and the sensor network, as it decreases computation at each node and communication overhead in the network. Fig.1.

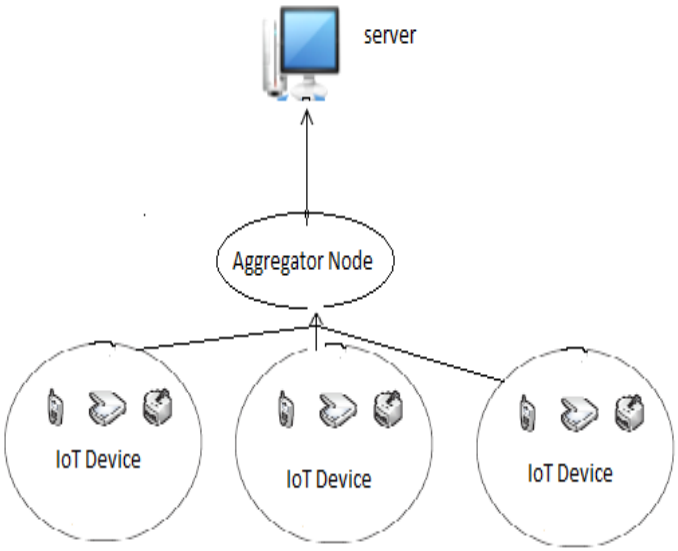

Fig.1. Data aggregation in IoT

In this paper, we discuss an efficient privacy-preserving data aggregation method for IoT. We present an analysis of privacy-preserving data aggregation in IoT.

We have reviewed the most recent approaches and analysis the security and privacy issue. Also know about, Data Aggregator that aggregates the received data without knowing each individual's actual data. To the best of our knowledge, this is the latest discussion to discuss these PPDA solutions.This paper is organized as follow, section 2 discuss PPDA methods in resource-constrained sensor nodes. In section 3 we provide an analysis of the techniques and finally, we conclude the paper in section 4.

II. PRIVACY-PRESERVING DATA AGGREGATION METHODS

Almost all the applications of IOT demand certified level of security and privacy. Providing effective data aggregation though preserving data privacy is a major issue in wireless sensor networks. There are lots of Privacy-preserving data aggregation Methods developed for WSN and smart grid. We review some PPDA methods and compare their operation. The methods are discussed below.

Bista et al. [2] design a method to preserve the privacy of WSN data from security threats. The existing schemes cluster-based private data aggregation [11] and Slice-Mix-AggRegaTe [11] have high communication cost, while the proposed scheme is efficient in terms of communication overhead and power dissipation.

Li et al. [9] propose an excellent sum aggregation protocol based on an additively homomorphic encryption, and also construct a highly efficient Min computation protocol based on their sum aggregation protocol. Besides the good efficiency and smart protocol designs, Li et al.'s protocols adopt a very delicate key system so that their protocols can thwart collusion attacks and are able to efficiently handle users' dynamic joining and leaving.

Yip et al. [8] use Incremental Hashing Function to propose a scheme for Privacy-preserving and Cheat-Resilient (PPCR) power management and broadcasting for Smart Grid (SG). IHF is suitable for resource-constrained smart meter. IHF need low storage and computation power. This system executes data aggregation and hashing at smart meter. It is a high secure and privacy based system. This system does not provide a result if data is overheard at device layer.

Kumar and Madria [5] design a novel energy efficient algorithms for preserve data privacy and data integrity in the strategy of data aggregation. This is based on Recursive Secret Sharing (RSS) and shares of the data d are used to store k 2 additional pieces of in-formation. A node with at least k shares can easily reconstruct all of the k1 pieces of hidden information. It provides a construction that prevents a node which has all the shares, from reconstructing and retrieving the unknown data. This is very efficient algorithm in terms of power utilization, memory save, bandwidth utilization and performance time. This algorithm does not discuss the method to support the variables in sensor nodes.

