International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

# Innovative Fog Cloud Offloading Scheme for Security Enhancement in Mobile System

*[1]Mr. G. Prabu, [2]K. Murali, [3]K. S. Thirunaarayan, [4]S. GokulaKrishnan.*

[1,2,3,4]Sri Manakula Vinayagar Engineering College, Puducherry, India

**ABSTRACT**

Running sophisticated software on smartphones could result in poor performance and be shortened. Recently, Fog Cloud computation workload to the cloud has become a promising solution to enhance both performance and security. However, it also consumes both time and energy to upload data or programs to the cloud and retrieve the results from the cloud. FC reduces network pressures by bringing resource-intensive functions closer to clients.

## I. INTRODUCTION

Fog computing is a middle layer between cloud data centers and IoT devices/sensors. provides computing services of computation along with storage and networking close to the IoT devices/sensors. The fog computing. This concept is based on Edge computing. proximity of iot devices sensors. the fog computing concept is derived from edge computing Because of their limited resources, edge devices in Edge computing are unable to support multiple applications in IoT, resulting in resource contention and increased latency. It integrates edge devices and cloud resources to overcome the limitations of Edge computing..By moving resource-intensive tasks including compute, analytics, communication, and storage closer to the clients, fog computing (FC), a new architecture, intends to minimize network stresses throughout the core network and cloud computing (CC). In order to overcome the issue of excessive energy utilization with electricity for Internet-of-Things (IoT) apps that require speed, FC systems can employ intelligence features to profit from data that is easily accessible with computational resources FC apps and services generate large volumes of data.

Furthermore, Deep Learning (DL), an important field, has made significant progress in a variety of research areas, including robotics, face recognition, neuromorphic computing, decision-making, computer Corporation report, there will be directly related to the quantity of data transmitted through IoT devices 41.6 billion to 1 trillion IoT devices and that will generate a huge to the cloud. Due to this reason, it causes a low quality of service

Fog computing is a decentralized computing infrastructure in data, compute, storage and applications are located somewhere between the data source and the cloud. Fog computing, like edge computing, brings the benefits and power of the cloud closer to where data is created and acted on.. Because both bring data mining and processing closer to where the data was created, many people use the terms “fog computing” and “edge computing” interchangeably. It may br done for security and compliance reasons,but is often done for efficiency.

Cisco coined the term "fog computing" in 2014. Fog computing is about the node between the host and the cloud..These systems are designed to bring computing power closer to the host system. IBM coined "edge Computing" in 2015.

Fog computing connects edge devices to the cloud. Small computing servers are used to power peripheral devices. communication between servers ensures intelligent information flow. The smaller units work together to process store, and monitor data. Fog computing architecture reduces the amount of data sent through the system and improves overall efficiency.

Fog is another distributed network layer closely related to with cloud computing and the internet of things (IoT). You can think of a Public infrastructure as a service (IaaS) cloud provider vendors can be thought of as a high-level, global endpoint for your data; the edge of the network is where data is generated by IoT devices. is created Fog computing is a network fabric that stretches from data creation to storage.

Fog computing can create low-latency network connections between devices and analytics endpoints. This architecture reduces the amount of bandwidth needed to process data.

## II. LITERATURE SURVEY

This section provides a detailed review of the literature on existing methods.

In the article [2], monitoring is a key mechanism in the iot healthcare platform. jia, et al. provided fog-based monitoring at a low cost., The platform also includes smart gateways and IoT performance sensors. The sensors also collects ECG signals, body temperature, and respiration rate and transmits wirelessly to the gateways for automatic assessment and notification. Ahmad, et al. proposed a fog-based healthcare platform, tailored to privacy and security content of the existing health care platforms, which was developed as a fog layer on the Cloud and end devices using a modular approach. A cloud Access Security Broker (CASB) has been used to improve privacy and security at the network's edge. In addition, data collection from various sources can be supported by the platform and satisfactory cryptographic evaluation. Latency -sensitive medical information appears to affect the performance of medical platform.

