Journal of Ambient Intelligence and Humanized Computing (2020) 11:3155–3173
https://doi.org/10.1007/s12652-019-01481-1

ORIGINAL RESEARCH

# An energy-aware multi-sensor geo-fog paradigm for mission critical applications

**Moumita Mishra[1] · Sayan Kumar Roy[1] · Anwesha Mukherjee[2] · Debashis De[1,3] · Soumya K. Ghosh[2] · Rajkumar Buyya[4]**

Received: 1 March 2019 / Accepted: 4 September 2019 / Published online: 12 September 2019


**Abstract**
Sensor cloud is an integral component for smart computing infrastructure. Cloud servers are largely used to store and process sensor data. For mission critical applications use of only wireless sensor network results in provisioning of service in a small area and the use of a long distant remote cloud servers increase delay that degrades the Quality of Service. Further, geospatial information differs over regions. Thus storing and processing the data of all regions inside the cloud data centres may not be efficient with respect to response time (latency), energy consumption etc., which are crucial factors for mission critical applications. To overcome these limitations, we propose multi-sensor geo-fog paradigm. We consider defense sector in our work as mission critical application. For energy optimized services with minimal delay fog computing has been used, where the intermediate devices process the data. The proposed paradigm will offer fast and energy-efficient processing of defense related sensor and geospatial data. A mathematical model of the paradigm is developed. The sensor and geospatial data processing and analysis take place inside the fog device. If abnormality is detected in the data or emergency situation occurs, then shortest path to the victim region is determined using intelligent K* heuristic search algorithm. The simulation results demonstrate that the proposed fog based network scenario reduces energy consumption, average jitter and average delay by 12–15%, 10–14% and 9–11% respectively than the cloud based network. The simulation results demonstrate that saving about 20% of resources increases the performance for priority user whereas the resource availability for the normal users is not compromised.

**Keywords** Energy · Fog computing · Heuristic search · K* algorithm · Geospatial · Wireless sensor network

## 1 Introduction

Geospatial information refers to the data related to earth surface in terms of geographic coordinates. The storage and analysis of geospatial information and usage of the information in real time scenario is a promising research area (Limkar and Jha 2018; MacEachren et al. 2005). With the major advances of wireless technology, large amount of heterogeneous data related to geospatial information has been gathered by different organizations. By processing the geospatial data, meaningful information is obtained by the organizations. Fast and energy-efficient processing of this information along with privacy management is vital for mission critical applications. Defense sector is a mission critical application that requires fast processing of data, confidentiality, and prompt decision making. Defense organization of a country is a critical sector which seeks latest technological solutions in every aspect. Defense forces work in an environment which is neither

✉ Debashis De
dr.debashis.de@gmail.com

[1] Centre of Mobile Cloud Computing, Department of Computer Science and Engineering, Maulana Abul Kalam Azad University of Technology, West Bengal, B.F.-142, Salt Lake, Sector-1, Kolkata 700064, India

[2] Department of Computer Science and Engineering, Indian Institute of Technology (IIT) Kharagpur, Kharagpur, West Bengal 721302, India

[3] Department of Physics, University of Western Australia, 35 Stirling Hwy, Crawley, WA 6009, Australia

[4] Cloud Computing and Distributed Systems (CLOUDS) Laboratory, School of Computing and Information Systems, The University of Melbourne, Melbourne, Australia

friendly nor stable. In a battlefield scenario, it is quite difficult to collect real time detailed information about the field. Use of wireless sensor network (WSN) for monitoring activities in remote and sensitive locations is well accepted. In conventional sensor cloud computing architecture the data captured using sensor nodes are processed and stored inside the cloud servers (Misra et al. 2017; Madria et al. 2014; Wang et al. 2016; Zhu et al. 2017; Sen and Madria 2017). But a drawback of WSN is that it is bound in a small area and the remote cloud servers increase the delay and energy consumption (Zhang et al. 2010; Gupta et al. 2017; Dastjerdi and Buyya 2016). Hence use of remote cloud servers for processing and storage of defense related highly confidential data may suffer from increase in delay and energy consumption. The objective of this work is to introduce a novel paradigm that will provide fast processing and storage of defense related data in an energy-efficient manner. With adoption of fog computing (Gupta et al. 2017; Dastjerdi and Buyya 2016; Huang et al. 2016), the proposed model will focus on the processing and storage of defense sector related information of various geographical regions inside the fog devices of the respective regions. The proposed sensor-fog paradigm is designed for military tri-services which brings all the field activities of the forces namely: Army, Navy and Air. The proposed paradigm enhances the physical time detailed information of the arena and enriches the capability of resource allocation. The proposed model aims to improve resource allocation for a priority user as well as a normal user, which helps the users for prompt decision making according to the real time situation.

### 1.1 Motivation and contributions

In the existing sensor cloud-based model for defense sector the defense related information are stored and processed inside the cloud servers. WSN is used to capture the data of different objects and the collected data are processed and stored inside the cloud servers. However, if WSN is only used for military field, the benefits can be provided in a tiny area and the use of remote cloud servers enhances the delay and energy consumption that affects the Quality of Service (QoS). Moreover, the data of different geographical regions differ. Thus storing and processing the data of all regions within a centralised cloud computing environment may not be efficient with respect to response latency and energy consumption. Our motivation is to introduce a new paradigm for defense sector that will offer fast and energy-efficient processing of defense related geospatial and sensor data.

To fulfil the objectives, the contributions of this paper are:

1. A multi-sensor fog computing based paradigm is proposed for mission critical application. Here defense sector is considered as the mission critical application. In the proposed paradigm multiple sensor nodes collect status of the environmental objects and geospatial information with respect to a particular geographical region. The fog device of the geographical region is used to process the sensor and geospatial data, which will reduce the delay and energy consumption over the remote cloud servers. The proposed paradigm is referred as multi-sensor geo-fog paradigm. Mathematical model of the proposed paradigm is developed.
2. After data processing inside the fog device, if any abnormality is detected or emergency situation arises, K* algorithm is used to find out the shortest path to the victim region.
3. The proposed network model is simulated in QualNet (Scalable Network Technologies 2018) to determine the throughput, delay, jitter and energy consumption of the proposed network scenario.
4. The proposed paradigm is simulated in iFogSim (Gupta et al. 2017) to evaluate the performance with respect to processor and memory utilization.

The rest of the paper is organised as follows: Sect. 2 presents the related work. Section 3 describes the proposed paradigm with the mathematical model. Section 4 presents an approach for calculation of delay and energy consumption. Section 5 evaluates the performance of the proposed paradigm. Section 6 draws conclusions with future research direction.

## 2 Related work

Geospatial information refers to the data related to a geographical place in terms of geographic coordinates (Limkar and Jha 2018; MacEachren et al. 2005). Geographic Information System (GIS) is used to collect, store, process and analyze geospatial data. A geospatial object denotes single geographic property that is characterized by a geospatial concept. To calculate the degree of potential semantic inter-operability between geospatial data semantic similarity is used. Semantics of geospatial objects and concepts are described by shape, size and location. The geospatial query placement, query scheduling and resource provisioning are important. Using Service Level Agreement Tree (SLA-Tree) a greedy scheduling algorithm has been discussed in Chi et al. (2011) that has focused on capacity planning, scheduling, and dispatching. The profit of each query varies according to the query response time. Usually geospatial information are stored, processed and analysed inside the remote cloud servers (Das et al. 2019). The sensor cloud paradigm also uses remote cloud servers to process and store sensor data (Misra et al. 2017; Madria et al. 2014; Wang et al. 2016; Zhu et al.

2017; Sen and Madria 2017). For health monitoring a sensor cloud paradigm has been discussed in Wang et al. (2016). A multi method data delivery for sensor cloud model has been discussed in Zhu et al. (2017). Attack graphs have been used for risk assessment in a sensor cloud network in Sen and Madria (2017). QoS provisioning for software defined fog computing using WSN has been discussed in Huang et al. (2016). A cloud computing based model for defense sector has been illustrated in Misra et al. (2016), where military tri-services operations and decision making have been discussed. Deadline aware self-adaptive resource control system for military purpose has been developed in Xiang et al. (2013). An emotion aware system for military environment has been discussed in Lin et al. (2019). In this system a decision making method has been proposed based on the emotions of the soldiers. For vital real time applications like defense sensor, which seek for fast processing of geospatial information and sensor data, remote cloud servers may not be a good option. In Ramasamy (2019) cognitive radio network has been used for emergency communication during disaster management. In Satyanarayanan et al. (2009), Mukherjee et al. (2016), Gai et al. (2016) the authors have discussed the use of cloudlets to reduce the delay and energy with respect to the cloud servers. Fog computing has come to enhance the QoS in terms of delay, energy etc. (Luan et al. 2015; Mukherjee et al. 2018). The use of fog computing in Internet of Things (IoT) has gained popularity (Dastjerdi and Buyya 2016; Chiang and Zhang 2016). The use of IoT in military sector has been discussed in Burmaoglu et al. (2019). The use of fog computing for health care system has been discussed (Kumari et al. 2018; Mutlag et al. 2019; Ahmad et al. 2016; Rahmani et al. 2018). The security issues in fog computing has been discussed in Zhang et al. (2018). The deployment of IoT applications using fog computing has been explored in Venticinque and Amato (2019). A mobile IoT device simulator has been designed in Kertesz et al. (2018). A cloud gateway has been also proposed to handle the devices for receiving, visualizing and processing sensor data coming from the mobile IoT device simulator in Kertesz et al. (2018). A fog computing based geospatial data infrastructure has been proposed for health care system in Barik et al. (2019). For diabetic patients a fog based health monitoring system has been proposed in Devarajan et al. (2019). The service placement in fog computing has been discussed in Guerrero et al. (2019). Based on fog computing a congestion avoidance scheme has been proposed for Internet of Vehicles in Yaqoob et al. (2019). For energy-efficient smart building, fog based architecture has been proposed in De Paola et al. (2019), where reactive intelligence and deliberative intelligence have been considered.

In our work, we propose a multi-sensor geo-fog computing paradigm for defense related sensor. Table 1 presents the novelty of the proposed paradigm with respect to the existing models on defense/military related application.

