Ph.D. Research Proposal

Doctoral Program in “Department Name”

ProFeC-IoT: Novel Protected Fog Enabled Cloud Environment for IoT Applications Using Blockchain and Secure Offloading Technique

by

<Name of the Candidate>

<Reg. No of the Candidate>

<Supervisor Name>

<Date of Submission (DD MM 20YY>

1. INTRODUCTION

Internet of Things (IoT) is an developing technology that enables keener world by using current communication and computing technologies [1]. In real-world, the IoT applications like smart city, e-healthcare, smart transportation, smart factory have contributed the enormous advantages. Cloud computing [2] is the one of the enabling technologies of IoT which provides the next generation internet based scalable distributed computing systems. Fog computing which is another distributed computing system has been widely adapted to address the latency of cloud computing and to deliver more sophisticated IoT services to users [3]. This distributed nature of fog computing has combined it with growing IoT applications [4]. In recent studies, IoT, cloud, and fog computing have been collaborated to ensure better performance [5]6. This combined environment opens up the way towards many real-time applications, smart building is one of them. Still, cloud, fog, and IoT have been subjected to many security threats [6]. Thus provisioning security becomes major challenging issue in fog-cloud-IoT environment.

As bring up earlier, security is a major aspect in IoT environment. In order to preserve data security an AES-GMAC operation was performed to balance security level and complexity [7]16. Here, high complexity of AES algorithm makes it as not suitable for resource constrained IoT environment. To enable effectual authentication, Physically Unclonable Functions (PUFs) have been utilized in cloud, and fog based IoT systems [8]17, [9]19. Although PUFs are highly secure, they have been only used for authentication but unable to ensure data security. Blockchain based techniques were also considered for providing security in IoT environment [10]20, [11]21. However, with remote user authentication is alone it is unable to ensure security. Further, using complex encryption schemes often increases energy consumption of devices. In fog layer, IDS system was equipped to detect malicious data in IoT systems [12]22. In the absence of secure offloading, the performance of the system will be degraded. Task offloading was enabled to improve scalability [13]23, energy efficiency [14]24, and latency [15]25. But absence of security mechanisms increases the vulnerability in the system.

2. Problem Statement

Though considerable works have been held on fog cloud IoT environment, there is security provisioning is still challenging in following aspects,

- ☑ Strong authentication for remote Users and IoT devices
- ☑ Data security for IoT data using lightweight cryptosystems
- ☑ Secure offloading to improve performance
- ☑ Secure searching and storage over cloud environment

2.1 Preliminary Literature Review

In this paper, the authors have presented an edge based smart healthcare for remote monitoring. The concept of edge computing is introduced to mitigate the problem of latency in healthcare applications. In the presence of edge computing, the severity level of the patient can be detected at the edge of network instead of processing at the cloud. This processing minimizes the latency for emergency applications considerably. The proposed system computed criticality measure index (CMI) from the gathered wearable data. Then alert message is triggered in emergency situations.

Paper 2

Title: Handling Big Data Using MapReduce Over Hybrid Cloud

Concept

Hybrid cloud comprises both public and private clouds in order to achieve better scalability and security. In majority of researches, public cloud is used to store the critical information while public cloud is used for non-critical data. In this paper, MapReduce framework is applied for hybrid cloud. Herein MapRduce framework is adapted to fetch data from hybrid cloud.

Paper 3

Title: Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach

Concept

In this paper, authors have presented a smart healthcare system by designing a fog-enabled gateway. The fog computing based gateway design explores a geo-distributed intermediary layer of intelligence. This layer is introduced between the sensors and the cloud. In fog enabled healthcare systems, the fog node takes the responsibility of the sensors such as severity detection. The authors have highlighted that use of fog layer in the e-healthcare system improves energy efficiency, scalability and reliability problems and also supports user mobility. Therefore, fog computing plays pivotal role in e-healthcare applications.

