phdprimehelp@gmail.com
+91-97 91 62 64 69

**Ph.D. Research Proposal**

**Doctoral Program in “Department Name”**

# High Performance Task Allocation and Security Aware Data Transmission for Heterogeneous Fog Environments

**by**

<Name of the Candidate>

<Reg. No of the Candidate>

**<Supervisor Name>**

**<Date of Submission (DD MM 20YY>**

# I. INTRODUCTION / BACKGROUND

In recent years, fog environment has received huge attention from research community. It is due to the growth of internet of things (IoT). Now these devices are heterogeneous in nature that sends multiple different tasks per second. All these tasks are delay sensitive and energy constraints. To address these problems, heterogeneous fog environment will be focused. There are more duplicates occurred during sensing, processing and analysis.

Healthcare, air pollution monitoring, smart grids, smart homes and smart vehicles are the best example applications that provides advantages via fog computing. However, mining the data stored by enormous edge servers is difficult in distributed computing environment. Cloud server or proxy server extracts this information and provide support to on-demand services to end users. Cloud server outsourcing non-sensitive information to end users, but it does not guaranteeing data security and integrity. Air pollution is one of such environment that affects the human life, animals and plants. It happens due to harmful amounts of the following,



- Gases
- Dust / Fumes or Odour
- Nitrogen Dioxide ($NO_2$)
- Carbon Dioxide ($CO_2$)
- Carbon Monoxide (CO)
- Methane ($CH_4$)
- Hydrogen Sulfide ($H_2S$)
- Hydrocarbons (Ethanol, Propane, Butane and Toluene)
- Ozone ($O_3$)

In air pollution monitoring, there will be a huge amount of duplicate data forwarded to data processing center. It upturns the storage capacity and efficiency of the monitoring system. Hence, data deduplication scheme is required in which the redundant or similar data is find out and eliminated. This will improve the storage requirement of the data. IoT devices whose submit the replicate sensing data should be ignored. On the other hand, task allocation is performed via fog computing for number of IoT devices. It reduces latency, communication overhead and communication cost for IoT devices. Fog nodes aggregate the sensing data and forward the computing results and then data upload to the cloud servers. Importance of fog computing for task allocation is follows:

- **Delay:** In many real world environments, low latency is a major constraint. To reduce the amount of time for task processing, fog nodes are deployed on the edge of the network. Fog nodes located very close to the IoT networks.
- **Security / Privacy:** Large amount of data generated and forwarded in network that cause major attacks. To avoid malicious activity, data encrypted and forwarded to end users or other processing centers. Fog computing is the best solution to prevent privacy leakage since it provides shortest distance path for data transmission
- **Data Indexing:** In order to perform data retrieval among end users, efficient indexing is required.

## 1.1 Research Outline & Scope

Combining heterogeneous IoT and fog environments are challenging, where meets service delay, and achieve security and privacy are the most important factors that need to focus in this environment.

## 1.2 Research Objectives

The main objective of the proposed heterogeneous fog model is to assign tasks from IoT to fog optimally and also detect redundant data at the fog layer for improving resource consumption. There are some sub-objectives are follows,

- To reduce the average latency while processing massive size and number of tasks
- To enrich user satisfaction when request for processing a new data retrieval
- To improve network lifetime for enriching the alive time period of both fog nodes and IIoT devices

- To minimize overall energy consumption at both fog and IoT layer
- To enhance the strength of security and privacy for both tasks and devices

## II. RESEARCH GAPS

This section presents the research gaps identified in the current task allocation and secure deduplication works under heterogeneous fog environment. In this research work we address the following problems:

- How can allocate fog resources to different IoT uses efficiently?
- Incorrect association of storage files result high energy consumption, and delay and also does not satisfy the user application requirements.

### 2.1 Common Problem Statement

Security / Privacy are a major issue in heterogeneous fog-IoT (i.e.) processing unauthorized user task consumes more resources and degrades the overall performance. Additionally, task allocation and secure deduplication considers limited parameters and follows conventional approaches those results in large waiting time. In fog environment, task allocation is handled with either task or fog oriented metrics. But it is necessary consider both in order to achieve better efficiency. Overall, secure task management is still challenging in fog-IoT environment.