In the article [3], Despite the growing popularity of cloud computing, concerns such as inaccurate latency, user mobility, and location awareness remain unresolved due to the inherent problems of cloud computing. FC addresses these issues by offering elastic infrastructure and services to end clients at the network's edge, whereas CC focuses on distributing resources across the core network. FC systems can use intelligence features throughout their activities to take full advantage of the availability of data with networking devices to address the challenges of energy efficiency and delay in IoT applications.

end-user and elevated service that provides deep analytics and more intelligent responses to challenges. While FC intelligence is still in its early stages, it has enormous potential for practical application, as discussed in our studies, and it unquestionably merits further consideration. This review convincingly demonstrates that using DL algorithms or incorporating them into FC improves fog performance and efficiency while also providing end- users with services such as protection, management of resources, traffic predictions, latency, and energy reduction, as well as cost, data analysis, and reliability.

In article [5], Depending on the different papers that we read and mentioned below and also selected the results of some of them. We notice that DL has a great role and positive impact in the case of integration and applied with FC. In (Li et al., Sensors are used to collect data from factory output, resulting in large amounts of data. The product inspection, among the most famous examples, is a tool that is used to detect product flaws.

They proposed a DL-based classification method to introduce a robust inspection system for greater accuracy that can find possible faulty items. Given the possibility of multiple assembly lines in a single plant, one major issue throughout this situation is how to handle such large volumes of data during real- time is the question. As a result, they developed the framework around the idea of FC. Machine transfers processing load to fog nodes to handle large amounts of data. There are two strong benefits to the system Adjusting CNN template to FC increases computing performance.

Fog-Device architecture as two-tier architecture consists of fog computing tier and device tier. In this architecture, fog nodes give different services in a coordinated way and without cloud servers' interferences. In contrast, in Cloud– Fog-Device architecture, fog nodes send data summary periodically according to internal hierarchical structure to the cloud after processing and analyzing collected data by IoT devices. In two-tier architecture, fog is responsible for processing data at the edge, storing and transmitting information from the data generated by mobile or fixed devices located in the devices tier.

In paper 4, we gathered information about fog computing platforms for application and Emerging IoT applications with stringent requirements on latency and data processing have posed many challenges to cloud-centric platforms for Smart Cities. Recently, Fog Computing has been advocated as a promising approach to support such new applications and handle the increasing volume of IoT data and devices. The Fog Computing paradigm is characterized by a horizontal system-level architecture where devices close to end-users and IoT devices are used for processing, storage, and networking functions. Fog Computing platforms aim to facilitate the development of applications and systems for Smart Cities by providing services and abstractions designed to integrate data from IoT devices and various information systems deployed in the city. Despite the potential of the Fog Computing paradigm, the literature still lacks a broad, comprehensive overview of what has been investigated on the use of such a paradigm in platforms for Smart Cities and open issues to be addressed in future research and development. A NAS device is optimized for serving files either by its hardware, software, or configuration. A computer appliance is a purpose-built specialized computer. NAS systems are networked appliances with storage drives arranged into RAIDs .Results: The results reflect that Tetra Mail is a better alternative for blind users due to its consistent and blind- friendly interface design. The results of this prototype implementation show an improved user experience, accuracy in task completion, and better control over touch screen interfaces in performing basic activities of managing emails. The results demonstrate that Data is an accessibility-inclusive email client enabling blind people to have a better user interaction experience and minimal cognitive overload in managing emails. The solution is tested through an empirical study. Results showed that this email client helps blind people to send and receive emails with comfort and ease.

Networking and infrastructure must be available to provide minimum latency and rapid response time for IoT applications.

### *Challenges Faced In Fog computing..*

Fog security challenges are divided into six aspects: reliability, access control, attacks, secure connection, privacy, and special cases. The core objective of this study is to analytically and statistically classify the existing research techniques related to security aspects and available solutions in fog computing.

**1. Reliability**: regarding the approach that fog nodes can per-

form certain activities without any security problems and give the results to the stakeholders.

**2. Authentication and access control**: regarding the approach whether an entity (node, person, process) can access the resources or not

**3. Analyzing attacks**: attacks' features, vulnerabilities and in-trusion detection in fog

**4. Analyzing privacy**: issues related to privacy with four approaches of personal privacy, data privacy, user privacy and situation privacy

5. **Secure connection**: analyzing the problems and challenges

in both internal and external relationships between fog nodes and other parts of fog environment, especially the internal network nodes

6. **Other cases:** including service accessibility, security appli-cations and secure sharing technology.

