SIT719 Security and Privacy Issues in Analytics

Distinction Task 9.1 Survey on Differential Privacy for Industrial IoT

Differential privacy may be a new model of cyber security that proponents claim can protect personal data much better than traditional methods. it's become a replacement standard for privacy preservation in IIoT. It defines a close attack model, reduces data disclosure privacy risk and ensure availability of information occasionally of query or decision.

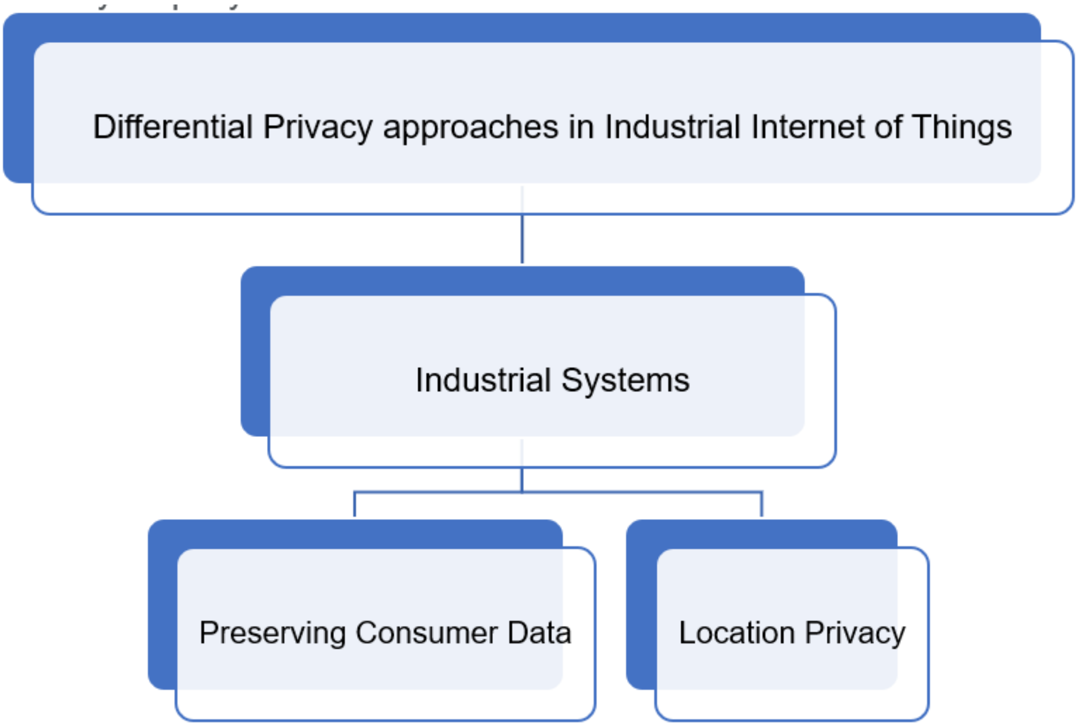

Differential Privacy approaches in Industrial Internet of Things
Industrial Systems
Preserving Consumer Data
Location Privacy

Fig 1. The differential privacy approach implemented in Industrial IoT in the field of Industrial System

Traditional techniques like anonymity fuzzification technology didn’t show considerable leads to IIoT systems due to multiple data fusion and reidentification of anonymized data. Hence, differential privacy looked as if it would suitable solution without compromising the integrity and privacy. The writers in [1] bettered the privacy of the data by combing differential privacy method with k-anonymity model. The writers made use of quality ideology of DP, combined this along with k-anonymity model and increased the anonymity of the data, they are visiting be added and transmit by not taking the risk of the privacy. Moreover, the writers in [2] considered the factor of preserving the location of business sensors using DP. They first showed that extracting location from the IIoT sensors can influence a giant threat to the industry and they provided the answer by combining DP with the sensors. By observing the above article regarding the industrial automation systems privacy and taking into consideration of the effectiveness of the dynamic nature exhibited by differential privacy strategies, it'll be safely told that DP can efficiently preserve privacy with combined application of Industrial system.