### 2.2 Problem Definition

Abbas et al., [1] have proposed Fog security scheme (FSS) to ensure end-to-end security with the effectual authentication procedure that follows RSA crypto function. This FSS provide security services include confidentiality, non-repudiation and confidentiality. The proposed FSS architecture is implemented and evaluated using OPNET simulator and also using different traffic loads. Further, testing is conducted for highly resource constrained environments such as memory, CPU, power and processing capacity.

**Problems**

- The considered authentication credentials such as ID, password has lower security level and easily forgeable.

- In particular, considering anyone of this credential will result high vulnerability.
- Additionally, RSA has higher computational time and overhead which is not suitable for the resource-constrained IoT devices

In [2] authors have introduced a new P-SEP based fog computing architecture which follows FECR and FEAR techniques for energy efficient routing and also these two techniques solve the limitations of WSN based IoT applications. The proposed architecture reduces 9% and 8% of energy usage in FECR and FEAR respectively. Similarly 74% of network lifetime is increased by 74% and 83% in FECR and FEAR, respectively.

**Problems**

- Clustering is not effective since node with more residual energy is selected as CHs
- Optimal fog node allocation does not investigated because it randomly selects the adjacent fog nodes (major reason for presenting fog computing is to reduce the processing delay and satisfy the user applications)

**Proposed Solutions**

- Clustering is performed using Firefly Algorithm which considers multiple metrics for form clusters that are residual energy, node degree and distance between nodes
- Optimal fog nodes are selected using Fuzzy AHP algorithm which follows multi criteria decision making

To authenticate the IoT users, multi authorities are allowed in the fog environment. Guan et al. [3] proposed scheme follows layered fog-IoT system in which fog layer (with smart devices, fog nodes, and local certificate authorities), and cloud layer (with trusted certificate authority and public cloud server) are organized in layered manner. All smart devices must be registered with LCA and TCA in order to receive certificate for authentication. In certificate generation, both LCA and TCA perform Rivest Shamir Adleman (RSA) based key generation for every user. For encryption, paillier scheme based key was generated for every user. The data was encrypted by smart devices and aggregated by fog nodes and then decrypted by cloud server.

**Problems**

- Here, involvement of RSA and Paillier schemes increases the time consumption.
- Besides, both algorithms have complex operations which make them not suitable for lightweight IoT devices.

**Proposed Solutions**

- Very less complexity required algorithms are proposed in this work such as PRESENT and mCrypton cryptography algorithms

A mobile crowdsensing challenge (increasing number of participating mobile users) is tackled through fog computing in [4]. Task allocation is finished by selecting near fog node and also task assignment is done based on user mobility. In this paper, a fog assisted secure data deduplication scheme is proposed which ensure data confidentiality. The fog nodes detect and remove replicate data. For that authors have presented BLS-oblivious pseudorandom number function and chameleon hash function is used to hide user's information to anonymous mobile users.

**Problems**

- BLS-oblivious pseudorandom number function is used for data deduplication verification and unauthorized users can easily generate pseudo random number of data deduplication and also it is time consuming process
- Task allocation/assignment does not effective since it find the fog nodes based on the mobile users local information such as mobility patterns

**Proposed Solutions**

- Optimal fog node is selected based on two fitness values in which first fitness value computed based on processing delay and task length and the second fitness value is computed based on node residual energy and distance between fog nodes and nodes.
- Task length and processing delay are important metrics which is required for task allocation to fog nodes

**A** sensor cloud based architecture based data acquisition scheme is proposed [5] using adaptive block compressive sensing and fog computing. There are three layers are comprised include WSN layer, Fog layer and Cloud layer. In WSN layer, all sensors are sensed data and forward to fog layers in which mobile nodes are considered as fog nodes (sink). Mobile nodes considered to improve the total network transmission and minimize the task processing delay