***Measures to Outfit these Challenges:***

An effective EASBF authentication scheme was demonstrated to secure fog-based Iot applications according to vehicle's identities. The scheme includes five parts: setup identity, enlistment, authentication, interchanging keys, agreement and certificate update. With the help of the elliptic curve cryptography, hash function, and Blockchain approach, the scheme achieves security characteristics such as confidentiality, integrity, authenticity, privacy, non-denial, and precise forward secrecy.

A certificate-based approach was proposed for cloud end, fog network, and IoT devices called Certificate Authority(CA). This approach is optimized by D souza et al. A method is presented to optimize security collaboration to make an access certificate to the resources.

A bi-directional fuzzy logic-based trust management system (TMS) offered safe offloading, and cooperation between fog nodes. This system permits a service requester (SR) to check the level of trust for a service provider (SP) and an SP to assess whether they can rely truthfully on the SR before establishing a communication. Direct trust computation is performed utilizing quality of service (QoS), quality of security (QoSfc), degree of safety and social communications measures. The security evaluation shows that the proposed system is resilient against trust-related attacks. Also, the performance evaluation has illustrated that the TMS accomplishes a permissible degree of validity, reliability, and proficiency.

To enhance reliability in location-based service (LBS) using a third party (TTP), a trustworthy middleware in the fog was presented to save significant partial data with dummy anonymity technology to support physical control, which can be assumed as actually trust. Thus, mobile users' partial significant information can be saved on a fog server to make sure it manages well. DR algorithm was designed to consider similarity, intersection, practicability and correlation.

***The access level in fog includes four approaches:***

***1. Access control by making behavioral identifier for the nodes:***

***Each node through a specific identifier has the right to use and access the resources. This identifier may be built in a group or for a particular node.***

***2. Access control using feature encryption and resources :making specialized cryptography method for resources and access level control through the essential management process.***

***3. Access control through certificate authority: making identifiers that a process can use to complete a cryptography method to access resources and authorities.***

***4. Predetermined policy-based access control: making a policy like a locality for a node in a region or having a level of energy for determining the authorities in a fog network.***

***Privacy Issue In fog Computing:***

**1. Privacy**: Fog computing networks contain a large number of IoT enabled devices that are inter-connected via sensors or wireless systems. IoT devices generate data and transmit it to fog nodes for processing. Sensitive data includes personal information, smart home data, healthcare information, and business information. and all of this data can be stolen by the intruder with a weak security system.

**2. Identity Privacy**: The identity of a user is extremely vulnerable to getting disclosed while having authentication of fog nodes as each user has to provide their identity related information to the nodes including name, phone number, home address, passport number, license ID etc. in order to get verified.

**3. Data Privacy**: The confidential data of a user can get exposed to a network attacker who is trying to steal the user's personal data from the transmission medium or relay nodes. This information consists of the user's personal address, preferences and political data. For example, the online system of voting can put the political preference of users at risk. The privacy of such data is very critical.

**4. Usage Privacy** Usage privacy is the pattern of user access to fog computing services.Intruders can identify when a user is accessing a channel and when they are not communicating.

**5. Location Privacy**: Nowadays, each mobile application asks for access to the device current or saved location along with access to the user 's internal data such as gallery User must sacrifice location privacy to access internet services.Location privacy is critical information that can be used by attackers to track users. Location privacy must be protected at all costs.

**6. Network privacy:** Wireless connections are vulnerable to security and privacy attacks. Fog nodes are costly and difficult to maintain due to their location at the edge of the Internet. Manual network configurations are used to manage network configurations manually.Privacy breach is easy to commit.. Encryption techniques such as Home-Area Network can help resolve security issues.

***Actions to counter these security trends:***

**1. Efficient Encryption Techniques:** Efficient encryption techniques can help resolve privacy issues. will be unable to decode the complex encryption algorithms. However, the developers should consider one fact while developing an encryption technique that as technology is advancing, the attackers are also getting equipped with modern systems and techniques. Hence, they are always one step ahead of the developers as the modern technology would help them to decode any encryption algorithm.