## 3 Multi-sensor geo-fog paradigm for defense sector

The proposed four-layer multi-sensor geo-fog paradigm for defense sector is presented in Fig. 1a. The flow chart of the working model of the proposed paradigm is presented in Fig. 1b.

The major components of the proposed paradigm are:

(a) Sensor network,
(b) Sensor network director,
(c) Sensor fog organizer,
(d) Cloud servers.

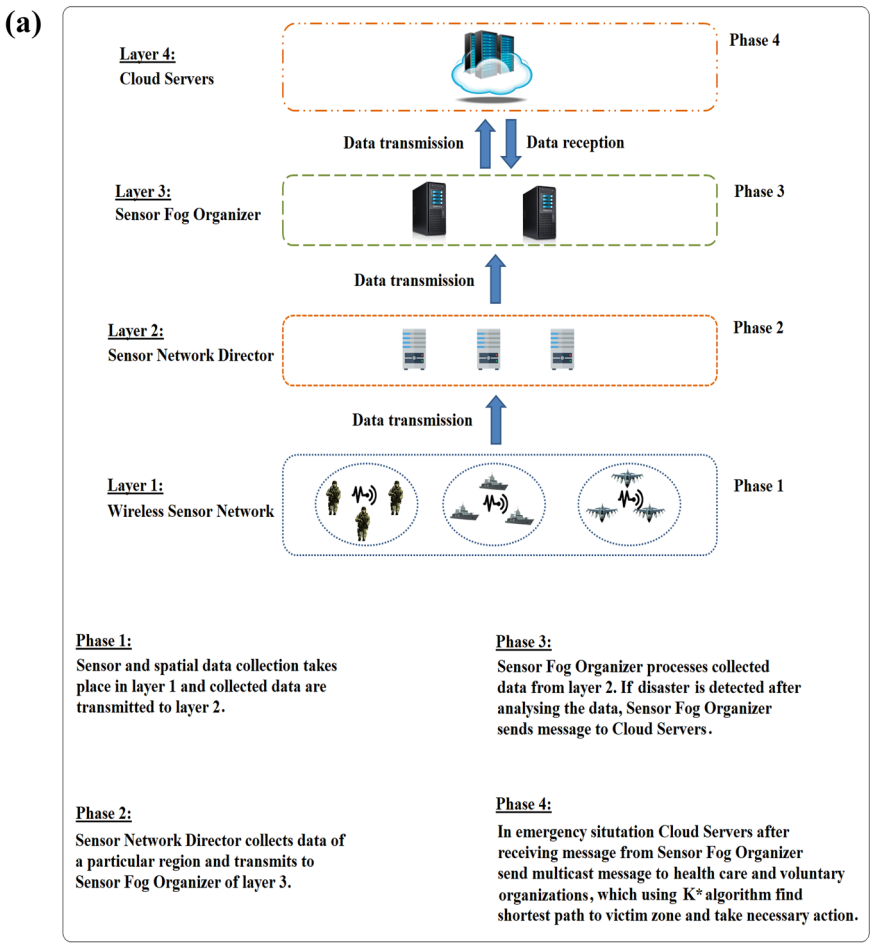
In our paradigm there are multiple sensor network directors and sensor fog organizers located in different geographical regions. Layer 1 contains multiple sensor nodes which are connected with the sensor network director of layer 2. Sensor network director is connected with sensor fog organizer of layer 3. Sensor fog organizer is connected with cloud servers of layer 4.

In our paradigm multiple sensor nodes, deployed in a particular geographical region, collect defense related sensor data and geospatial data of that region, communicate with sensor network directors with respect to their location. Sensor network director continuously gathers data from multiple sensors of layer 1 and provide services for the power management and security. Sensor network director integrates the collected data from multiple sensors, and transmits the integrated sensor and geospatial data to the sensor fog organizer. The defense related sensor and geospatial data offloading takes place to the sensor fog organizer. The sensor fog organizer is connected to the cloud servers. The collected defense related sensor and geospatial data of a particular geographical region are offloaded inside the sensor fog organizer of that region. The sensor fog organizer maintains the grouping of multiple sensor network directors. The resource virtualization takes place under them. Sensor fog organizer works as a connector between the sensor network director and cloud servers in a distributed manner. It is responsible for allocating, tracking and sharing of available resources. The working model of proposed paradigm is illustrated as follows.

- *Defense data collection by sensor network* The sensor nodes are attached with the objects to collect their status, e.g. light sensor, gas sensor, motion sensor, infrared sensor, GPS sensor etc., in a particular geographical region. In defense sector infrared sensors are largely used. These sensors can measure heat of an object and its motion. In infrared sensor LM358 IC transmitter and receiver pair, resistors of kΩ, different registers and

**Table 1** Comparison between existing and proposed strategies for defense/military related application

| Feature | Mils-cloud (Misra et al. 2016) | Deadline aware resource control in military cloud (Xiang et al. 2013) | Cognitive Radio Sensor Network for emergency (Ramasamy 2019) | IoT in military sector (Burmaoglu et al. 2019) | Proposed fog based paradigm for defense sector |
|---|---|---|---|---|---|
| Contribution | Sensor cloud architecture for military tri-services has been proposed | A deadline based self-adaptive resource control framework has been proposed, which can be used in military sector | Cognitive Radio Network with Software Defined Radio has been used for emergency communication during disaster. The white spaces in the spectrum are detected and sensed to be used for emergency communication during disaster using Discrete Wavelet Packet Transform | The use of IoT for military sector has been discussed | A fog based paradigm for defense sector is proposed, where sensor data along with geospatial information are processed and analysed inside the fog device. In case of emergency situation shortest path to the victim region is generated using K* heuristic search algorithm |
| Related to defense/military/diaster management application | ✓ | ✓ | ✓ | ✓ | ✓ |
| Fog device is used | × | × | × | × | ✓ |
| Geo-location/spatial information/geographical region is considered | × | × | ✓ | ✓ | ✓ |
| Shortest path algorithm is used | × | × | ✓ | ✓ | ✓ |



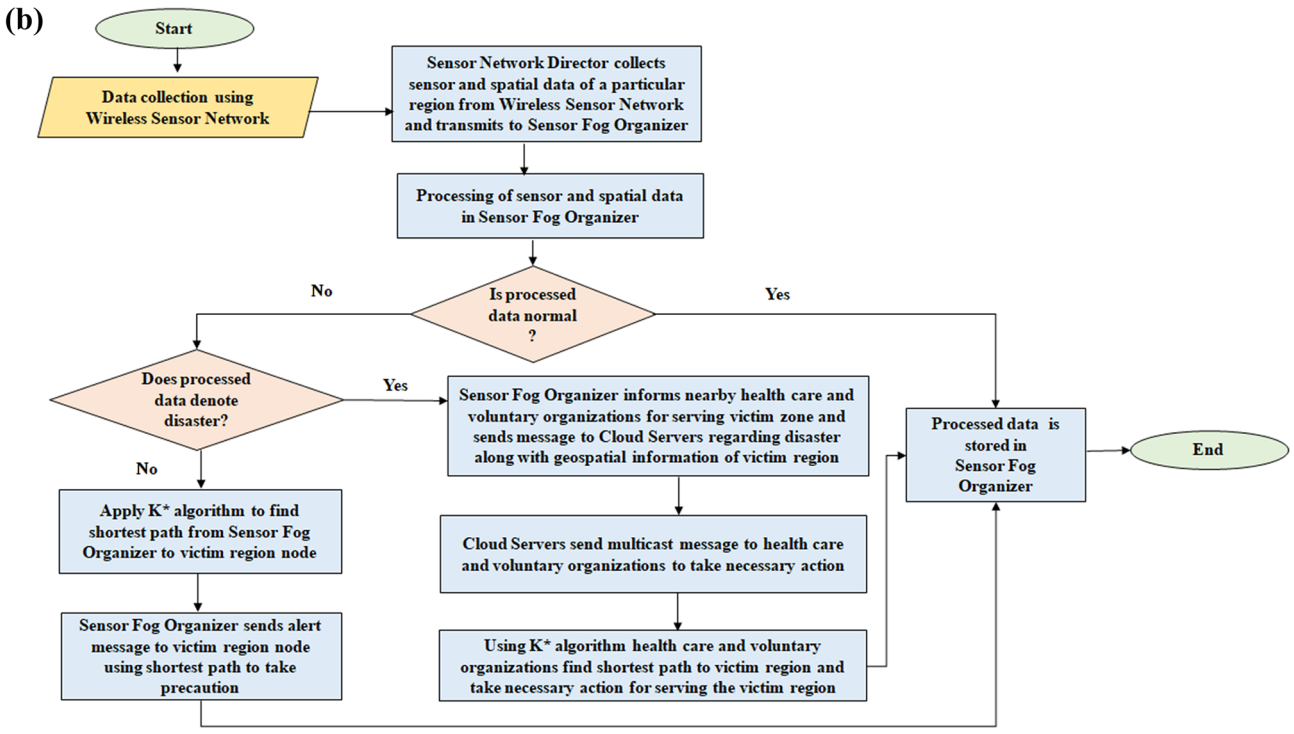




**Fig. 1** **a** Proposed four-layer multi-sensor geo-fog paradigm for defense sector. **b** A flowchart of the working model of proposed paradigm

LED are used. There are two types of infrared sensors: thermal and quantum. Ultrasonic sensors are also used in defense. Ultrasonic sensors measure the reflection of moving object. When a voltage is applied to the sensor, it vibrates. Smart position sensors are also used in military sector. The GPS sensor is used to collect the geo-location information of the region. The sensor data collected by sensor nodes are transmitted to the sensor network director of the geographical region.

- *Data offloading to sensor fog organizer by sensor network director* The sensor network director forwards the collected defense related sensor data and geo-location information to the sensor fog organizer. The sensor fog organizer stores and processes the data. As the sensor fog organizer processes the data instead of the remote cloud servers, the propagation and communication delays are reduced. If any problem occurs, precautions can be taken promptly. As the geo-location information is collected, if any abnormality is detected in the collected sensor data after processing, the sensor fog organizer sends alert message to the victim region node using shortest path obtained using K* algorithm. If any disaster is detected after processing the data, based on the geo-location information sensor fog organizer informs the health centres and voluntary organizations nearby the victim region to take necessary action for serving the victim region. The sensor fog organizer also sends a message to the cloud servers informing about the disaster along with the geo-location information of the victim region. The cloud servers then inform the health centres and voluntary organizations of different area about the victim region. Based on the geo-location information the health centres and voluntary organizations obtain shortest path to the victim region using K* algorithm. By following the shortest path they reach the victim region and take necessary action.