**Problems**

- Adaptive block compressed sensing is an image compression technique which proposed in the lower WSN layer for signal acquisition and processing and hence ABCS is high complexity and it does not lightweight. In addition ABCS cause high energy utilization at fog node
- In lower WSN layer, virtual clusters are created, which does not formed effectively

**Proposed Solutions**

- We proposed lightweight approaches for secure deduplication and task allocation
- Clustering is performed using Firefly which considers multiple metrics for form clusters that are residual energy, node degree and distance between nodes



## III. RESEARCH CONTRIBUTIONS

Large amount of IoT devices and its large size of data sensed, and transmitted them to data processing center (cloud). In this work, we proposed fog assisted task allocation and secure data deduplication in cluster-based industrial IoT (IIoT). The proposed system estimates several air pollutants such as $NO_2$, $CO_2$, $SO_2$, $O_2$, $PM_{2,5}$, $PM_{10}$. The proposed fog assisted IIoT environment consists of five entities include IoT devices (sensors), fog nodes (gateways), trusted authority, proxy server and cloud server. And also there are four layers are considered this work: IoT device layer, fog layer, cloud layer and service layer. Firstly, IoT devices are registered to cloud server through TA using **PRESENT and mCrypton algorithm.**

- To solve the scalability issues, clustering the specific region is considered. For each IoT device we calculate three metrics that are residual energy, node degree (number of neighbor connections), and distance between nodes. These three values are fed into **Firefly algorithm** for optimal cluster head selection. All sensors sense the data (air chemical values) and forward to the cluster head and CH send the sensed information for the fog node.

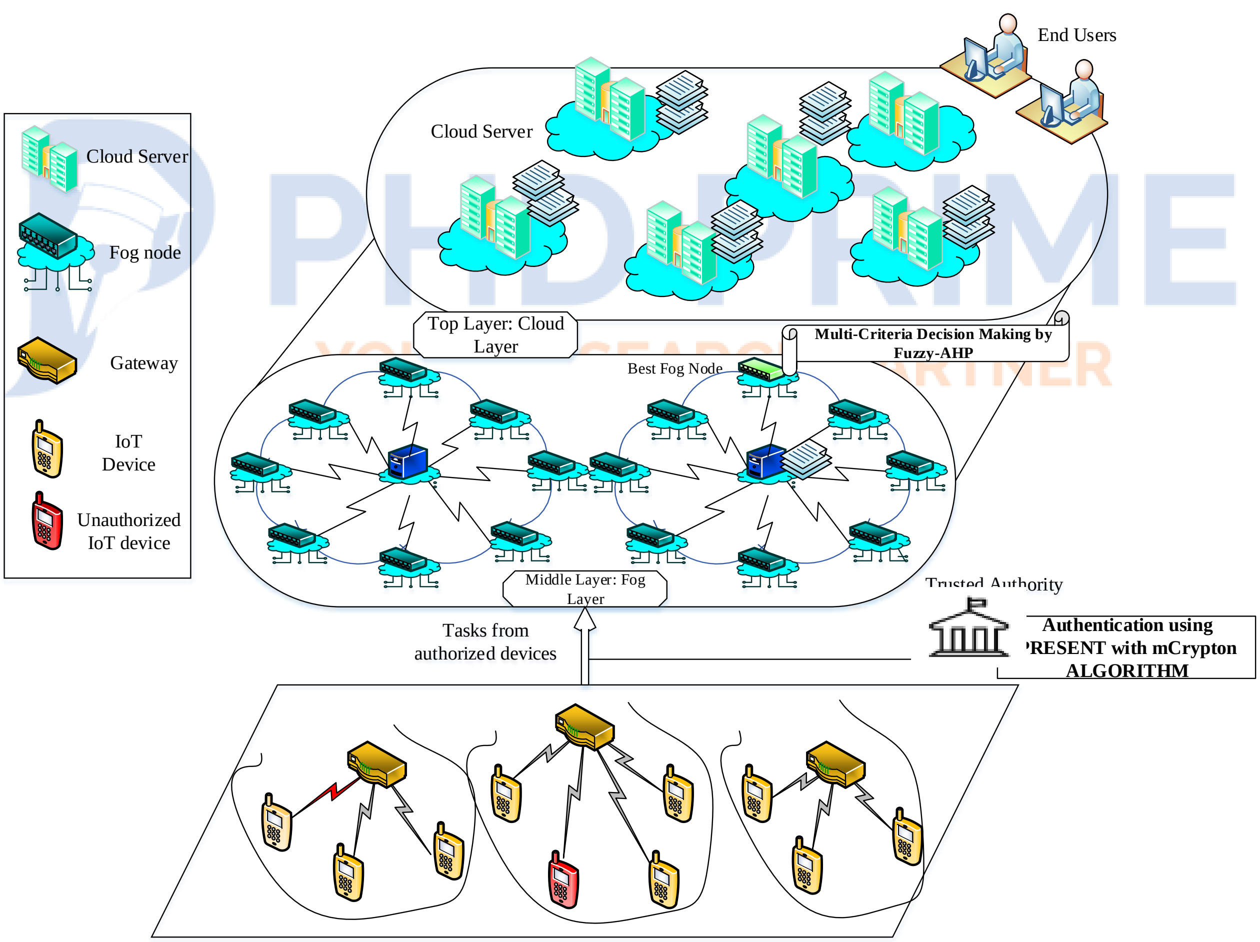
- Then CH chunk packets into number of partitions. For each partition, hash value is generated using **BLAKE2S algorithm**. CH send *duplicate service check (DSC) request* to near fog nodes by giving query using any hash value. Then CH receives duplicate service check response from number of fog nodes. Based on the available fog nodes, CH select the best fog node using **Fuzzy AHP Algorithm** which runs based on the **multicrietria decision making.** This algorithm is inspired by the collection of movement of the fish and their various behaviours. The major reason for using this algorithm is follows: good robustness, global search ability and tolerance parameter setting.
- After optimal fog node selection, CH upload the whole data to fog nodes and fog node encrypt data using Present private key. In service layer, indexing is constructed using **Refined Hash Tree,** which constructed based on the hash value (at proxy server). It is used to provide the query results for end users after the authentication success.