**2. Decoy Technique**: It is a security technique that is used to authenticate the data of a user present in the computing network. It replaces the original information with the fake one which is then provided to the attackers. When an attacker causes a security breach in the system, it finds a fake information file in place of the original file. This file is known as the decoy file and the proposed method is called the decoy technique. The decoy files are formed in the start to ensure improved security. The system hides the original data, which can only be accessed by the authenticated users, and replaces it with the decoy file by default for system intruders.

**3. Authentication Schemes**: Authentication allows verification of user’s identity by verifying user’s given credentials that whether they match with information present in the database through an authentication server. This help in defending against the intrusions of malicious entities. Fog computing network enables users to access the fog services from the fog infrastructure if the user is well authenticated from the system first in order to be a part of the network processing infrastructure.

In this system, instead of the costly option of blanket encryption of all data, the transmitted data is blurred, divided, and shuffled to reduce the user’s operations and increase the efficiency of real-time services. Such precautions are also sufficient to prevent man-in-the-middle attackers, eavesdroppers, and brute force assailants from achieving their goals. However, while this proposed system protects user privacy, it requires a lot of simultaneous operations (blurring, filtering, encryption, decryption, and ordering and reordering),which increase the overhead load for both the user and the FN, especially as the TV remote sends data continuously. This research area needs more evaluation of time consumption in order to prove its effect on real-time services, and to reduce overheads for the entities.

A smart meter is a device to monitor the energy consumption at the user's side. Over regular time periods it records the energy consumed and sends this data to the operation center via a region gateway (which plays the role of the FN), and a response is sent back to the smart meter. Taking advantage of the tiny homomorphic data generated by smart meters, this scheme uses the Paillier cryptosystem to achieve the confidentiality objective during data transmission and to prevent FN from decrypting user data.

The results for the small size of the data set are the same. It is better to compare the results with other encryption algorithms to get a more accurate evaluation of performance, or the performance could be compared across different key sizes. In general, it is not recommended to add encryption tasks to the FN.

In most of the papers, it can be seen that the whole process of data transfer makes it more interactive and easy for the offline user people. This system makes the disabled people feel like normal users. Also, voice based is useful for handicapped and illiterate people. Data mana recognizer is of the major advantages. We can see a reduction in cognitive load taken by blind to remember and type characters using a keyboard. Voice based email system is a user-friendly system.

In almost all the papers, it can be seen that there is use of mouse clicks for many tasks. It gets difficult for visually impaired people. Also, the Indian subcontinent is not benefited by this as there are so many languages and speech recognizers cannot recognize these languages. Mostly the English language is preferred. The following section is the proposed system for the visually impaired.

***Why fog computing..***

Cloud is used to store data that is to be used by the user to perform his operations on the data. In this project Fog Cloud is used as a cloud service provider This could act as a storage of required media files. For this purpose we need to allocate some space on the cloud where it will be possible to store and retrieve information from the cloud.

A fog computer, by definition, is not capable of data collection or generation. As such, fog computing would not exist without edge computing. Edge computing is normally used in less resource-intensive applications due to the limited capabilities of the devices that collect data for processing.

***Advantages of fog computing..***

Reduces the response time of the system. It improves the overall security of the system as the data resides close to the host. It provides better privacy as industries can perform analysis on their data locally.

Latency Reduction. Reduced latency is the primary benefit of edge and fog computing. Data does not necessarily need to be sent to the cloud for processing as some of the compute can be performed nearer the data source for time-sensitive services. Network latency, or lag, is the term used to describe delays in communication over a network. In networking, it is best thought of as the amount of time taken for a packet of data to travel through multiple devices, then be received at its destination and decoded.

The data loss during the transfer is an important area to study and makes our project more efficient while data transfer .Fog computing provides processing, storage, and analyzing the data nearer to IoT and end-users to overcome the latency. The novel Intelligent Multimedia Data Segregation (IMDS) scheme using Machine learning (k-fold random forest) is proposed in the fog computing environment that segregates the multimedia data and the model used to calculate total latency (transmission, computation, and network).