Paper 4

Title: Fog-based Computing and Storage Offloading for Data Synchronization in IoT

Concept

This paper proposes a fog-based IoT environment with effective offloading scheme. In this work, data privacy is provided by offloading a part of computational and storage to fog nodes. Fog-based differential synchronization algorithm is proposed to reduce communication cost and latency. This work mainly concentrates on minimizing the redundant communication due to frequent data modification. Thus, the synchronization is performed in the fog layer. To preserve user privacy, Reed-Solomon code is introduced.

Paper 5

Title: A Method Based on the Combination of Laxity and Ant Colony System for Cloud-Fog Task Scheduling

Concept

A laxity and ant colony system (LBP-ACS) is proposed for handling task scheduling in cloud-fog environment. The proposed LBP-ACS algorithm considers the priority as well as deadline of the task for scheduling. The priority algorithm adopts the laxity-based algorithm to construct the task scheduling sequence. The cloud-fog broker is responsible for analyzing and estimating tasks and resources. Based on the analyzed resources, ant colony system assigns the tasks to fog nodes. However, ant colony algorithm is relatively slow which increases the time consumption.

Paper 6

Title: A Hesitant Fuzzy Based Security Approach for Fog and Mobile-Edge Computing

Concept

In this paper, security of fog computing is majorly concentrated. In fog computing, security is one of the major services. This paper presents a Soft Hesitant Fuzzy Rough Set (SHFRS) approach. The SHFRS is applied to solve the multi-criteria decision making problems. The SHFRS is the extension of hesitant fuzzy rough set theory by fusing it with the hesitant fuzzy soft set. This paper presents upper and lower approximation operators for SHFRS. Finally, the SHFRS is applied to select optimal security service in fog environment.

Paper 7

Title: Preserving data security in distributed fog computing

Concept

In this paper, AES-GMAC operation is proposed to ensure security in distributed fog computing based IoT environment. Here authors have concentrated on data confidentiality, integrity, and availability along with source authentication. In order to balance security level and computational complexity a dynamic key-dependent approach is proposed. Data encryption is performed by fog nodes along with the keys of n-neighbor nodes in order to complicate the decryption process for attackers.

Problem

- In general, AES increases complexity which is not suitable for resource constrained environment. Further, adding computations to AES algorithm increases complexity level.

Proposed Solution

- Hybrid hummingbird encryption scheme is proposed which is a ultra-lightweight protocol and suitable for resource constrained environment

Paper 8

Title: A PUF-based mutual authentication scheme for Cloud-Edges IoT systems

Concept

In this paper, mutual authentication is performed based on physically unclonable functions (PUFs) which is a special integrated circuits provided with unclonability, uniqueness, and tamper-evident properties. In this work, three-tier architecture is designed and the authentication protocol is designed to meet all constraints of three-tier architecture.

Limitation

- Not able to ensure data security as well as user authentication

Proposed Solution

- An ultra-lightweight encryption algorithm is proposed for data security
- Blockchain based authentication is enabled for user authentication

Paper 9

Title: A Privacy-Preserving, Mutual PUF-Based Authentication Protocol

Concept

In this paper, a hardware embedded delay PUF (HELP) is presented to enable mutual authentication. In this approach, AES and SHH-3 are implemented in order to introduce randomness in PUF authentication. The PUF alternative bitstrings are stored in a secure server (verifier). The authors have highlighted that privacy and security is ensured by using HELP protocol.

Limitation

- Although PUF enables strong authentication it is able to ensure data security

Proposed Solution

- Hybrid hummingbird algorithm is proposed for data security

Paper 10

Title: BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0

Concept

In this paper, blockchain based mutual authentication scheme is proposed and named as BseIn which enforces authentication along with fine access control policies. The proposed system is integrated with attribute signature, multi-receiver encryption, and message authentication code. Privacy and security is guaranteed with anonymous authentication, auditability, and confidentiality.