Othman et al. [6] design a method that ensure data privacy through aggregation and improve efficiency of data transmission. This method is founded the homomorphic symmetric encryption and ensures data integrity using homomorphic signature. An energy efficient data aggregation method is design by Othman et al. [7] for data privacy and integrity. This method is secure against node cooperation attack. It is based on Elliptic Curve

Okamoto-Uchiyama (EC-OU) for data Privacy and Elliptic Curve Digital Signature Algorithm (ECDSA) for data integrity during data aggregation in WSN.

We mainly summarize state-of-the-art privacy preserving data aggregation schemes. Current privacy preserving data aggregation scheme provide privacy protection as either the private data of the user or the intermediate information may be disclosed. We discuss many efficient and practical data aggregation schemes in which collected data are confused to preserve users' privacy.

III. REQUIREMENTS OF PRIVATE DATA AGGREGATION

The main design objective of this paper is to provide an analysis of privacy-preserving data aggregation structure, which is robust against eavesdropping, and capable to detect data pollution and node crashes. Protecting the data privacy in many IoT applications is a main theme. The following criteria summarize the key characteristics of a private data aggregation scheme:

1) Privacy: Privacy is one of the key problems to apply the IoT networks, where each node's data should be only known to itself. Privacy is measured as a significant part of maintaining data without data loss. Furthermore, the private data aggregation schemes should be able to manage to some attacks and collision among compromised nodes. When a sensor network is under a different attack, it is possible that some nodes may collide to uncover the private dataof other node(s). It is very important to develop privacy-preserving data aggregation systems to confirm data privacy against.

2) Energy Efficiency: IoT Sensor's lifetime is strictly dependent on its resource and power usage. The data aggregation is decreasing the number of messages communicated within the sensor network, thus decrease resource and power usage. Data aggregation achieves bandwidth efficiency by using in network managing. In private data aggregation systems, additional overhead is introduced to protect privacy, which cannot be avoided. A suitable and efficient system should keep that additional communication overhead, computation cost, memory and payload size as small as possible.

3) Data Accuracy: Data may be loss due to wireless link during communication or node failure, hence the accuracy of the outcome can be affected. An accurate aggregation of sensor data is wanted, with the constraint that no other sensors should know the exact value of any separate sensor. Accuracy should be a measure to evaluation the performance of private data aggregation schemes.

4) Fault Tolerance: Sensor nodes are breakdown due to lack of energy, hardware failure, and unauthorized attack. IoT network must be robust against breakdown of sensor node and the network functionality must be preserved. New nodes can be added into the network to compensate for failure nodes. A best system should allow node accumulation during data aggregation for preserve network functionality.

5) Flexibility: IoT network must be flexible. Besides, it should be convenient for system to add a new Node in a residential area.

6) Data Integrity: Data aggregation outcome may be used to build critical conclusions, a base station requirement to attest the integrity of the aggregated result before accept it. Hence, it is preferred that data aggregation scheme has the ability for integrity check.

IV. COMPARATIVE ANALYSIS

In this section, we give the performance analysis of the existing Privacy preserving data aggregation algorithms for IoT. The most important performance parameters are computation cost, communication overhead, Privacy level and Privacy against aggregator IoT sensor node.

Computational Cost: Computational cost (CC) will examine the algorithms based on the complexity of mathematical steps involved.

Communication Overhead: The total numbers of packets are to be transferred or transmitted from one node to another is known as the communication overhead.

Privacy preservation Level and Privacy against aggregator: Ensure data privacy against eavesdropping.

The comparative analysis of techniques are discussed below and summarized in Table 1.

Table1. Comparative analysis of Privacy preserving data aggregation Techniques for IoT.