*Faulty data detection using PCA* In the proposed paradigm there may be errors in the measured data. For faulty data detection we have used Principal Component Analysis (PCA) (Mnassri et al. 2009; Xie et al. 2011). PCA is a well-known method that transforms the original space into subspace that preserves maximum variance of the original space in minimum number of dimensions. Let there are $a$ sensors and $b$ samples. Then the data matrix given as (Mnassri et al. 2009; Xie et al. 2011), $X_{b\times a} \in \Re^{b\times a}$. The data matrix is normalized to zero mean and unit variance to obtain the standardized matrix denoted as $\overline{X_{b\times a}}$. The covariance matrix is generated and singular value decomposition is performed on the covariance matrix. The standardized matrix is projected into the principal component space and residual space, given as (Mnassri et al. 2009; Xie et al. 2011),

$$\overline{X_{b\times a}} = \hat{X} + \tilde{X}, \tag{1}$$

where $\hat{X} = \overline{X_{b\times a}}\hat{C}$ and $\tilde{X} = \overline{X_{b\times a}}\tilde{C}$, and $\hat{C}$ is the projection matrix of the principal component space and $\tilde{C}$ is the projection matrix of the residual space. As $\tilde{X}$ contains measurement noise, if a sensor node fails, the measurement data of residual space will increase. The sensor data fault detection is implemented in the subspace by the squared prediction error given as (Mnassri et al. 2009; Xie et al. 2011),

$$SPE = \left\|\tilde{C}\overline{X_{b\times a}}\right\|^2. \tag{2}$$

The control limit for squared prediction error is $\delta^2_{SPE}$ that can be determined with its sample distribution. If $SPE > \delta^2_{SPE}$, then it means a data fault has occurred.

In the proposed paradigm, when an abnormal data is detected, then first it is verified whether any data fault has occurred or not. Here PCA is used for making the decision that whether the data is a faulty data or not. If it is not a faulty data, then the abnormality is detected as true and the sensor fog organizer sends alert message to the victim region node using shortest path obtained using K* algorithm.

### 3.1 Mathematical model

The components of the proposed paradigm are mathematically defined as follows.

*Sensor node set* ($S$) $S$ is a set of sensor nodes for defense data collection, defined as,

$$S = \{S_1, S_2, \ldots, S_n\},$$

where $n$ is the number of sensor nodes.

*Event type set* ($E$) Each sensor node detects a specific type of event. The event refers to the purpose for which the sensor is used, e.g. movement is the type for movement detector, light is the type for light sensor. The set denoting the event types sensed by all the sensors is defined as:

$$E = \{E_1, E_2, \ldots, E_n\},$$

where $n$ is the number of sensor nodes.

**Definition 1** (*Sensor node*) A sensor node is defined as a set containing the ID of the node and the event type sensed by the node, given as $\{S_i,\ E_i\}$,where $S_i$ represents the unique ID of a sensor node and the event type that the sensor node $S_i$ detects is denoted by $E_i$, and $1 \le i \le n$.

*Sensor network director set* ($N$) $N$ is denoting the set of sensor network directors defined as,

$$N = \{N_1, N_2, \ldots, N_k\},$$

where $k$ is the number of sensor network directors.

*Specification set of sensor network directors* ($Hn$) The hardware related specifications for all sensor network directors is put in a set denoted by,

$$Hn = \{Hn_1, Hn_2, \ldots, Hn_k\},$$

where $k$ is the number of sensor network directors.

*Spatial data set of sensor network directors* ($Gn$) The geospatial data for all sensor network directors is put in a set denoted by,

$$Gn = \{Gn_1, Gn_2, \ldots, Gn_k\},$$

where $k$ is the number of sensor network directors.

*Security schemes used in sensor network directors* ($Cn$) The security schemes used in all sensor network directors is put in a set denoted by,

$$Cn = \{Cn_1, Cn_2, \ldots, Cn_k\},$$

where $k$ is the number of sensor network directors.

**Definition 2** (*Sensor network director*) A sensor network director is defined as a set containing the ID, specifications, geospatial data, and security measures used, given as,

$$\{N_j,\ Hn_j,\ Gn_j,\ Cn_j\},$$

where $N_j$ represents the unique ID of a sensor network director, $Hn_j$ represents the hardware specifications of the sensor network director, $Gn_j$ represents the geospatial data for the sensor network director, and $Cn_j$ represents the security scheme used in the sensor network director, and $1 \leq j \leq k$.

The mapping from the sensor nodes of layer-1 to the sensor network director of layer-2 is many-to-one and it is denoted as,

$$M'_{12}(.) : S' \rightarrow N_j,$$

where $S'$ is a set containing few sensor nodes, i.e. it is a subset of $S$, and $N_j$ denotes a sensor network director. This represents multiple sensor nodes are mapped into a single sensor network director.

*Sensor fog organizer set* ($F$) $F$ is denoting the set of sensor fog organizers defined as,

$$F = \{F_1, F_2, \ldots, F_m\},$$

where $m$ is the number of sensor fog organizers.

*Specification set of sensor fog organizers* ($Hf$) The hardware related specifications for all sensor fog organizers is put in a set denoted by,

$$Hf = \{Hf_1, Hf_2, \ldots, Hf_m\},$$

where $m$ is the number of sensor fog organizers.

*Security schemes used in sensor fog organizers* ($Cf$) The security schemes used in all sensor fog organizers is put in a set denoted by,

$$Cf = \{Cf_1,\ Cf_2, \ldots, Cf_m\},$$

where $m$ is the number of sensor fog organizers.

**Definition 3** (*Sensor fog organizer*) A sensor fog organizer is defined as a set containing the ID, specifications and security measures used, given as,

$$\{F_l,\ Hf_l,\ Cf_l\},$$

where $F_l$ represents the unique ID of a sensor fog organizer, $Hf_l$ represents the hardware specifications of the sensor fog organizer, and $Cf_l$ represents the security scheme used in the sensor fog organizer, and $1 \leq l \leq m$.

The mapping from the sensor network director of layer-2 to the sensor fog organizer of layer-3 is many-to-one and it is denoted as,

$$M'_{23}(.) : N' \rightarrow F_l,$$

where $N'$ is a set containing few sensor network directors, i.e. it is a subset of $N$, and $F_l$ denotes a sensor fog organizer. This represents multiple sensor network directors are mapped into a single sensor fog organizer.

*Cloud computing instance set* ($C$) $C$ is denoting the set of cloud computing instances given as,

$$C = \{C_1, C_2, \ldots, C_r\},$$

where $r$ is the number of cloud computing instances.

**Definition 4** (*Cloud computing instance*) A cloud computing instance at cloud servers' layer is defined as, $\{C_q,\ \{P_q\}\}$ where, $C_q$ is the cloud component ID, $\{P_q\}$ denotes the set of the processing unit IDs of all the essential cloud servers of the instance $C_q$, and $1 \leq q \leq r$.

The mapping from sensor fog organizer at layer-3 to cloud computing instance at layer-4 is many-to-many and it is denoted as:

$$M'_{34}(.) : F' \rightarrow C',$$

where $F'$ is a set containing few sensor fog organizers, i.e. it is a subset of $F$ and $C'$ is a set containing few cloud computing instances, i.e. it is a subset of $C$. This represents multiple sensor fog organizers are mapped into multiple cloud computing instances.

*Memory utilization* The memory utilization is given as,

$$Mem_{ut} = \frac{Mem_{used}}{Mem_{available}},$$

where $Mem_{used}$ and $Mem_{available}$ denotes the amount of used memory and available memory respectively.

*CPU utilization* The CPU utilization is given as,

$$CPU_{ut} = \frac{CPU_{active}}{CPU_{idle} + CPU_{active}},$$

where $CPU_{active}$ and $CPU_{idle}$ denotes the active time period and idle time period of the CPU respectively.

In the mathematical model, we have discussed the mapping between the components of different layers. In the simulation, we implement the same in iFogSim (Gupta et al. 2017). We have used Netbeans IDE for implementing iFogSim. In our simulation classes are created in iFogSim using Java language. The topology for the proposed paradigm is created. It displays the multiple application modules which are formed and endorsed to run on dissimilar physical setup. We first create a physical object and then simulate our proposed paradigm. The created topology is presented in Fig. 2.

As observed from Fig. 2 the sensor nodes are placed in layer 1. The sensor nodes collect respective object status in the environment and transmit the information to the sensor network director in layer 2. Sensor may be homogeneous, heterogeneous, single or multi-dimensional. In layer 2 we have sensor network director. The sensor network director continuously gathers data from the sensors and provides services for the power management and security. The sensor network director sends the collected data to the sensor fog organizer in layer 3. The sensor fog organizer maintains the grouping of multiple sensor network directors and resource virtualization. It acts as a connector between the sensor network director and cloud in a distributed manner. Receiving the request from an application manager or user, it allocates the resources and also responsible for tracking and sharing of available resources. The sensor and geospatial data processing is performed by the sensor fog organizer. Layer 4 contains the cloud.

As we can observe from Fig. 2, multiple sensor nodes of layer 1 are mapped into one sensor network director in layer 2, i.e. the mapping is many-to-one. We have four subsets of sensor nodes. Each subset is mapped to a single sensor network director. We also observe multiple sensor network directors of layer 2 are mapped into one sensor fog organizer in layer 3, i.e. the mapping is many-to -one. We have two subsets of sensor network directors. Each subset is mapped to a single sensor fog organizer. Two sensor fog organizers are connected with the cloud in layer 4, which contains multiple cloud instances. Therefore the mapping is many-to-many. The CPU and memory utilization in case of the proposed paradigm is presented in Fig. 3. For the demand of urgency and privacy the priority resolver is used to deliver the priority request.