Problem and limitations

- Remote user authentication is provided with blockchain technology however IoT nodes are unauthorized which increases the possibility of compromising IoT nodes
- The generated data is not ensured with security which increases the vulnerability

Proposed Solutions

- Both user and IoT node authentication is proposed
- Hybrid hummingbird based encryption scheme is proposed

Paper 11

Title: A Secured Proxy-Based Data Sharing Module in IoT Environments Using Blockchain

Concept

A secure proxy re-encryption scheme is proposed with inner-product encryption scheme to ensure security with access control in IoT. Here blockchain network is utilized for re-encryption. The processing nodes of blockchain network are act as the proxy server and perform re-encryption process. For primary users, the data is delivered without re-encryption and for secondary users the data is re-encrypted by proxy server.

Problem and limitation

- Efficiency of this system needs improvement in terms of time consumption
- Involvement of attribute based encryption in re-encryption increases time consumption

Proposed Solution

- Ultra-lightweight hybrid hummingbird encryption scheme is proposed for data security which minimizes time consumption

Paper 12

Title: Design of Cognitive Fog Computing for Intrusion Detection in Internet of Things

Concept

This paper presents an intrusion detection system (IDS) to detect malicious activities in IoT environment. For IDS, online sequential extreme learning machine (OS-ELM) algorithm is proposed. Herein intrusion detection is performed in a decentralized manner in which fog nodes are assisted in IDS. Authors have highlighted that scalability, flexibility, and interoperability have improved in their work.

Problem

- However IDS is performed in each fog node according the data received from IoT devices. Thus there is high possibility for a fog node to become overloaded. Thus effectual offloading is required to support improved performance.

Proposed Solution

- Intelligent secure offloading is performed based on ISOMAP algorithm which improves the efficiency.

Paper 13

Title: Efficient and dynamic scaling of fog nodes for IoT devices

Concept

In this paper, scalability is concentrated in fog-IoT environment. Here a queuing mathematical and analytical model is designed to support effective scalability. Herein the minimal number of fog nodes is identified under any offered IoT workload. Thus the number of fog nodes to be deployed to handle the IoT workload is determined by this work.

Problem

- In order to handle IoT workload in fog layer, offloading is an effective approach which is not focused in this work

Proposed Solution

- Intelligent secure offloading is performed based on ISOMAP algorithm which improves the efficiency.

Paper 14

Title: Joint energy and latency optimization for upstream IoT offloading services in fog radio access networks

Concept

This paper presents a joint energy and latency optimization (JELO) scheme is presented for upstream IoT offloading. The system is designed with IoT devices, high-capacity fog servers, medium capacity fog servers, and low capacity fog servers. The resource required by individual task is considered as major constraint for making offloading decision.

Problem

- However, in IoT environment security is major constraint which is not considered in this work

Proposed Solution

- Intelligent secure offloading is performed based on ISOMAP algorithm which improves the efficiency.

Paper 15

Title: Energy and time efficient task offloading and resource allocation on the generic IoT-fog-cloud architecture

Concept

In this paper a generic IoT-fog-cloud architecture is considered and energy efficient task offloading is performed. An energy and time efficient computation offloading and resource allocation (ETCORA) algorithm is proposed in which both computation offloading and transmission power allocation is performed jointly. The major objective this work is to minimize energy consumption and time consumption.

Problem

- Security is a major constraint in fog-IoT environment which is not considered in this work

Proposed Solution

- Intelligent secure offloading is performed based on ISOMAP algorithm which improves the efficiency.

3. PROBLEM DEFINITION

Problem Statement: Security in IoT environment is the major objective of this research work which has been focused by many researchers. However, we formulate our problem as follows,

"In current studies, security provisioning in Fog-Cloud-IoT environment is ineffective due to lack of decentralized authentication, data security, and secure offloading processes". The major issues in IoT environment are,

☑ Complex cryptography schemes
☑ Lack of key generation and preservation schemes
☑ Ineffectual and centralized authentication schemes
☑ Performance degradation by ineffectual offloading

The detailed problem definition is given as follows,

Paper 16

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

Concept

This paper focuses on secure data storage, data retrieval, and data aggregation. Fog and cloud computing is integrated with Industrial IoT (IIoT) in order to improve the system efficiency. Initially, the data from IIoT devices is aggregated by fog nodes. Local data (control information) is stored locally in fog nodes and the long-term data is stored in cloud. Before transmitting to cloud, the data is encrypted by proxy server using symmetric scheme. Here ID-AVL tree is constructed based on hash functions and retrieval feature (RF) tree is constructed. Searching is carried out by secure KNN approach.