Technique	Privacy preservation efficiency	Communication overhead	Aggregation accuracy	Computational overhead	Privacy against aggregator
CPDA	Excellent	Fair	Good	Fair	Yes
SMART	Excellent	Large	Good	Small	Yes
PPCR	High	Very Small	-	Medium	No
PIP	Medium	Medium	-	Medium	Yes
SPDA	-	Light-weighted	Very High	-	Yes
EC-OU & ECDSA	High	Small	-	Very High	Yes

The above table provides a comparative analysis of these state of the art techniques based different performance parameters. These parameters are the preferred features of any privacy algorithm in the Internet of Things.

V. CONCLUSION AND FUTURE WORK

Privacy preserving Data aggregation is an important method to save communicationn bandwidth for private data collection in wireless sensor networks. In this discussion, privacy preserving data aggregation system for IoT have been analyzed and issues for designing privacy preserving data aggregation system have been identified. We believe that our critical analysis of the existing system will provide new research strategies to expand the existing systems and to implement new secure and privacy preserving data aggregation system for IoT. The existing privacy-preserving data aggregation protocols have used different systems to accomplish data privacy, such as privacy homomorphism, perturbation and shuffling. Each type of the above systems has some advantages and disadvantages.

In this review article, we analyzed existing PPDA in IoT sensor nodes and provide comparison of existing methods based on different performance parameters. This analysis will help the new researchers to understand the PPDA method and will help to propose more efficient privacy-preserving techniques.

In future this work can be extended to implement an Efficient and Secure privacy-preserving data aggregation approach for IoT (i.e. preserve the privacy of IoT data from security threats), Efficiency of Communication overhead and power dissipation to be improved. Another aim of this proposed research is this approach can resist against the false data injection from the external attacks.

References

[1]. Atzori L, Iera A, Morabito G. “The Internet of Things: a survey”, Compute Netw 2010; 54:2787-805.

[2]. Bista R, Jo K, Chang J. “A new approach to secure aggregation of private data in wireless sensor networks” in IEEE international conference on dependable, autonomic and secure computing; 2009. p. 394-9.

[3]. He W, Liu X, Nguyen H, Nahrstedt K, Abdelzaher T. “PDA: privacypreserving data aggregation in wireless sensor networks” in Proceedings of the INFOCOM; May 2007. p. 2045-53.

[4]. J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami “Internet of Things (IoT): a vision, architectural elements, and future directions”, Future GeneratComputSyst, 29 (7) (2013), pp. 1645-1660

[5]. Kumar V, Madria S. “PIP: privacy and integrity preserving data aggregation in wireless sensor networks” in IEEE 32nd international symposium on reliable distributed systems (SRDS); 2013. p. 10-9.

[6]. Othman S., Bahattab A., Trad A. “Confidentiality and integrity for data aggregation in WSN using homomorphic encryption Wireless PersCommun”, 80 (2) (2014), pp. 867-889.

[7]. Othman S, Alzaid H, Trad A. “An efficient secure data aggregation scheme for wireless sensor networks” in IEEE international conference on information, intelligence, systems and applications (IISA); 2013.

[8]. Q. Li and G. Cao, “Efficient and privacy-preserving data aggregation in mobile sensing” in Proc. IEEE ICNP , Oct./Nov. 2012, pp. 1–10.

[9]. Q. Li and G. Cao, “Providing efficient privacy-aware incentives for mobile sensing” in Proc. IEEE 34th Int. Conf. Distrib. Comput. Syst. (ICDCS), Madrid, Spain, Jun./Jul. 2014, pp. 208–217.

[10]. Wenbo He, Hoang Nguyen, Xue Liu, KlaraNahrstedt, TarekAbdelzaher. “SPDA: Secure and Privacy - preserving Data Aggregation in Wireless Sensor Networks”.

[11]. W.He, X.Liu, H.Nguyen, K.Nahrstedt, T.Abdelzaher, “PDA: privacy-preserving data aggregation in wireless sensor ne tworks", IEEE INFOCOM, 2007.

Manas Ranjan Mohapatra. “An Overview of Privacy-Preserving Data Aggregation in IoT.” IOSR Journal of Engineering (IOSRJEN), vol. 09, no. 02, 2019, pp. 56-59.