In Fig. 4 the percentage of Virtual Machine (VM) access without delay with respect to the normal and priority users are presented. By the term VM access without delay refers to that when a request arrives for VM allocation, without delaying the request is granted. However during VM allocation some latency will obviously be consumed. This is observed from Fig. 4 that if fog computing is used then the VM access without delay is achieved if approximately 20% resources are reserved for priority user. However, if cloud based paradigm Mils-Cloud (Misra et al. 2016) is used, the

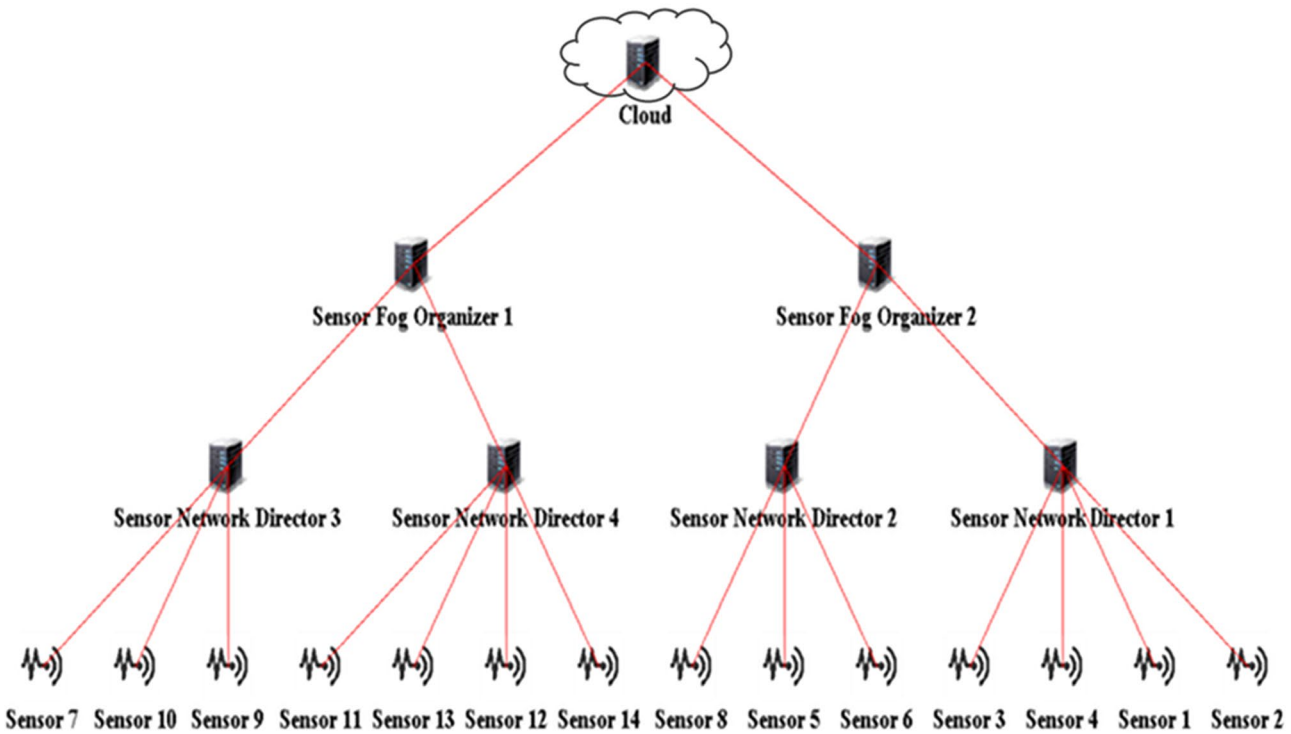



**Fig. 2** Created topology of the proposed multi-sensor geo-fog paradigm in iFogSim

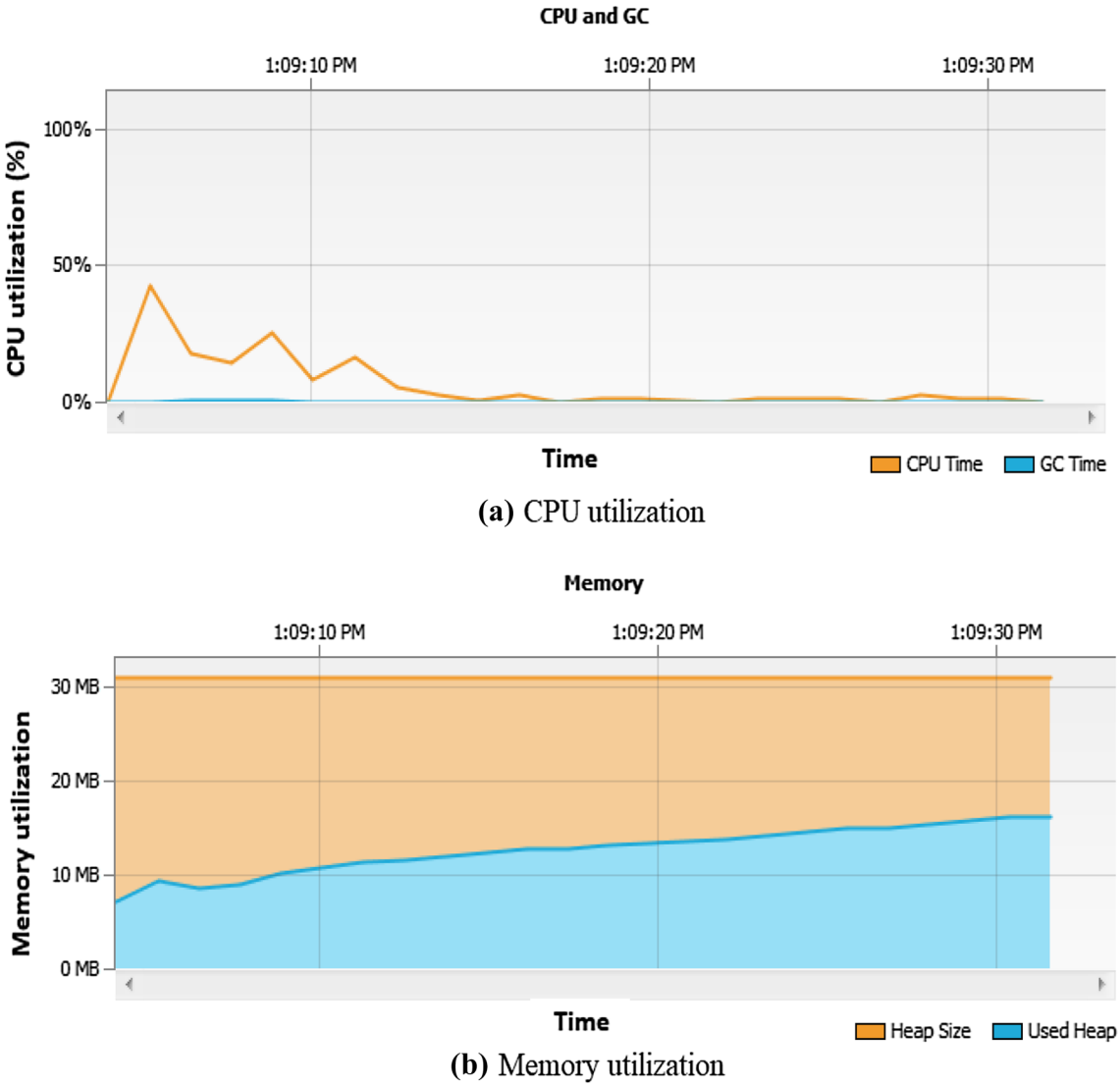



**Fig. 3** CPU and memory utilization during simulation

VM access without delay is achieved if approximately 30% resources are reserved for priority users.

Hence, this is observed that reserving lesser resources in fog based paradigm access to VM can be provided without delay that leads to reduction in resource wastage.

### 3.2 Security mechanism

Defense sector data is very confidential for a country. Unauthorized access and tamper to such information will be harmful. Storing of such confidential information inside the remote cloud servers may compromise with data privacy. The security issues in fog computing has been explored in Zhang et al. (2018). Use of fog device for storing such sensitive data adds an extra layer of security in terms of data privacy (Kumari et al. 2018). However, as sensor fog organizer stores and processes the data, security mechanism should be implemented. Elliptic Curve Cryptography (ECC) (Alowolodu et al. 2013), Hierarchical Identity Based Cryptography (HIBC) (Yan et al. 2009), Keyed-Hash Message Authentication Code (HMAC)-Secure Hash Algorithm (SHA) (Michail et al. 2004), Triple Data Encryption Standard (Triple DES) based Cipher Block Chaining (CBC) and Advanced Encryption Standard (AES) based Cipher Block Chaining (CBC) (Stark et al. 2009) can be used for data security, described as follows:

- As the proposed paradigm is a layered paradigm, for securing fog computing services HIBC can be used. In HIBC at different layer Private Key Generator (PKG) is used. The root PKG hands over private key generation and identity authentication to lower layer PKGs. The root

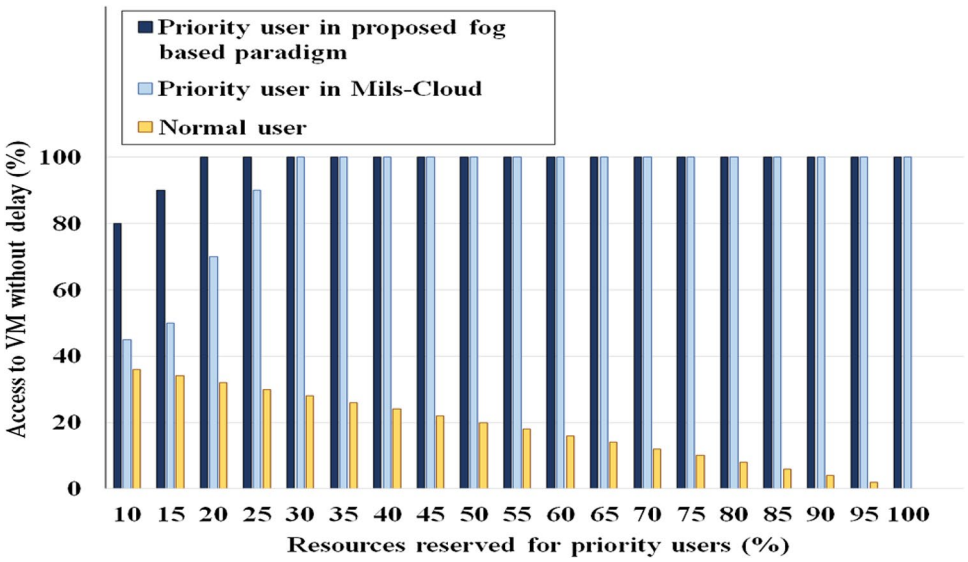



**Fig. 4** VM access without delay (%) for priority user and normal user in proposed fog based paradigm and existing cloud based paradigm

PKG generates private keys for immediate lower layer PKGs, which in turn generate PKGs for their lower levels. The private key transmission and authentication are performed locally. However, instead of HIBC, ECC can also be used for securing fog computing services.