Problems

- In symmetric scheme, whenever data is retrieved by user it is necessary to exchange secret key. When the number of exchange is increased, then the vulnerability on data is also increased.
- User response time is high since the search time must be carried out on both ID-AVL and RF tree

Limitations

- New indexing structure is required to improve efficiency and to support all type of search
- Lack of authentication causes unauthorized user access

Proposed Solutions

- Hybrid hummingbird encryption scheme is used which is lightweight and also preserves access control
- AA-Tree is proposed for secure indexing which supports searching, insertion, and deletion without complexity
- Attributed based blockchain network is presented for user authentication

Paper 17

Title: APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT

Concept

In this paper, multi authorities are allowed to authenticate IoT users. This 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). 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 RSA based key generation for every user. For encryption, paillier scheme based key is generated for every user. The data is encrypted by smart devices and aggregated by fog nodes and then decrypted by cloud server.

Problems

- Key generation by RSA and Paillier scheme increases time consumption for authentication
- Aggregated data is decrypted in public cloud in order to enable searching on stored data. However, decryption of data in public cloud increases vulnerability of data but Paillier and RSA support homomorphic operations on encrypted data.

Proposed Solutions

- Proposed hybrid hummingbird scheme is ultra-lightweight which minimizes time consumption
- Secure indexing by AA-tree is proposed which enables secure searching over encrypted data
- Data is secured by hybrid hummingbird encryption scheme

Paper 18

Title: Advanced lightweight multi-factor remote user authentication scheme for cloud-IoT applications

Concept

In this paper, the authors have designed a lightweight remote user authentication scheme over internet of things. The three factors used for registration is id, password and random number. On submitting these three parameters into server, then it generates id, password with random number by performing XOR operation. Further, these entities are stored into users‟ smart card which is required to login into the server and create a session key. If the user needs to change the password, then it is essential to present smart card into the reader.

Problems

- The entire authentication system depends upon smart card which user must hold every time

- If smart card is stolen or tampered the authentication will be failed since password and key can be cracked by hacker easily

Proposed Solutions

- Authentication is performed by attribute based blockchain network which improves the authentication efficiency
- Multiple user attributes are considered for authentication and stored in blockchain which is difficult to hack

Paper 19

Title: SecOFF-FCIoT: Machine learning based secure offloading in Fog-Cloud of things for smart city applications

Concept

In this paper authors have proposed a secure offloading scheme in fog-cloud-IoT. The data generated by IoT devices is offloaded to fog nodes through smart gateway. Before offloading, gateway ensures security by classifying the aggregated data into normal and malicious based on sensed value and time. Then gateway selects optimal fog node for offloading by PSO algorithm. In fog node, offloading decision is taken based on sensitivity level of data. For classification, reinforcement learning approach is proposed. Finally, non-sensitive data is offloaded to public cloud and sensitive data is offloaded to private cloud.

Problem

- Offloading decision by PSO algorithm is inefficient and takes much more time for offloading

Limitations

- Data security is not ensured since the stored in cloud is subjected to many security threats
- Blockchain based security can be enabled

Proposed Solution

- New locally connected topology is designed in fog layer and ISOMAP based topology extraction algorithm is proposed
- Data security is ensured by lightweight cryptography scheme
- Attribute based blockchain network is proposed for authentication

Paper 20

Title: Encryption Protocol for Resource-Constrained Devices in Fog-Based IoT using One-Time Pads

Concept

In this paper, an encryption scheme is proposed for resource constrained devices in fog-IoT. Authors have highlighted that the proposed algorithm is also suitable for resource constrained fog nodes. Here encryption is performed based on one time pad (OTP) which is sued as secret key. Each OTP can be used for single encryption and decryption. OTPs are generated by random number generator (RNG). The security level of encryption scheme depends upon the randomness introduced by RNG.