**Performance Evaluation**

Finally we compare the performance of our proposed work with the following metrics:

- Latency (ms) vs. No. of IoT devices
- User satisfaction vs. No. of IoT devices
- Network lifetime vs. No. of IoT devices
- Energy consumption vs. No. of IoT devices
- Security Strength
    - Key Size
    - Message Size
    - Encryption Time
    - Decryption Time

SYSTEM ARCHITECTURE




## IV. RESEARCH NOVELTIES

- The proposed fog model balances time consumption as well as performance.
- It has lower response time, processing time, delay, and energy consumption with higher throughput.
- The major reason behind the results is the combined concept of task management (i.e.) security and task management.
- As the security approach eliminates the unauthorized access

V. PREVIOUS WORKS & LIMITATIONS

In this section, what are the works have been done previously for latency aware resource management is described in this section.

**Paper 1**

**Title –** Towards Workload Balancing in Fog Computing Empowered IoT

**Concept –**

In this paper, delay is considered as an important criterion for fog nodes and IoT devices. To meet this objective, workload balancing is proposed in this work which distributes workloads among multiple fog nodes. It assigns IoT devices to suitable for base stations and fog nodes for all data flows. A queuing model is proposed which balances the workload for multiple fog nodes located in nearest region.

**PAPER 2**

*Title* – A Fog based Security Framework for Intelligent Traffic Light Control System

**Concept** – In this paper, intelligent transportation systems (ITS) based application is proposed which based on fog based security framework. The proposed framework is called FSF-ITLCS that comprised of three components such as Department of Motor Vehicles (DMV), Road Side Units (RSUs), and Vehicles and also the proposed work addresses various security attacks such as Sybil, DoS and Impersonation and Replay.