The motivation came from a study about how to generate minimum response time with a better quality of service for time-sensitive healthcare IoT based applications. The cloud alone is not able to satisfy the aforementioned requirements due to their limitations. The patient’s physical status varies with time and needs rapid response as an action to monitor remote patients. This is possible when there is a very good network available. Otherwise, it will take more time to

respond. In fact, due to unpredictable networks, there is high latency. The health data of patients are not considered as real-time data. This shows that the data become unreliable, worthless, and insufficient. The delay may increase for these IoT time-sensitive data from milli-seconds (ms) to seconds and then reaches to minutes, When the size of health data increases, therefore the situation become worsening in handling real-time operation

A high volume of data transmission over the network increases the probability of occurrence of an error and the delay. The loss of data packets and transmission latency is directly related to the quantity of data transmitted through IoT devices to the cloud. Due to this reason, it causes a low quality of service QoS) produced to the end-user. Cloud computation and data storage are generally not desired in most of the time-sensitive applications of the IoT. Extreme time-bounded problems must be completed nearer to the IoT devices. As the healthcare infrastructures' main requirements are minimization in latency and reduction in network bandwidth, for this it requires data in real-time for a time-critical scenario

Dinh et al. used a service-oriented schema related to cost-effectiveness for providing the service of the IoT-Fog-Cloud network.The authors also used to measure VNF (Virtual Network Function)with development in the capabilities to enhance the availability of SFC (service function chaining) with the proposed metric. Mahmud et al .discussed the problem that occurred in the use of healthcare due to the large volume of transmission of data and high latency. As a solution to these issues, the author presented an IoT-healthcare structure based on fog and explored the cloud-fog service over the traditional cloud. An improvement result is shown for network-traffic, power usage, and the cost. Ahsan et al. highlighted the security, protection, and integrity of the data is a major concern in cloud computing. The author proposed a fog-centric scheme for the storage of data in the cloud. Data security issues had been discussed. Xor-combination is implemented to provide the protection and security of data in the cloud.

The encrypted data is transmitted to the user from the cloud via the FN again. The mobile user then undertakes the decryption operation. The model evaluation uses three data sets, with different data types and sizes.

***Downloading the files on smart phone and playing***

The user can send emails, listen to what they have written and also receive emails and listen to them with voice commands. In Email, the application makes use of the SMTP protocol for sending emails and POP3 protocol for receiving emails. SMTP (Simple Mail Transfer Protocol) is the reliable protocol to send emails and it works in a simple way that the SMTP server passes on the email messages quickly. POP3 (Post Office Protocol) is used to receive emails. The POP3 server stores the email and on request the emails are displayed. The same is implemented in our application, that on the request by the user the emails are downloaded The Fog nodes are highly distributed and heterogeneous, and most of them are constrained in resources and spatial sharing.

Fog computing, an extension of Cloud at the edge network, can execute these applications closer to data sources. Thus, Fog computing can improve application service delivery time and resist network congestion.

It is a web development platform that provides the services necessary for developers to build enterprise-class web applications. Microsoft SQL Server

A Relational Database Management System (RDBMS) to store the new user registration and other details in the database.

## III. Related work on Fog and Edge Computing:

Since fog and edge are now emerging as new computing concepts, frameworks or models to satisfy fog and edge requirements are not well established. Research challenges globe software, middleware and hardware layers. The inherent characteristics of the devices also play an important role since many of the fog and edge nodes might be mobile devices. Existing methods used in the cloud may therefore not be appropriate in a fog or edge environment.

The use cases for fog and edge analytics also differ from normal workflows since the focus is more on user-driven applications rather than data-driven applications, on lightweight analytic techniques instead of memory-intensive analytics and on algorithms with less memory footprint for edge nodes.Six main considerations for fog and edge environments are: partitioning and offloading tasks, sustainable energy consumption, edge analytics, edge security, edge node and data discovery and edge quality of service.As a result, it increases the rate of cloud computing by removing the need to manage and store vast volumes of data that aren't needed. The growing number of smart apps assists the FC model significantly.

The below diagram represents the difference between the fog , cloud and edge computing and highlights the key features between them.