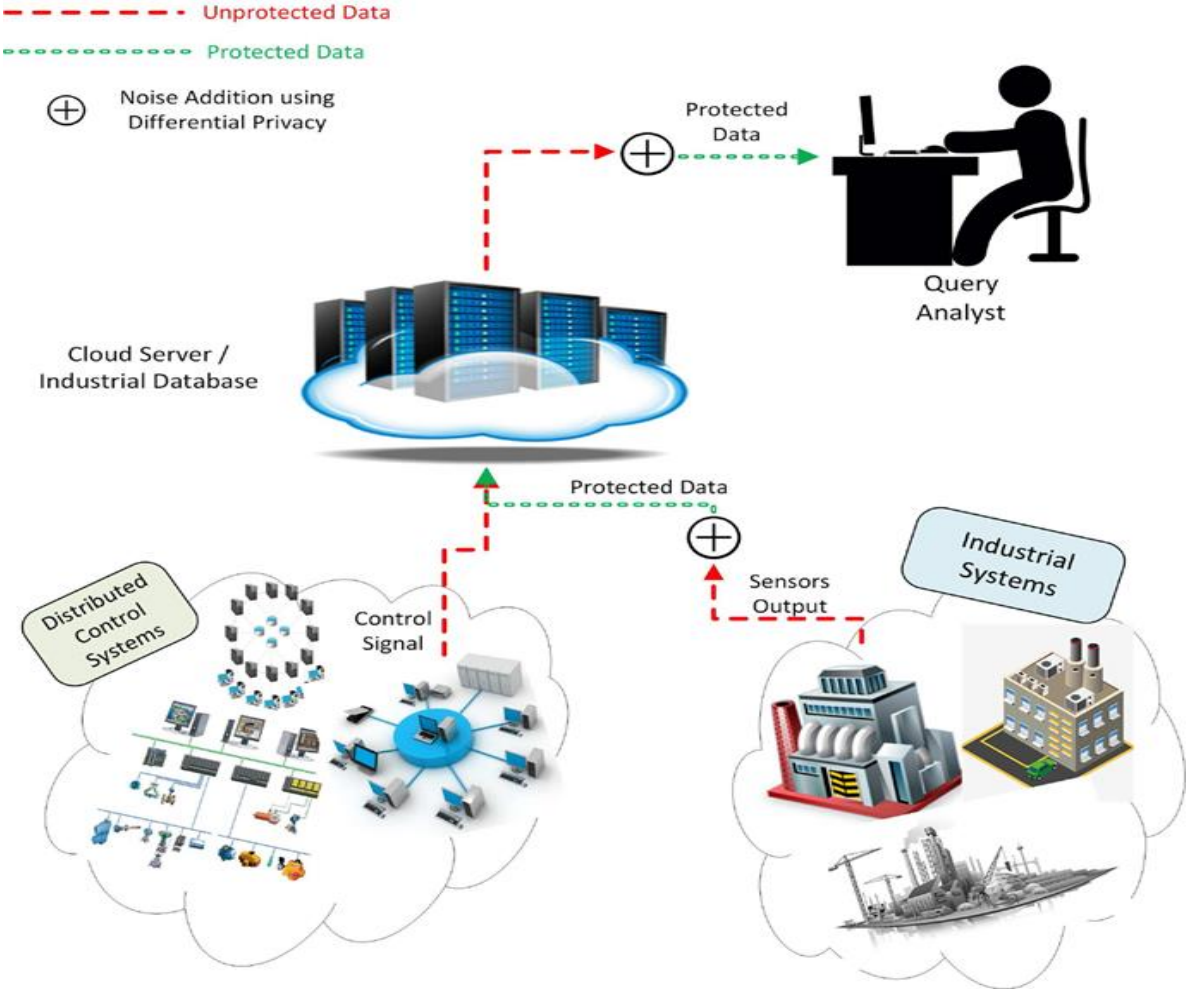


Fig 2. DP implementation in IIoT.