**Limitations**

- Overall computation time is high

**PAPER 3**

*Title* – Lightweight Authentication and Matrix-based Key Agreement Scheme for Healthcare in Fog Computing

**Concept** – In this paper, matrix-based key agreement and lightweight authentication schemes are considered to make communication via fog computing. The proposed lightweight authentication technology is presented for the aim of verify multi-party identities. In matrix-based key agreement technology, healthcare data is encrypted and uploads into cloud server.

**Limitations**

- Encryption and decryption time is high

**PAPER 4**

*Title* – Architecture for Latency Reduction in Healthcare Internet-of-Things using Reinforcement Learning and Fuzzy based Fog Computing

**Concept** – In this paper hybrid approach is proposed which is an integration of reinforcement learning and fuzzy logic scheme. The major purpose of this hybrid approach is to integrate healthcare IoT devices with cloud environment for provide fog services. The proposed integrated FRLDPA algorithm is proposed to assign packets to different processors of virtual machines available in fog gateway.

**Limitations**

- Service latency is high in the application layer

**PAPER 5**

*Title* – Hybrid Evolutionary Scheduling for Energy Efficient Fog-Enhanced Internet of Things

**Concept** – In this paper, authors have evaluated the resource scheduling problem which reduces makespan and energy consumption. A multi-objective EDA with partition operator is adopted which divides the graph and find the task processing permutation and processor assignment.

**Limitations**

- In real time application scenario, the makespan and energy consumption of devices are large

**PAPER 6**

*Title* – Fog Computing for Energy-Aware Load Balancing and Scheduling in Smart Factory

**Concept** – In this paper, authors have proposed an energy-aware load balancing and scheduling (ELBS) is proposed, which is based on fog computing. Initially, fog node workload is considered which is based on the energy consumption model. The improved particle swarm optimization (PSO) is proposed to obtain an optimal solution and the priority for tasks achievement is considered under manufacturing cluster. Finally, a multi-agent system is considered to achieve the distributed scheduling of clusters in manufacturing.



**Limitations**

- The proposed ELBS scheme is considered on complex energy consumption problem in the smart manufacturing

**PAPER 7**

*Title* – An Efficient Indexing Model for the Fog Layer of Industrial Internet of Things

**Concept** – In this paper, fog nodes are deployed in industrial IoT, which restrain their efficiency by providing appropriate services to the clients. In this paper, a new indexing model is proposed which is based on the relations. The proposed method named DM-index model, which considered for service retrieval and maintenance in the fog layer of industrial applications. In this paper authors have concentrated multi-level indexing and also perform various indexing operations.

**Limitations**

- This approach is not suitable for adaptive environment

**PAPER 8**

*Title* – Service Popularity-based Smart Resources Partitioning for Fog Computing Enabled Industrial Internet of Things

**Concept** – In this paper, smart resources partitioning is proposed in fog computing enabled IIoT. We firstly exploit Zipfs law to measure the relationship between popularity ranks of computing control layer from data processing layer of IIoT. The proposed scheme noted the simulation result for successful response time, delay time and response rate.

**Limitations**

- High complexity due to large number of fog nodes are geographically distributed in the computing layer.

**PAPER 9**

*Title* – Secure Deduplication with Reliable and Revocable Key Management in Fog Computing

**Concept** – In this paper secure deduplication technique is proposed to eliminate the redundant copies of data and also stores single copy of the data. This paper solves two major problems in this domain that are key management and dynamic ownership management. In key management, convergent encryption scheme generates number of encryption keys whose size is large with the unique contents whereas dynamic ownership management is added with the support of fog device data ownership.

**Limitations**

- Communication cost in server side is high when the number of users/requests are high

**PAPER 10**

*Title* – A Study on the Design of Fog Computing Architecture using Sensor Networks

**Concept –** In this paper**,** a fog computing architecture is proposed which deliver IoT data in efficient manner. With the support of fog computing, the proposed fog computing architecture provides efficient and time sensitive energy management in IoT device communication among sensors. Furthermore, secure data management is employed to decrypt IoT data by user attributes.