- For securing data storage inside the sensor fog organizer ECC can be used. ECC is a public key cryptography method that generates key using an elliptic curve equation. An elliptic curve over a finite field is given as, $y^2 = x^3 + cx + d$, that contains points which satisfy the equation and a point at infinity. For using ECC, the parties should agree on all elements which define the curve, e.g. the domain parameters. However, for securing data storage homomorphic encryption (Ahmad et al. 2016) can be used. In homomorphic encryption a specific algebraic operation is performed on the plain text data, which is equivalent to a different algebraic operation performed on the cipher text.
- For security during data transmission Triple DES-CBC, HMAC-SHA or AES-CBC can be used. Triple DES (3-EDS) is private key cryptographic algorithm which uses DES three times on each data block. 3-EDS uses three DES keys each of 56 bits. AES is based on substitution-permutation principle. AES uses key size of 128, 192 or 256 bits. HMAC is a message authentication code that uses a cryptographic hash function and a secret key. It is used for data integrity and message authentication. Cryptographic hash function like SHA256 or SHA3 can be used in the calculation of HMAC and then it is called as HMAC-SHA256 or HMAC-SHA3 (Ravilla and Putta 2015; Naito and Wang 2016).

### 3.3 Shortest path algorithm

In the proposed paradigm the sensor data and geospatial data processing is performed inside the sensor fog organizer. After the data processing if any abnormality is detected, then an immediate action will be required from the defense sector to inform the victim region. As the geospatial information processing and analysis takes place inside the sensor fog organizer, a shortest path for communication from the sensor fog organizer to the victim region node will be required. We have used artificial intelligence to find the shortest path. Our paradigm uses a heuristic search algorithm which will find the shortest path. K* (Aljazzar and Leue 2011) is heuristic search algorithm, which is used for finding shortest path between the source ($a$) and target ($b$) nodes. The advantages of K* algorithm are:

- K* avoids exploring and processing of entire problem graph $G$, whereas it partially generates and processes graph portions according to the requirement.
- K* uses the advantage of heuristic search, that improves memory and runtime. K* has an asymptotic worst case complexity of $O(e + vlogv + k)$ with respect to space and time both (Aljazzar and Leue 2011), where the number of vertices and edges are denoted by $v$ and $e$ respectively.

In K* algorithm, A* search is executed in a graph $G$ and Dijkstra's algorithm is used to search in $P(G)$ in an interleaved manner. First A* is executed on $G$ until the target vertex $b$ is selected for the purpose of expansion. After that Dijkstra's algorithm is executed on the available portion of $P(G)$. If $k$ shortest paths are found using Dijkstra's algorithm, then K* successfully terminates. Otherwise to explore bigger portion of the graph $G$, A* resumes execution. This will grow $P(G)$,

which is used by Dijkstra's algorithm afterwards. This process is repeated until Dijkstra's algorithm finds $k$ shortest paths. Now the time complexity of Dijkstra's algorithm is $O(V^2)$ (Arslan and Manguoglu 2018). However, in our paradigm we need an algorithm that will find shortest path for arbitrarily distributed larger graphs in sub-linear time. Hence instead of using Dijkstra's algorithm, we use Δ-stepping algorithm (Arslan and Manguoglu 2018; Meyer and Sanders 2003) in the K*. The Δ-stepping algorithm has time complexity of $O(log^3|V|/loglog|V|)$ (Arslan and Manguoglu 2018; Meyer and Sanders 2003). The K* algorithm (Aljazzar and Leue 2011) based on A* and Δ-stepping is stated in Algorithm 1. The Δ-stepping algorithm (Arslan and Manguoglu 2018; Meyer and Sanders 2003) is stated in Algorithm 2.

**Algorithm 1: K* based shortest path algorithm**

**Input:** A natural number $k$, a graph $G$ with start vertex $a \in V$ and its successor function $suc()$

**Output:** A list $L$ that contains $k$ sidetrack edge sequences which represent $k$ solution paths

**Start**
$queue_D \leftarrow$ Empty priority queue
$table_D \leftarrow$ Empty hash table
$L \leftarrow$ Empty list
$P(G) \leftarrow$ Empty path graph
Run A* on $G$ until $b$ is chosen for expansion
**If** $b$ is not reached, there is no solution and **exit**
**End if**
Add $L$ into $queue_D$
**While** A* queue or $queue_D$ is not empty,
    **If** A* queue is not empty,
        **If** $queue_D$ is not empty,
            Consider $x$ as the head of the search queue of A* and $y$ as the head of $queue_D$
            **Set** $d \leftarrow \max\{d(y) + \Delta(y.y') \mid y' \in suc(y)\}$
            **If** $g(b) + d \le f(x)$, **go to** step 22
            **End if**
        **End if**
        Resume A* to discover a larger portion of the graph $G$
        Refresh $P(G)$ and bring Δ-stepping search into a consistent status
        **Go to** step 10
    **End if**
    **If** $queue_D$ is empty,
        **Go to** step 10
    **End if**
    Remove from $queue_D$ and place on $table_D$ the node $y$ with the minimal $d$-value
    **For** each $y'$ referred by $y$ in $P(G)$
        **Set** $d(y') := d(y) + \Delta(y, y')$
        Attach to $y'$ a parent link that refers to $y$
        Insert $y'$ into $queue_D$
    **End for**
    Consider $\sigma$ as the path in $P(G)$ via which $y$ was reached
    Add $seq(\sigma)$ at the end of $L$
    **If** $|L| = k$,
        **Go to** step 37
    **End if**
**End while**
**Return** $L$ and **exit**
**End**

**Algorithm 2: Δ-stepping search algorithm**

**Input:** $G(V, E)$, $a$ is source vertex, $b$ is target vertex, and weights, $w: E \to R^{+}$
**Output:** The shortest path from $a$ to $b$

**Start**
**For** $v \in V$
  $hev(v) \leftarrow \{(v,u) \in E : w(v,u) > \Delta\}$
  $lit(v) \leftarrow \{(v,u) \in E : w(v,u) \leq \Delta\}$
  $dis(v) \leftarrow \infty$
**End for**
$rex(a,0)$
**Set** $i \coloneqq 0$
**While** $M$ is not empty
  $X \coloneqq \phi$
  **While** $M[i]! = \phi$
    $Q \coloneqq \{(u, dis(v) + w(v,u)) : v \in M[i] \wedge (v,u) \in lit(v)\}$
    $X \coloneqq X \cup M[i]$
    $M[i] \coloneqq \phi$
    **For** $(v,x) \in Q$
      $rex(v,x)$
    **End for**
  **End while**
  $Q \coloneqq \{(u, dis(v) + w(v,u)) : v \in X \wedge (v,u) \in hev(v)\}$
  **For** $(v,x) \in Q$
    $rex(v,x)$
  **End for**
  **If** the target node is processed,
    **break**
  **End if**
  **Set** $i \coloneqq i + 1$
**End while**
**End**

The *rex* function is calculated using the following steps:

**If** $x < dis(v)$,
  $M[\lfloor dis(v)/\Delta \rfloor] \leftarrow M[\lfloor dis(v)/\Delta \rfloor] \setminus \{v\}$
  $M[\lfloor x/\Delta \rfloor] \leftarrow M[\lfloor x/\Delta \rfloor] \cup \{v\}$
  $dis(v) \leftarrow x$
**End if**

Using this algorithm the shortest path from the sensor fog organizer node to the victim region node is found and the alert message is sent to the node if abnormality is detected after processing the defense related sensor data of a region. After receiving the message, the defense sector admin at the victim region will take necessary action to protect the region. As in the proposed paradigm K* heuristic search algorithm is used to find the shortest path, the proposed multi-sensor geo-fog paradigm is referred as an intelligent paradigm.

#### 3.3.1 Shortest path to victim zone during disaster management

The sensor fog organizer has the geospatial information of a geographical region along with the sensor data. When a disaster is detected from the collected sensor data after processing, the sensor fog organizer sends a message to the cloud servers along with the geo-location information of the victim region. The sensor fog organizer also sends messages to the voluntary organizations and the health care centres nearby

the victim region, so that they can provide the preliminary support. The cloud servers when receives a message from the sensor fog organizer regarding disaster in an area, the cloud servers send multicast message to different supporting organizations and health centres. In such situation providing faster service is a promising issue. For this purpose it is required to find out the shortest path for travelling from the supporting agency to the victim region. From the geospatial information the location of the victim region is determined and using K* algorithm shortest paths from the supporting organizations and health centres to the victim region are found. The personnel from the supporting organizations and health centres reach the affected region following the shortest path.

## 4 Delay and energy consumption of proposed paradigm

The mathematical notations used for determining the delay and energy consumption in the proposed paradigm are listed in Table 2.