Differential Privacy in preserving consumer data in IoT:

In the article [1], the authors propose a hybrid privacy protection model with the goal of balancing privacy and value of information. The authors model makes use of traditional de-identification methods like k-anonymity under low-privacy requirements. The methodology also allows for transmission of aggregate statistical results obtained using privacy preserving method i.e. Differential Privacy.

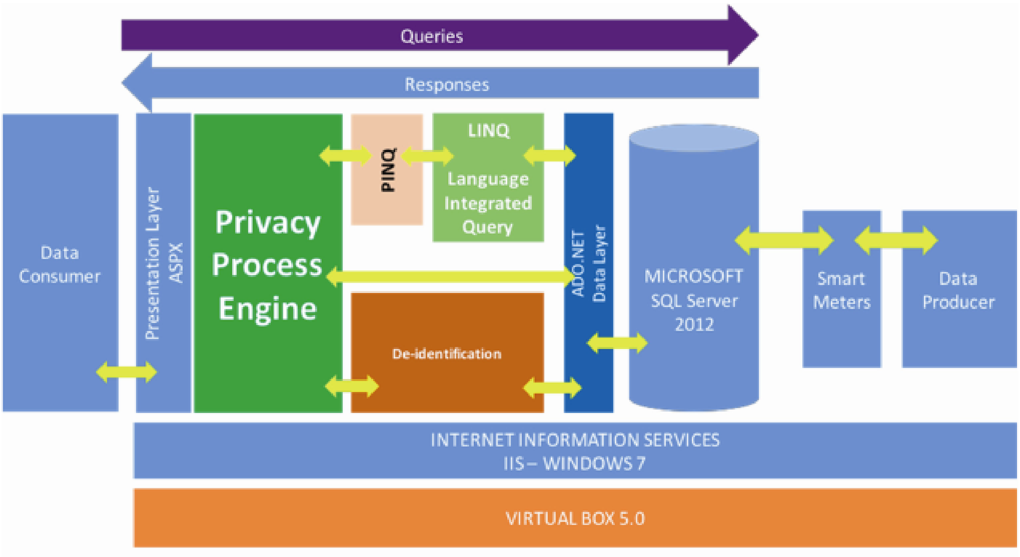


Fig 3. Logical architecture of the proposed model.

The proposed model works sequentially, firstly by checking if the info requested can be provided under any global rules if therefore the table from the query are syntactically anonymized using k-anonymity using the principles triggered by the patron. Following which a loss metric is calculated if the info loss isn't within the negotiated threshold the set of aggregated statistical descriptors are calculated from the initial data employing a privacy-preserving method i.e. Differential Privacy.

As a result, rather than delivering an almost useless de-identified dataset to the patron, a group of statistical descriptors was provided, partially preserving utility for a hypothetical consumer application.

Differential privacy in Location privacy in IoT:

In the article [2], the authors try and tackle the challenge where privacy protection issue in location privacy was being overlooked. To tackle this the authors, proposed using location privacy protection methodology that convinces DP constraint to shield Privacy of the location data and amplify the atmost use of knowledge information and the algorithm used in IIoT.