**Limitations**

- The proposed fog computing architecture solves latency in service response time and does not consider high QoS metrics and also security oriented metrics.
- Due to its simple development of architecture, it is supported for low latency and low network traffic based fog environment
- This paper considers static IoT environment that does not move freely in the network and also does not considers dynamic arrival of new nodes

**PAPER 11**

*Title* – Secure Data Storage and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing

**Concept –** In IIoT, a large amount of data is generated in different sources. However IoT devices are vulnerable and insecure to various threats. Hence in this paper authors presented various key concepts such as data processing, secure data storage, effective data retrieval and dynamic collection of data by different sources. For above functions, fog computing and cloud computing is integrated and various security schemes are proposed for data confidentiality.

**Limitations**

- High query processing cost due to ID-AVL tree since AVL tree asymptotically faster, but rebalance time is high
- Secure KNN algorithm is computationally very expensive and thus privacy preserving data search is difficult

- Secure KNN is not suitable for dense area and also not suitable for large amount of data (real data set) processing

**PAPER 12**

*Title* – P-SEP: A Prolong Stable Election Routing Algorithm for Energy-Limited Heterogeneous Fog-Supported Wireless Sensor Networks

**Concept** – In this paper, P-SEP protocol is proposed in energy constrained fog-assisted WSNs. The major contributions of this paper are follows: (1). P-SEP protocol controls the random selection of CH for each round. (2). P-SEP exploits heterogeneity energy threshold to avoid less residual energy nodes are nominated as CH in the next rounds, (3). CH optimize the minimum distance between the CHs and fog nodes, (4) Increases energy efficiency of fog nodes and decreases the overhead

**Limitations**

- P-SEP protocol does not consider any priority to select CHs which increases energy consumption in WSN
- High communication overhead and packet loss under fog assisted WSN



**PAPER 13**

*Title* – Privacy-aware Task Allocation and Data Aggregation in Fog-Assisted Spatial Crowdsourcing

**Concept** – In this paper spatial crowdsourcing assisted task owners based task allocation and data aggregation have been proposed via fog computing. The SC server is enabled to collect the sensed information from mobile users. Data aggregation is a specific task which has drawn much attention in mining the massive spatial crowdsensing data. The fog nodes are deployed in several regions, which can assist the SC server to distribute tasks and aggregate data in a privacy aware manner.

**Limitations**

- Privacy of participants such mobile users are lacking due to inefficient cryptography scheme

**PAPER 14**

*Title* – Industrial IoT Data Scheduling based on Hierarchical Fog Computing: A Key for Enabling Smart Factory

**Concept** – In this paper, industrial internet of things (IIoT) based technology in industry based applications is considered. In this paper a hierarchical fog server's based deployment is considered in real time constraints, particularly in big factories. In this work, industry based IoT sensed data is categorized into two categories such as high priority and low priority. The high priority requests are scheduled firstly since it's based on emergency or urgent demands. In addition, a workload assignment algorithm is used to offload high load of fog nodes over higher fog tiers.

**Limitations**

- In this work, end-to-end delay is large due to large amount of workloads at fog tier



**PAPER 15**

*Title* – Adaptive Fog Configuration for the Industrial Internet of Things

**Concept** – In this paper, different industrial services are like imminent failure detection, and automatic monitoring control is provided at the fog nodes, which improve the performance of industrial systems. Online distributed algorithm called adaptive fog configuration based Lyapunov Optimization and Parallel Gibbs Sampling is proposed.

**Limitations**

- The proposed work is not suitable for real world application.

BIBILIOGRAPHY

Abbas, N., Asim, M., Tariq, N., Baker, T., & Abbas, S. (2019). A Mechanism for Securing IoT-enabled Applications at the Fog Layer. J. Sensor and Actuator Networks, 8, 16.

Borujeni, E. M., Rahbari, D., & Nickray, M. (2018). Fog-based energy-efficient routing protocol for wireless sensor networks. The Journal of Supercomputing.