### 4.1 Delay calculation

The delay for sensor data collection is given as,

$$D_s = \frac{d_s}{d_{sc}}. \tag{3}$$

The delay for geospatial data collection is given by,

$$D_{gs} = \frac{d_{gs}}{d_{gsc}}. \tag{4}$$

The delay for data transmission from sensor nodes to sensor network director is given by,

$$D_{s\_tr} = (1 + f_{s\_snd})\frac{d_s}{R_{s\_snd}}. \tag{5}$$

The delay for data transmission from geospatial data collecting node to sensor network director is given by,

$$D_{gs\_tr} = (1 + f_{gs\_snd})\frac{d_{gs}}{R_{gs\_snd}}. \tag{6}$$

The delay for data transmission from sensor network director to sensor fog organizer is given by,

$$D_{snd\_sfo} = (1 + f_{snd\_sfo})\frac{d_s + d_{gs}}{R_{snd\_sfo}}. \tag{7}$$

The data processing delay inside the sensor fog organizer is given as,

$$D_{proc\_sfo} = \frac{d_s + d_{gs}}{Sp_{sfo}}. \tag{8}$$

The delay for data transmission from sensor fog organizer to the cloud servers is given as,

$$D_{sfo\_cld} = p_{cl}(1 + f_{sfo\_cld})\frac{d_{sfo\_cld}}{R_{sfo\_cld}}. \tag{9}$$

The propagation delay is given as,

$$D_{prop} = \left(\frac{di_{s\_snd}}{c} + \frac{di_{gs\_snd}}{c} + \frac{di_{snd\_sfo}}{c}\right) + p_{cl} \cdot \frac{di_{sfo\_cld}}{c}. \tag{10}$$

The delay for the proposed paradigm is obtained by summing up Eqs. (3)–(10) as follows,

$$D_{def} = D_s + D_{gs} + D_{s\_tr} + D_{gs\_tr} + D_{snd\_sfo} + D_{proc\_sfo} + D_{sfo\_cld} + D_{prop}. \tag{11}$$

### 4.2 Energy consumption calculation

The energy consumption for data collection by sensor nodes is given as,

$$E_s = D_s \cdot e_c. \tag{12}$$

The energy consumption for data collection by geospatial data collecting node is given by,

$$E_{gs} = D_{gs} \cdot e_{gc}. \tag{13}$$

The energy consumption for data transmission from sensor nodes to sensor network director is given by,

$$E_{s\_tr} = D_{s\_tr} \cdot e_t. \tag{14}$$

The energy consumption for data transmission from geospatial data collecting node to sensor network director is given by,

$$E_{gs\_tr} = D_{gs\_tr} \cdot e_{gt}. \tag{15}$$

The energy consumption for data transmission from sensor network director to sensor fog organizer is given by,

$$E_{snd\_sfo} = D_{snd\_sfo} \cdot e_{sndt}. \tag{16}$$

The energy consumption for data processing inside the sensor fog organizer is given as,

$$E_{proc\_sfo} = D_{proc\_sfo} \cdot e_{sfop}. \tag{17}$$

The energy consumption for data transmission from sensor fog organizer to the cloud servers is given as,

$$E_{sfo\_cld} = D_{sfo\_cld} \cdot e_{sfot}. \tag{18}$$

The energy consumption during propagation is given as,

**Table 2** List of mathematical notations used for delay and energy calculation

| Parameter | Definition |
|---|---|
| $d_{sc}$ | Sensor data collection per unit time |
| $d_{gsc}$ | Geospatial data collection per unit time |
| $d_s$ | Collected sensor data |
| $d_{gs}$ | Collected geospatial data |
| $d_{sfo\_cld}$ | Data amount transmitted from sensor fog organizer to cloud servers |
| $R_{s\_snd}$ | Data amount transmission from sensor nodes to sensor network director per unit time |
| $R_{gs\_snd}$ | Data amount transmission from geospatial data collecting node to sensor network director per unit time |
| $R_{snd\_sfo}$ | Data amount transmission from sensor network director to sensor fog organizer per unit time |
| $R_{sfo\_cld}$ | Data amount transmission from sensor fog organizer to cloud servers per unit time |
| $f_{s\_snd}$ | Link failure rate during data transmission from sensor node to sensor network director |
| $f_{gs\_snd}$ | Link failure rate during geospatial data transmission from geospatial data collecting node to sensor network director |
| $f_{snd\_sfo}$ | Link failure rate during data transmission from sensor network director to sensor fog organizer |
| $f_{sfo\_cld}$ | Link failure rate during data transmission from sensor fog organizer to cloud servers |
| $Sp_{sfo}$ | Data processing speed of sensor fog organizer |
| $di_{s\_snd}$ | Distance between sensor node and sensor network director |
| $di_{gs\_snd}$ | Distance between geospatial data collecting node and sensor network director |
| $di_{snd\_sfo}$ | Distance between sensor network director and sensor fog organizer |
| $di_{sfo\_cld}$ | Distance between sensor fog organizer and cloud servers |
| $c$ | Propagation speed |
| $p_{cl}$ | Probability of sending data to cloud servers |
| $e_t$ | Energy consumption for data transmission by sensor nodes per unit time |
| $e_c$ | Energy consumption of sensor nodes per unit time during data collection |
| $e_{gt}$ | Energy consumption of geospatial data collecting node for data transmission per unit time |
| $e_{gc}$ | Energy consumption of geospatial data collecting node per unit time during data collection |
| $e_{sndt}$ | Energy consumption of sensor network director for data transmission per unit time |
| $e_{sfot}$ | Energy consumption of sensor fog organizer for data transmission per unit time |
| $e_{sfop}$ | Energy consumption of sensor fog organizer for data processing per unit time |
| $e_s$ | Energy consumption of a node per unit time during propagation period |
| $e_{snd}$ | Energy consumption of sensor network director per unit time during propagation period |
| $e_{sfo}$ | Energy consumption of sensor fog organizer per unit time during propagation period |

$$E_{prop} = \left( \frac{di_{s\_snd} \cdot e_s}{c} + \frac{di_{gs\_snd} \cdot e_s}{c} + \frac{di_{snd\_sfo} \cdot e_{snd}}{c} \right) + p_{cl} \cdot \frac{di_{sfo\_cld} \cdot e_{sfo}}{c}. \quad (19)$$

The energy consumption for the proposed paradigm is obtained by summing up Eqs. (12) to (19) as follows,

$$E_{def} = E_s + E_{gs} + E_{s\_tr} + E_{gs\_tr} + E_{snd\_sfo} + E_{proc\_sfo} + E_{sfo\_cld} + E_{prop}. \quad (20)$$

## 5 Performance evaluation

In this section, we analyse the performance of the proposed paradigm based on theoretical results obtained using MATLAB and simulation results obtained using QualNet (Scalable Network Technologies 2018).

### 5.1 Theoretical analysis

We have used MATLAB 2015 for the theoretical analysis. The amount of data collected, transmitted and processed in considered 100–1000 MB.

Figure 5 presents the delay of the proposed fog computing based paradigm for defense sector calculated using Eq. (11) and in the existing cloud based paradigm Mils-Cloud for military tri-services. The data collection, transmission, processing and propagation delays are summed up to calculate the total delay. The delay is measured in second (s).

In the proposed paradigm as the sensor fog organizer performs the data processing, the data transmission and propagation delays are reduced. Consequently the total delay is decreased. With respect to the existing cloud based paradigm Mils-Cloud (Misra et al. 2016), the proposed paradigm

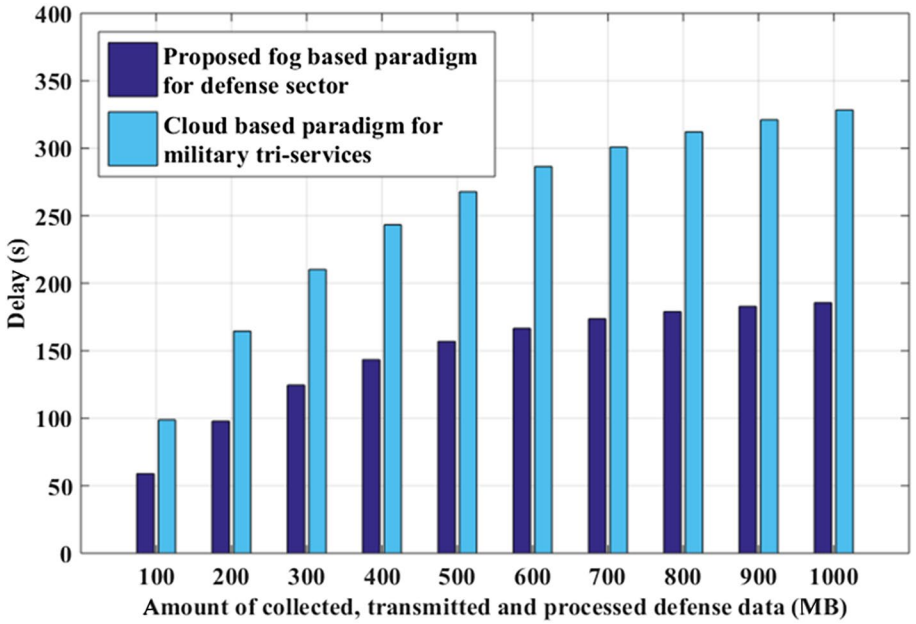



**Fig. 5** Delay of the proposed fog based paradigm for defense sector and existing cloud based paradigm for military tri-services

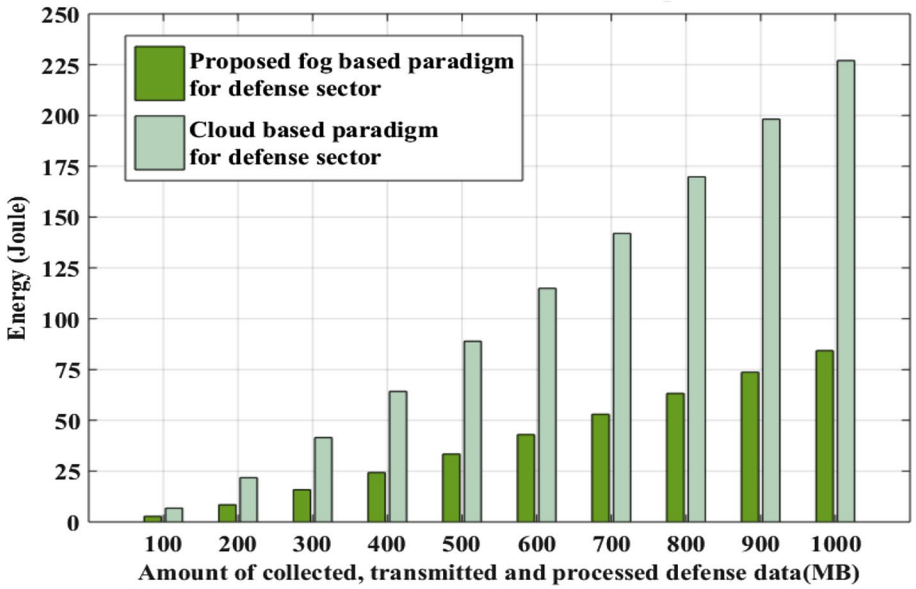



**Fig. 6** Energy consumption of the proposed fog based paradigm and existing cloud based paradigm for defense sector

reduces the delay by approximately 40–43%, as observed from Fig. 5.