Problems

- However, RNG needs to generate multiple OTPs high randomness which increases overhead on resource constrained devices
- Scalability is also major issues since when number of nodes increases then the number of OTPs are also increased. Thus this method is not suitable for large scale networks.

Proposed Solutions

- Encryption by hybrid hummingbird algorithm increases data security without complexity
- Data encryption is performed by fog nodes in a distributed manner which supports high scalability

4. PROPOSED WORK

This research work aims to overthrow all research problems in prior research works. In this work a **novel ProFeC-IoT environment** which combines IoT with cloud computing and fog computing in a protected manner. The proposed ProFeC-IoT environment is comprised with three different layers as follows,

- ☑ IoT layer-IoT devices such as sensors, actuators, and access points (APs)
- ☑ Fog layer-Fog nodes and Master nodes
- ☑ Cloud layer-Cloud server

Objectives

The major objectives of this work is listed as follows,

- ☑ To improve security in IoT environment with both user and data level security
- ☑ To improve system performance by secure offloading
- ☑ To enable secure searching over cloud environment

Proposed Methodology

1. *Secure data aggregation*

Data aggregation is performed in IoT layer in which the sensed data are aggregated by SAPs. At SAPs, all IoT nodes are authenticated before data transmission in order to ensure security in IoT layer. For enabling authentication, **Hardware Mutual Authentication (HMA)** is proposed. Thus the SAPs collect data from only authorized nodes to ensure security. Further, SAPs construct Dentrimer-Tree for data in order to enable secure search in cloud environment.

2. *Ultra-lightweight data encryption*

The aggregated data is fused by SAPs and transmitted to nearest fog node to provide data security. Instead of encrypting all data by SAPs, the encryption task is assigned to distributed fog layer. In fog layer, the data is encrypted by using **Hybrid Prince Encryption (HPE)** algorithm. In HPE algorithm, attribute based encryption scheme is integrated with hummingbird algorithm in order to ensure high level security. Furthermore, fog node encrypts the Dentrimer-Tree by using Paillier encryption scheme.

3. *Distributed Task offloading*

The encryption task is assigned by SAPs to the nearer fog nodes which increases load on particular fog node. In order to handle this issue, secure offloading is performed in ProFeC-IoT environment. For efficient task offloading, the fog nodes are organized in an **Master-Slave Connected Topology (M-SCT) topology** in fog layer. For secure offloading, Master node extracts the topology information by **ISOMAP** scheme and makes offloading decision based on extracted information.

4. *Decentralized user authentication*

When a remote user needs to search data over cloud environment, the user must be authenticated before accessing IoT data. For decentralized and strong authentication, **Attribute aware DODAG Blockchain Network (A2-DBN)** is utilized in this work. In blockchain network, the users are authenticated based on user attributes and then allowed to search over cloud environment. After authentication is completed, the user requested data is searched over Dentrimer-tree and retrieved to the user.