The user has to register themselves by creating their account. It will prompt for user id and Password, following which, the authentication will take place. For correct credentials entered the user's registration process will be successfully completed. The user can log into their data l systems, Check and transfer the data between them. Here, the data read and write modules Come handy. Fog tier includes network equipment with routers, gate- ways, bridges, switches and base devices with computing capability, including local servers. Each of these devices is considered a fog node. In three-tier architecture, the cloud tier is a storage and computing platform. The cloud has considerable storage capacity and computing resources, and it is accessible for users everywhere. Also, in this architecture, fog acts as a bridge between the computing resources available in the cloud and the data generating resources located in the devices tier and processing and storing.

The usage of the network is also minimized with the average result being kilo bytes. The existing state-of-art is compared with the proposed algorithm that minimized latency. We compared the proposed model by Hermes , Fog Store , and Hipster , where an improvement in the minimization of latency with the model presented by Hermes, a reduction in latency is demonstrated as a comparison to cloud computing by iFogStor, and Hipster improves the latency for web-searching . Raafat shows the reduction in overall service latency in the fog environment.

The research work by Cito et al.  can further be deployed in a fog or edge environment and enhanced by partitioning or offloading requests to another fog or edge node. It would then be more interesting to evaluate the performance and analytics requirements of mobile fog and edge nodes based on recurrent advertisements and analytics requests. One important metric which could be investigated in the study by Morabito ] is the selective partitioning of tasks on low power nodes. For example, if an edge node can process a maximum of four parallel instances, the node could dynamically adapt itself to offload execution on another edge node with less computing requirements. The research work by Kartakis et al.  could be improved by profiling the edge sensor nodes in terms of computing requirements. For example, battery-powered sensor nodes could choose a lightweight algorithm based on battery status at runtime.

They categorized the various threats as follows: network infrastructure (Denial of service, man-in-the-middle, rogue gateway), edge data center (physical damage, privacy leakage, privilege escalation, service manipulation, rogue data center), core infrastructures (privacy leakage, service manipulation, rogue infrastructure), virtualisation infrastructure (denial of service, misuse of resources, privacy leakage, privilege escalation, VM manipulation), user devices (injection of information, service manipulation).

In article3 , we discussed the performance of the model. In this model, data is transferred from one layer to another layer starting from IoT devices and reaches to cloud through a fog environment. The time consumed by data in traveling is calculated. As data is classified, it is processed and as per requirement, the data is sent to the end-user or cloud. To complete the research task, we use the tool of python editor. The result will be visualized after the completion of the simulation process. Here, the data set is divided into tenfold as we applied a k-fold random forest learning algorithm. 70% of the data set will be used for training purposes whereas 30% of data used for testing purposes. Python 3.7 is used as a platform for implementing this work. Random forest algorithm classifies the data in high risk, low risk, and normal with the accuracy of 92% in the proposed work. It took 14 seconds as computation time.

***The main contributions of the research work-study are as follows:***

1. An analytical model based on fog computing is proposed to transfer healthcare sensor data to end-users in real-time.
2. A random forest algorithm is implemented which reduces and avoids the "over-fitting" issues.
3. The proposed research scheme minimizes the total latency between healthcare sensors and cloud servers. A performance comparison is conducted for the proposed analytical model with existing models on different parameters.
4. To improve the quality of service for e-healthcare.

## IV.CONCLUSION

In this project, we have designed and implemented a decision framework for computation Fog offloading. The decision is based on estimated execution time and energy consumption. We aim to save both execution time and energy consumption at the same time. Based on our decision framework, the Task module tends to be offloaded to more powerful processors, such as local GPU or cloud.

### REFERENCES

[1] K. Kumar and Y.-H. Lu, "Cloud Computing for Mobile Users: Can Offloading Computation Save Energy?" Computer, vol. 43, no. 4,pp. 51–56, 2018.

**[2]** S. Perez, “Why Cloud Computing is the Future of Mobile,” Aug.4 2009. [Online]. Available:http://readwrite.com/2009/08/04/ why cloud computing is the future of mobile.

**[3]** A. P. Miettinen and J. K. Nurminen , “Energy Efficiency of Mobile Clients in Cloud Computing,” in Proc. of the 2nd USENIX conference on Hot topics in cloud computing (HotCloud’10), 2017.

**[4]** Assad Abbas, Samee U. Khan, Albert Y. Zomaya, “Fog Computing: theory and practice” Wiley ISBN: 9781119551690, 2020.