Guan, Z., Zhang, Y., Wu, L., Wu, J., Li, J., Ma, Y., & Hu, J. (2019). APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT. J. Network and Computer Applications, 125, 82-92.

Ni, J., Zhang, K., Yu, Y., Lin, X., & Shen, X. S. (2018). Providing Task Allocation and Secure Deduplication for Mobile Crowdsensing via Fog Computing. IEEE Transactions on Dependable and Secure Computing, 1–1.

Liu, Z., & Li, S. (2018). Sensor-cloud data acquisition based on fog computation and adaptive block compressed sensing. International Journal of Distributed Sensor Networks, vol. 14. Issue. 9, 155014771880225.

Fan, Q., & Ansari, N. (2020). Towards Workload Balancing in Fog Computing Empowered IoT. IEEE Transactions on Network Science and Engineering, 7, 253-262.

Khalid, T., Khan, A. N., Ali, M., Adeel, A., ur Rehman Khan, A., & Shuja, J. (2018). A fog-based security framework for intelligent traffic light control system. Multimedia Tools and Applications.

Shen, J., Yang, H., Wang, A., Zhou, T., & Wang, C. (2018). Lightweight authentication and matrix-based key agreement scheme for healthcare in fog computing. Peer-to-Peer Networking and Applications.

Shukla, S., Hassan, M. F., Jung, L. T., & Awang, A. (2018). Architecture for Latency Reduction in Healthcare Internet-of-Things Using Reinforcement Learning and Fuzzy Based Fog Computing. Recent Trends in Data Science and Soft Computing, 372–383.

Wu, C., Li, W., Wang, L., & Zomaya, A. (2018). Hybrid Evolutionary Scheduling for Energy-efficient Fog-enhanced Internet of Things. IEEE Transactions on Cloud Computing, 1–1.

Wan, J., Chen, B., Wang, S., Xia, M., Li, D., & Liu, C. (2018). Fog Computing for Energy-aware Load Balancing and Scheduling in Smart Factory. IEEE Transactions on Industrial Informatics, 1–1.

Miao, D., Liu, L., Xu, R., Panneerselvam, J., Wu, Y., & Xu, W. (2018). An Efficient Indexing Model for the Fog Layer of Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 1–1.

Li, G., Wu, J., Li, J., Wang, K., & Ye, T. (2018). Service Popularity-based Smart Resources Partitioning for Fog Computing-enabled Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 1–1.

Kwon, H., Hahn, C., Kang, K., & Hur, J. (2018). Secure deduplication with reliable and revocable key management in fog computing. Peer-to-Peer Networking and Applications.

Cha, H.-J., Yang, H.-K., & Song, Y.-J. (2018). A Study on the Design of Fog Computing Architecture Using Sensor Networks. Sensors, vol. 18, issue. 11, 3633.

Fu, J., Liu, Y., Chao, H.-C., Bhargava, B., & Zhang, Z. (2018). Secure Data Storage and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing. IEEE Transactions on Industrial Informatics, 1–1.

Naranjo, P. G. V., Shojafar, M., Mostafaei, H., Pooranian, Z., & Baccarelli, E. (2016). P-SEP: A prolong stable election routing algorithm for energy-limited heterogeneous fog-supported wireless sensor networks. The Journal of Supercomputing, vol. 73, issue.2, 733–755.

Wu, H.-Q., Wang, L., & Xue, G. (2019). Privacy-aware Task Allocation and Data Aggregation in Fog-assisted Spatial Crowdsourcing. IEEE Transactions on Network Science and Engineering, 1–1.

Chekired, D. A., Khoukhi, L., & Mouftah, H. T. (2018). Industrial IoT Data Scheduling based on Hierarchical Fog Computing: A key for Enabling Smart Factory. IEEE Transactions on Industrial Informatics, 1–1.

Chen, L., Zhou, P., Gao, L., & Xu, J. (2018). Adaptive Fog Configuration for the Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 1–1.