Figure 6 presents the energy consumption of proposed fog based paradigm calculated using Eq. (20) and existing cloud based paradigm for defense sector. The energy consumption during data collection, transmission, processing and propagation, are summed up to calculate the total energy consumption of the paradigm. The energy consumption is measured in Joule.

Figure 6 illustrates that the proposed paradigm has 59–62% less energy consumption than the cloud based paradigm for defense sector. Use of the sensor fog organizer for data processing and storage instead of the cloud servers saves energy. Thus we can refer the proposed multi-sensor geo-fog paradigm as an energy-efficient paradigm.

## 5.2 Simulation results

We created the proposed multi-sensor geo-fog network scenario in QualNet (Version 7) (Scalable Network Technologies 2018). The simulation parameters are defined in Table 3. Figure 7 presents the proposed network scenario created using QualNet. We have considered two sensor

network directors and one sensor fog organizer. Under each sensor network director four sensors including GPS are placed. Sensors 1 (node 1), 2 (node 2), 3 (node 3) and 4 (node 4) are placed under sensor network director 1 (node 5). Sensors 5 (node 6), 6 (node 7), 7 (node 8) and 8 (node 9) are placed under sensor network director 2 (node 10). These two sensor network directors are connected with sensor fog organizer (node 11), which is connected with the cloud server (node 12). The performance of the proposed paradigm has been analyzed with respect to throughput, delay, jitter, and energy consumption. The simulation time has been considered 600 s. The size of data item has been assumed 4096–20,480 bits and number of data items sent between consecutive nodes has been assumed 100.

**Table 3** List of parameters used in simulation

| Layer | Parameter | Value |
|---|---|---|
| Physical layer | Radio type used | 802.11b radio |
| | Antenna model used | Omni directional |
| | Packet reception model used | PHY 802.11b |
| | Noise Factor | 10.0 |
| | Temperature | 290.0 K |
| MAC layer | MAC protocol | 802.11 |
| Network layer | Network protocol | IPV4 |
| Transport layer | Buffer size for data transmission and reception | For sensor node: 1024 bytes<br>For sensor network director: 4096 bytes<br>For sensor fog organizer: 8192 bytes<br>For cloud server: 16,384 bytes |

### 5.3 Throughput of network

Throughput is the rate of successful message delivery over a network, and it has been measured in bits per second. The throughput of the network in case of our proposed paradigm is 50,000–25,000 bits/s approximately for the considered parameter values. Figure 8 presents the throughput of the proposed network scenario.

### 5.4 Average delay of network

Figure 9 presents the average delay of the proposed multi-sensor geo-fog network and sensor cloud network scenarios for defense sector and the delay has been measured in second. The delay is the time required by the data to travel from the sending node to the receiving node.

From the simulation results it is observed that in proposed fog based network and in cloud based network the average delay are approximately 0.015–0.019 s and 0.016–0.021 s respectively for the considered parameter values. Thus it is illustrated that the proposed fog based network scenario reduces the average delay by approximately 9–11% than the cloud based network scenario.

### 5.5 Average jitter in network

Figure 10 presents the average jitter of the proposed multi-sensor geo-fog network and sensor cloud network scenarios for defense sector and the jitter has been measured in second. The jitter is the difference between the delay in transmission of the current and previous packets.

From the simulation results, it can be observed that in proposed fog based network and in cloud based network for defense sector the average jitter are approximately 0.006–0.01 s and 0.0065–0.011 s respectively for the considered parameter values. Thus it is illustrated that the proposed fog based network scenario reduces the average jitter by approximately 10–14% than the cloud based network scenario.

### 5.6 Energy consumption of network

Figure 11 presents the energy consumption of the proposed multi-sensor geo-fog network and sensor cloud network and the energy consumption is measured in milliwatthour. The energy consumption of the nodes in transmit and receive modes are summed up to determine the total energy consumption.

From the simulation results it is observed that in proposed fog based network and in cloud based network for defense sector the energy consumption are approximately 0.85–1.81 mWh and 1.01–2.06 mWh respectively for the considered parameter values. Thus it is illustrated that the proposed fog based network scenario reduces the energy consumption by approximately 12–15% than the cloud based network scenario.

### 5.7 Inference from the simulation results

From the results, we observe that the proposed paradigm will provide:

- Approximately 9–11% less delay than the cloud based scenario for defense sector.
- Approximately 10–14% less jitter than the cloud based scenario for defense sector.
- Approximately 12–15% less energy consumption than the cloud based scenario for defense sector.

Thus we can conclude that the proposed fog based paradigm for defense sector reduces delay, jitter, and energy consumption than the existing cloud based paradigm.

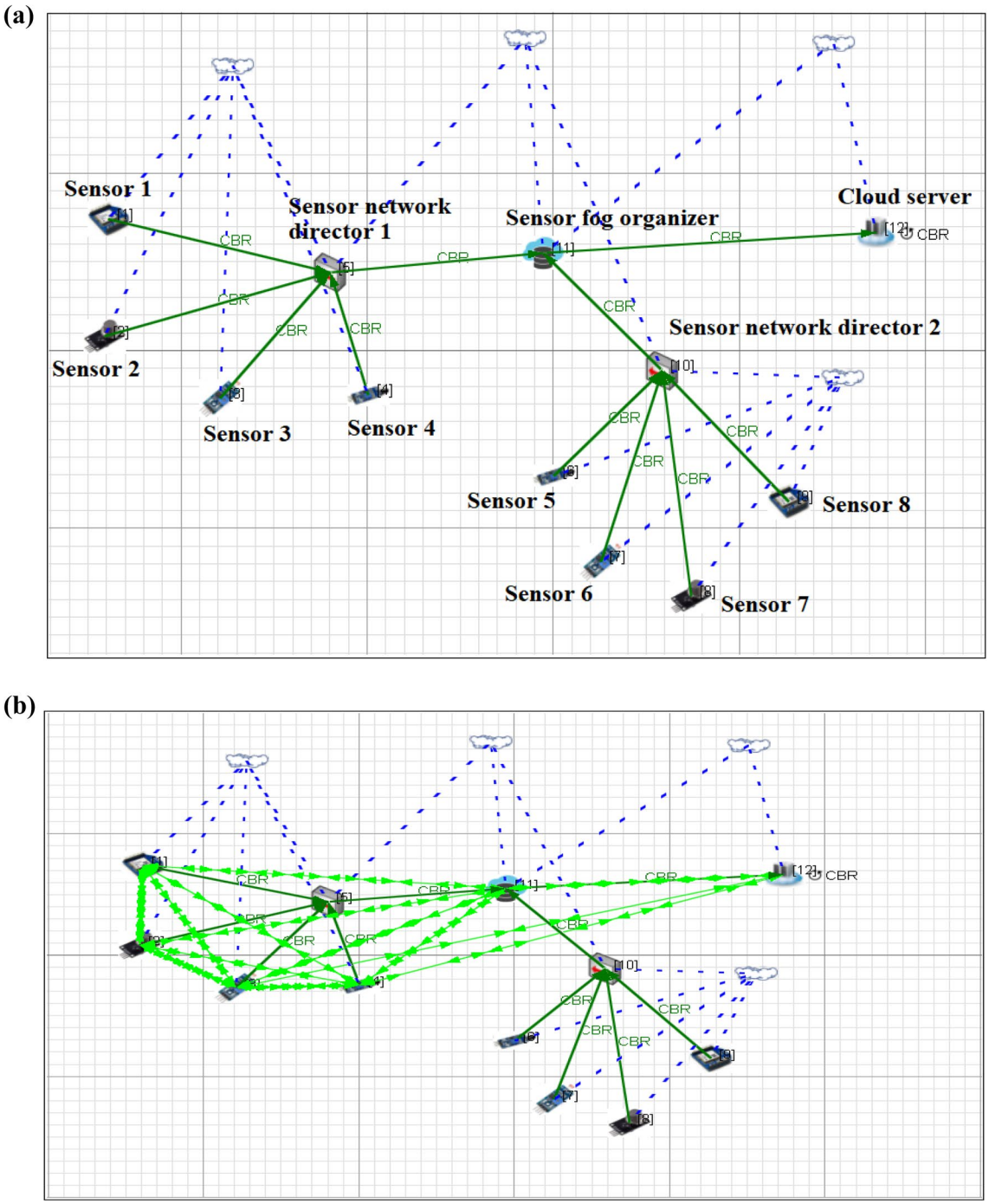



**Fig. 7** **a** Simulation scenario of proposed multi-sensor geo-fog network for defense sector. **b** Simulated multi-sensor geo-fog network for defense sector during execution

## 6 Conclusions and future work

In a geographical region sensor and geospatial data are collected, and processed inside the fog device of the respective region. After processing if any abnormality is detected in the data or emergency situation occurs, then shortest path to the victim region is determined using intelligent K* heuristic search algorithm, where A* and Δ-stepping algorithm are used. The mathematical model of the proposed paradigm is developed. Use of the fog device for data storage and