**[5]** Juego-Soren Preden, Amir M. Rahmani, Pasi Liljeberg, Axel Jantsch ,“Fog Computing in the Internet of Things - Intelligence at the Edge” Springer ISBN: 978-3-319-57638-1.

**[6]** U. Ahmed, J. C. W. Lin, G. Srivastava, M. Aleem, “A load balance multi scheduling model for OpenCL kernel tasks in an integrated cluster”, *Soft Computing*, 2020, pp. 1-14.

**[7]** T. A. Rashid, P. Fattah, D. K. Awla, “Using accuracy measures for improving the training of LSTM with metaheuristic algorithms”, *Procedia Computer Science*, *140*, 2018, pp. 324-333.

**[8]** A. Janosi, M. Pfisterer, W. Steinbrunn, R. Detrano, J. Schmid, S. Sandhu, K. Gupta, S. Lee , V. Froelicher, UCI Machine Learning Repository 2019. https://archive.ics.uci.edu/ml/datasets/heart+disease

**[9]** F. Bonomi, R. Milito, J. Zhu, S. Addepalli S, “Fog computing and its role in the internet of things”, in Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, 2012, pp. 13–16.

**[10]** **]** S. Yi, C. Li C, Q. Li Q, “A survey of fog computing: Concepts, applications and issues”, in Proceedings of the 2 Workshop on Mobile Big Data, ACM, 2015, pp. 37–42.

**[11]** P. G. Lopez, A. Montresor, D. Epema, A. Datta, T. Higashino, A. Iamnitchi, M. Barcellos, P. Felber, E. Riviere, “Edge-centric computing: Vision and challenges”, SIGCOMM Computer Communication Review, vol. 45, no. 5, 2015, pp. 37–42.

**[12]** M.Changand T. Zhang "Fog and the Internet of Things: Investigating Research Opportunities", IEEE Internet of Things Journal, vol. 3, no. 6, 2016, pp. 854-

**[13]** T. N. jia M. jiang, A. M. Rahmani, T. Westerlund, p.Liljeberg H. Tenhunen,"Internet of Things Fog Computing in Healthcare: A Case Study of ECG Feature Extraction",IEEEInternationalConference on Computer and InformationTechnology,2015; ubiquitous computing and communications; stable, autonomous and secure computing;Pervasive Intelligence and Computing, IEEE, 2015, pp. 356-363**.**

**[14]** S.C. Hung, D. Liau, S.Y. Lien, K.C. Chen, “Low latency communication for Internet of Things”, in IEEE/CIC International Conference on Communications in China (ICCC), IEEE, 2015, pp. 1-6. [10] G. Lee, W. Saad, M. Bennis, “An online optimization framework for distributed fog network formation with minimal latency”, IEEE Transactions on Wireless Communications, vol. 18, no. 4, 2019, pp. 2244-2258.

**[15]** H. Gupta, A. V. Dastjerdi, S. K. Ghosh, R. Buyya, “iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments”, Practice and Experience, vol. 47, no. 9, 2017, pp.1275-1296.

**[16]** L. Skorin-Kapov and M. Matijasevic, “Analysis of QoS requirements for e-health services and mapping to evolved packet system Q

**[17]** T. N. Gia, M. Jiang, V. K. Sarkar, A. M. Rahmani, T. Westerlund, P. Liljeberg, H. Tenhunen H, “Low-cost fog-assisted healthcare IoT system with energy-efficient sensor nodes” in Proceedings of 13th international wireless communications and mobile computing conference (IWCMC), IEEE, 2017, pp. 1765-1770.

**[18]** M. I. Naas, P. R. Parvedy, J. Boukhobza, L. Lemarchand, “iFogStor: an IoT data placement strategy for fog infrastructure”, in IEEE 1st International Conference on Fog and Edge Computing (ICFEC), 2017, pp. 97-104.

**[19]** A. M. Rahmani, T. N. Gia, B. Negash, A. A. I. Azimi, M. Jiang, P. Liljeberg, “ Exploiting smart e-Health gateways at the edge of healthcare Internet Of-Things: A fog computing approach”, Future Generation Computer Systems, vol. 78, 2018, pp. 641-658.