<u>Performance Metrics</u>

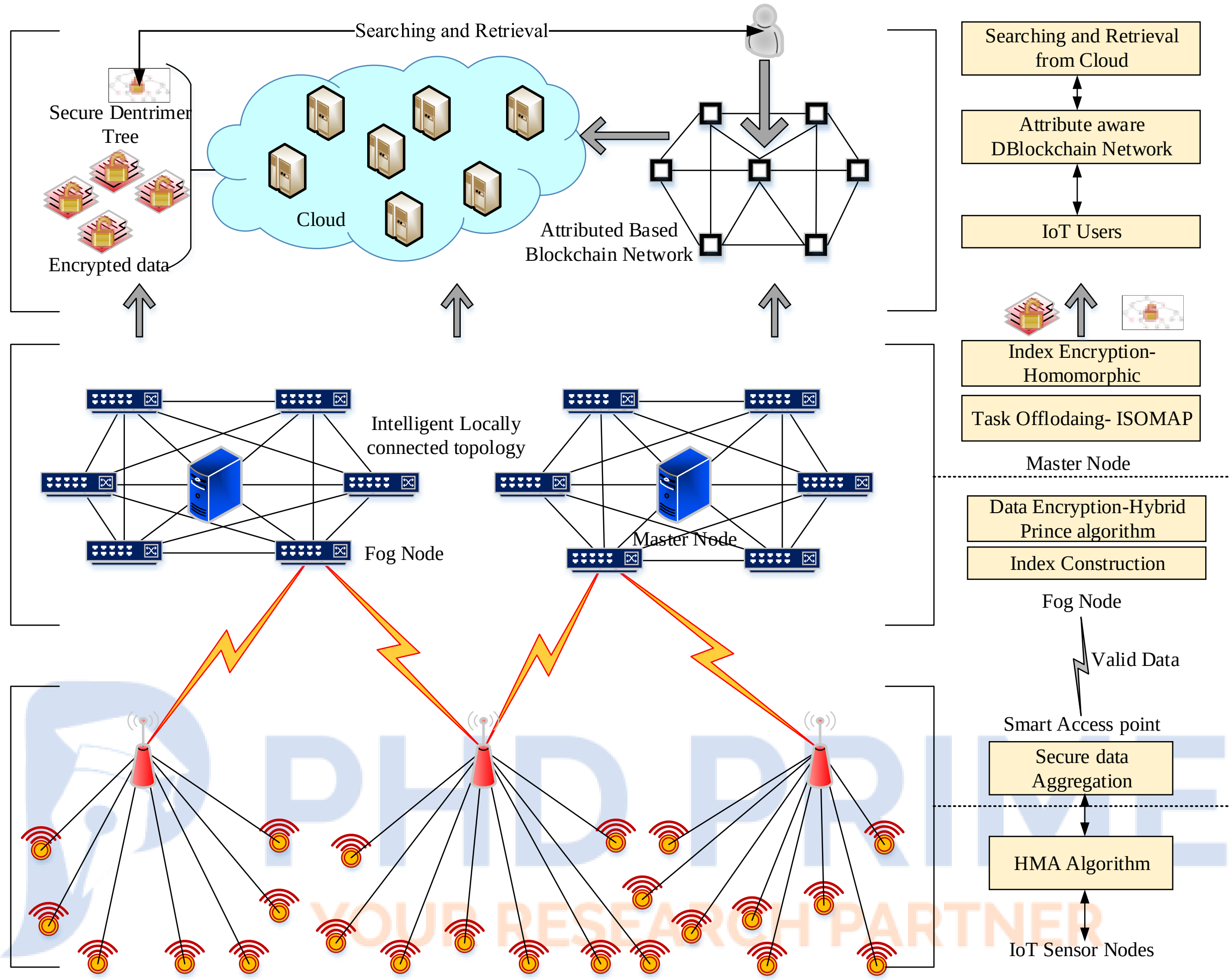
The proposed system is evaluated based on following performance metrics,

- ☑ Energy consumption
  - ✓ In IoT layer
  - ✓ In fog layer
- ☑ Throughput
- ☑ Encryption time
- ☑ Decryption time
- ☑ Authentication time
  - ✓ Hardware based

- ✓ Blockchain based

☑ Response time

Architecture of Proposed ProFeC-IoT Environment


Searching and Retrieval
Secure Dentrimer Tree
Encrypted data
Cloud
Attributed Based Blockchain Network
Intelligent Locally connected topology
Fog Node
Master Node
Searching and Retrieval from Cloud
Attribute aware DBlockchain Network
IoT Users
Index Encryption-Homomorphic
Task Offlodaing- ISOMAP
Master Node
Data Encryption-Hybrid Prince algorithm
Index Construction
Fog Node
Valid Data
Smart Access point
Secure data Aggregation
HMA Algorithm
IoT Sensor Nodes

References

Pathinarupothi, R.K., Durga, P., & Rangan, E. (2018). IoT-Based Smart Edge for Global Health: Remote Monitoring With Severity Detection and Alerts Transmission. IEEE Internet of Things Journal, 6, 2449-2462.

Saxena, A., Chaurasia, A., Kaushik, N., & Kaushik, N. (2018). Handling Big Data Using MapReduce Over Hybrid Cloud. Lecture Notes in Networks and Systems, 135–144. doi:10.1007/978-981-13-2354-6_16.