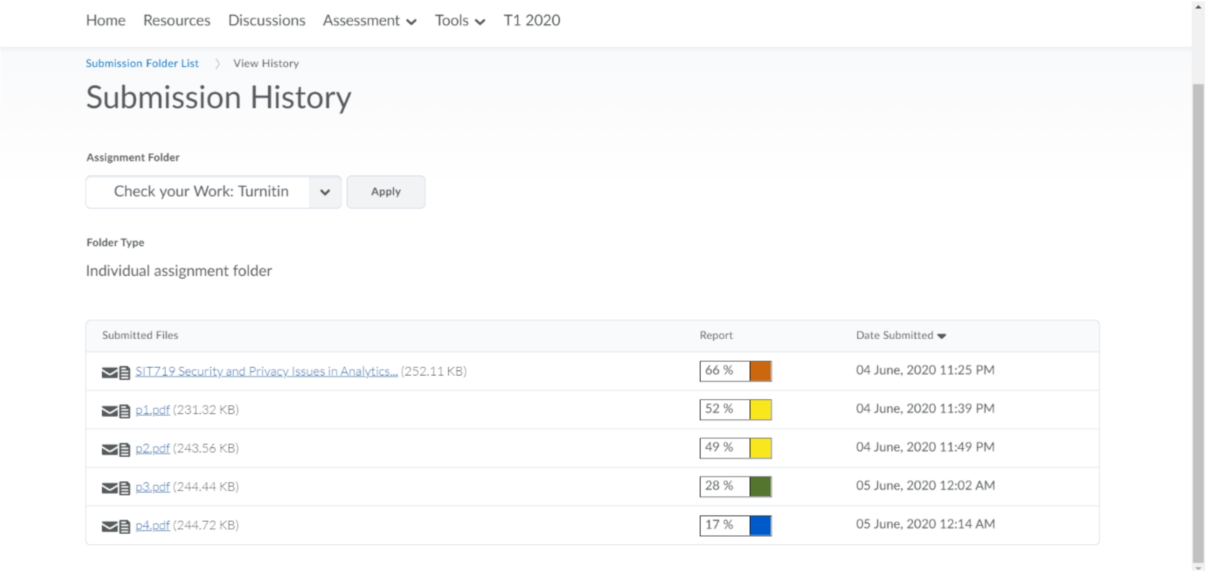
The proposed method combines the data utility with privacy to make a multilevel information tree model of location data which will solves the matter of location data which are difficult to specific. Followed by the Differential privacy to decide on data in line with the tree node accessing frequency which is more accurate and has greater utility and process coherence compared to traditional approach. At the end the Laplace scheme is employed to feature noise to access the frequency of chosen data.

As a result, from theoretical analysis and practical results the proposed methodology was able to achieve notable improvements in security, privacy and applicability.

Table of comparative view of the differential privacy techniques in IIoT:

Category	Privacy Mechanism	Techniques of DP used	Enhancement due to DP	Scenario
Industrial Systems	Differential privacy for IoT	k-anonymity eith traditional DP	Enhanced anonymization	Real-time
	Location privacy for IIoT using DP	Tree node accessing frequency model is used with Laplacian noise	Maximize data utility and timeliness	Real-time

Plagiarism check:



Submission History

Assignment Folder

Check your Work: Turnitin

Folder Type

Individual assignment folder

Submitted Files	Report	Date Submitted
SIT719 Security and Privacy Issues in Analytics... (252.11 KB)	66 %	04 June, 2020 11:25 PM
p1.pdf (231.32 KB)	52 %	04 June, 2020 11:39 PM
p2.pdf (243.56 KB)	49 %	04 June, 2020 11:49 PM
p3.pdf (244.44 KB)	28 %	05 June, 2020 12:02 AM
p4.pdf (244.72 KB)	17 %	05 June, 2020 12:14 AM

Reference:

[1] C. R. G. Rodríguez and S. E. G. Barrantes, “Using differential privacyfor the Internet of Things,” in IFIP International Summer School on Privacy and Identity Management. Cham, Switzerland: Springer, 2016, pp. 201–211.

[2] C. Yin, J. Xi, R. Sun, and J. Wang, “Location privacy protection based on differential privacy strategy for big data in industrial Internet-ofThings,” IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3628–3636, Aug. 2017.

[3] Hassan, M, Rehmani, M & Chen, J 2020, "Differential Privacy Techniques for Cyber Physical Systems: A Survey", *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 746-789.