Rahmani, A.M., Gia, T.N., Negash, B., Anzanpour, A., Azimi, I., Jiang, M., & Liljeberg, P. (2018). Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. Future Generation Comp. Syst., 78, 641-658.

Wang, T., Zhou, J., Liu, A., Bhuiyan, M.Z., Wang, G., & Jia, W. (2019). Fog-Based Computing and Storage Offloading for Data Synchronization in IoT. IEEE Internet of Things Journal, 6, 4272-4282.

Xu, J., Hao, Z., Zhang, R., & Sun, X. (2019). A Method Based on the Combination of Laxity and Ant Colony System for Cloud-Fog Task Scheduling. IEEE Access, 7, 116218-116226.

Rathore, S., Sharma, P.K., Sangaiah, A.K., & Park, J.H. (2018). A Hesitant Fuzzy Based Security Approach for Fog and Mobile-Edge Computing. IEEE Access, 6, 688-701.

Noura, H., Salman, O., Chehab, A., & Couturier, R. (2019). Preserving Data Security in Distributed Fog Computing. Ad Hoc Networks, 101937.

Barbareschi, M., De Benedictis, A., La Montagna, E., Mazzeo, A., & Mazzocca, N. (2019). A PUF-based mutual authentication scheme for Cloud-Edges IoT systems. Future Generation Computer Systems.

Wang, D., Bai, B., Lei, K., Zhao, W., Yang, Y., & Han, Z. (2019). Enhancing Information Security via Physical Layer Approaches in Heterogeneous IoT With Multiple Access Mobile Edge Computing in Smart City. IEEE Access, 7, 54508–54521.

Che, W., Martin, M., Pocklassery, G., Kajuluri, V.K., Saqib, F., & Plusquellic, J. (2017). A Privacy-Preserving, Mutual PUF-Based Authentication Protocol. Cryptography, 1 (3).

Lin, C., He, D., Huang, X., Choo, K.-K. R., & Vasilakos, A. V. (2018). BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. Journal of Network and Computer Applications, 116, 42–52.

Obour Agyekum, K., Xia, Q., Sifah, E., Gao, J., Xia, H., Du, X., & Guizani, M. (2019). A Secured Proxy-Based Data Sharing Module in IoT Environments Using Blockchain. Sensors, 19(5), 1235.

Prabavathy, S., Sundarakantham, K., & Shalinie, S. M. (2018). Design of cognitive fog computing for intrusion detection in Internet of Things. Journal of Communications and Networks, 20(3), 291–298.

El Kafhali, S., & Salah, K. (2017). Efficient and dynamic scaling of fog nodes for IoT devices. The Journal of Supercomputing, 73(12), 5261–5284.

Vu, D.-N., Dao, N.-N., Jang, Y., Na, W., Kwon, Y.-B., Kang, H., … Cho, S. (2018). Joint energy and latency optimization for upstream IoT offloading services in fog radio access networks. Transactions on Emerging Telecommunications Technologies, e3497.

Sun, H., Yu, H., Fan, G., & Chen, L. (2019). Energy and time efficient task offloading and resource allocation on the generic IoT-fog-cloud architecture. Peer-to-Peer Networking and Applications.

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.

Guan, Z., Zhang, Y., Wu, L., Wu, J., Li, J., Ma, Y., & Hu, J. (2018). APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT. Journal of Network and Computer Applications.

Sharma, G., & Kalra, S. (2019). Advanced lightweight multi-factor remote user authentication scheme for cloud-IoT applications. Journal of Ambient Intelligence and Humanized Computing.

Alli, A. A., & Alam, M. M. (2019). SecOFF-FCIoT: Machine learning based secure offloading in Fog-Cloud of things for smart city applications. Internet of Things, 7, 100070.

Boakye-Boateng, K., Kuada, E., Antwi-Boasiako, E., & Djaba, E. (2019). Encryption Protocol for Resource-Constrained Devices in Fog-Based IoT using One-Time Pads. IEEE Internet of Things Journal, 1–1.