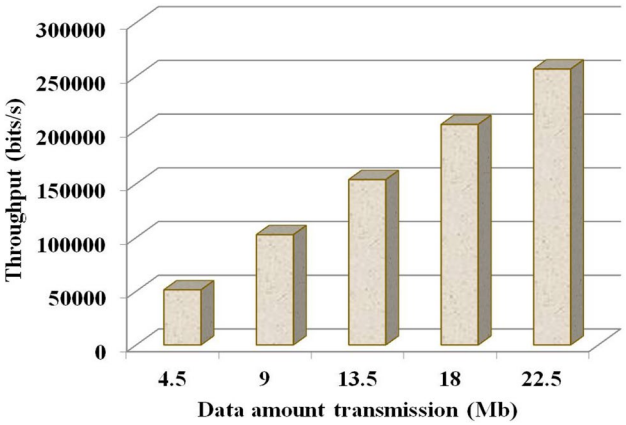



**Fig. 8** Throughput of the proposed multi-sensor geo-fog network

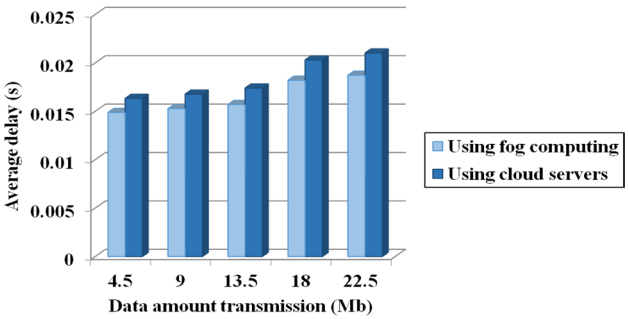



**Fig. 9** Average delay of proposed multi-sensor geo-fog network and sensor cloud network

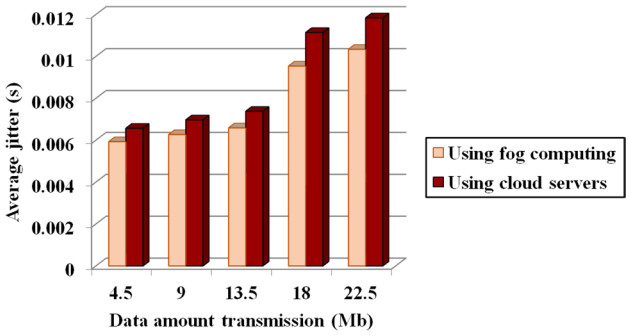



**Fig. 10** Average jitter of proposed multi-sensor geo-fog network and sensor cloud network

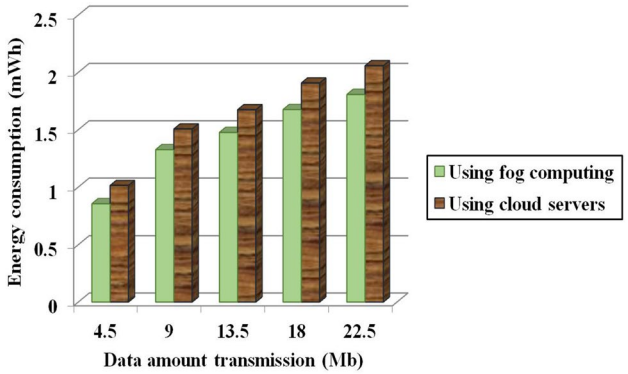



**Fig. 11** Energy consumption of proposed multi-sensor geo-fog network and sensor cloud network

processing for a particular region instead of sharing data over the cloud servers reduces energy and delay. The proposed network scenario is simulated in QulaNet. The simulation results present that using the proposed fog based network scenario average delay, jitter and energy consumption are reduced by 9–11%, 10–14% and 12–15% respectively than the cloud based network. Thus we can conclude that the proposed paradigm is energy-efficient. The proposed paradigm is simulated in iFogSim and its performance is evaluated based on CPU, memory utilization and access to VM without delay for prioritized and normal users. The simulation result shows that reserving around 20% of resources increases performance of the proposed paradigm to the priority user and availability of the normal user is also not compromised. In our paradigm the fog device plays the key role in the storage and processing of geospatial data. However, as different regions are considered, the collaboration of the fog and edge devices of adjacent regions can also take an important role to make the decision making faster in emergency situation. Hence, collaboration between edge and fog devices of different regions is a promising future scope of the proposed paradigm.

**Acknowledgements** This research work is partially supported by TEQIP-III, MAKAUT, West Bengal and Department of Science and Technology, Government of India through research project under Indian Institute of Technology Kharagpur, and Melbourne-Chindia Cloud Computing (MC3) Research Network.

## References

Ahmad M, Amin MB, Hussain S et al (2016) Health Fog: a novel framework for health and wellness applications. J Supercomput 72(10):3677–3695

Aljazzar H, Leue S (2011) K*: a heuristic search algorithm for finding the k shortest paths. Artif Intell 175(18):2129–2154

Alowolodu OD, Alese BK, Adetunmbi AO et al (2013) Elliptic curve cryptography for securing cloud computing applications. Int J Comput Appl 66(23):10–17

Arslan H, Manguoglu M (2018) A parallel bio-inspired shortest path algorithm. Computing 101:969–988

Barik RK, Dubey H, Mankodiya K, Sasane SA, Misra C (2019) GeoFog4Health: a fog-based SDI framework for geospatial health big data analysis. J Ambient Intell Human Comput 10(2):551–567

Burmaoglu S, Saritas O, Yalcin H (2019) Defense 4.0: Internet of Things in military. In: Emerging technologies for economic development. Springer, Cham, pp 303–320

Chi Y, Moon HJ, Hacigümüş H et al (2011) SLA-tree: a framework for efficiently supporting SLA-based decisions in cloud computing. In: Proceedings of the 14th international conference on extending database technology. ACM, pp 129–140

Chiang M, Zhang T (2016) Fog and IoT: an overview of research opportunities. IEEE Internet Things J 3(6):854–864

Das J, Dasgupta A, Ghosh SK et al (2019) A learning technique for VM allocation to resolve geospatial queries. In: Recent findings in intelligent computing techniques. Springer, Singapore, pp 577–584

Dastjerdi AV, Buyya R (2016) Fog computing: helping the Internet of Things realize its potential. Computer 49(8):112–116

De Paola A, Ferraro P, Re GL, Morana M, Ortolani M (2019) A fog-based hybrid intelligent system for energy saving in smart buildings. J Ambient Intell Human Comput. https://doi.org/10.1007/s12652-019-01375-2

Devarajan M, Subramaniyaswamy V, Vijayakumar V, Ravi L (2019) Fog-assisted personalized healthcare-support system for remote patients with diabetes. J Ambient Intell Human Comput. https://doi.org/10.1007/s12652-019-01291-5

Gai K, Qiu M, Zhao H et al (2016) Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing. J Netw Comput Appl 59:46–54

Guerrero C, Lera I, Juiz C (2019) A lightweight decentralized service placement policy for performance optimization in fog computing. J Ambient Intell Human Comput 10(6):2435–2452

Gupta H, Dastjerdi AV, Ghosh SK et al (2017) iFogSim: a toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments. Softw Pract Exp 47(9):1275–1296

Huang L, Li G, Wu J et al (2016) Software-defined QoS provisioning for fog computing advanced wireless sensor networks. In: SENSORS, 2016 IEEE. IEEE, pp 1–3

Kertesz A, Pflanzner T, Gyimothy T (2018) A mobile IoT device simulator for IoT-Fog-Cloud systems. J Grid Comput. https://doi.org/10.1007/s10723-018-9468-9

Kumari A, Tanwar S, Tyagi S et al (2018) Fog computing for Healthcare 4.0 environment: opportunities and challenges. Comput Electr Eng 72:1–13

Limkar SV, Jha RK (2018) A novel method for parallel indexing of real time geospatial big data generated By IoT devices. Future Gener Comput Syst 97:433–452

Lin K, Xia F, Li C et al (2019) Emotion-aware system design for the battlefield environment. Inf Fusion 47:102–110

Luan TH, Gao L, Li Z et al (2015) Fog computing: Focusing on mobile users at the edge. arXiv:1502.01815

MacEachren AM, Robinson A, Hopper S et al (2005) Visualizing geospatial information uncertainty: what we know and what we need to know. Cartogr Geogr Inf Sci 32(3):139–160

Madria S, Kumar V, Dalvi R (2014) Sensor cloud: a cloud of virtual sensors. IEEE Softw 31(2):70–77

Meyer U, Sanders P (2003) Δ-stepping: a parallelizable shortest path algorithm. J Algorithms 49(1):114–152

Michail HE, Kakarountas AP, Milidonis A et al (2004) Efficient implementation of the keyed-hash message authentication code (HMAC) using the SHA-1 hash function. In: Proceedings of the 2004 11th IEEE international conference on electronics, circuits and systems, 2004. ICECS 2004. IEEE, pp 567–570

Misra S, Singh A, Chatterjee S et al (2016) Mils-cloud: a sensor-cloud-based architecture for the integration of military tri-services operations and decision making. IEEE Syst J 10(2):628–636

Misra S, Chatterjee S, Obaidat MS (2017) On theoretical modeling of sensor cloud: a paradigm shift from wireless sensor network. IEEE Syst J 11(2):1084–1093

Mnassri B, Ananou B, Ouladsine M (2009) Fault detection and diagnosis based on PCA and a new contribution plot. IFAC Proc Vol 42:834–839

Mukherjee A, De D, Roy DG (2016) A power and latency aware cloudlet selection strategy for multi-cloudlet environment. IEEE Trans Cloud Comput 7(1):141–154

Mukherjee A, Deb P, De D et al (2018) C2OF2N: a low power cooperative code offloading method for femtolet-based fog network. J Supercomput 74(6):2412–2448

Mutlag AA, Ghani MKA, Arunkumar N et al (2019) Enabling technologies for fog computing in healthcare IoT systems. Future Gener Comput Syst 90:62–78

Naito Y, Wang L (2016) Replacing SHA-2 with SHA-3 enhances generic security of HMAC. In: Cryptographers' track at the RSA conference. Springer, Cham, pp 397–412

Rahmani AM, Gia TN, Negash B et al (2018) Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: a fog computing approach. Future Gener Comput Syst 78:641–658

Ramasamy M (2019) Design and implementation of cognitive radio sensor network for emergency communication using discrete wavelet packet transform technique. In: International conference on distributed computing and internet technology. Springer, Cham, pp 270–278

Ravilla D, Putta CSR (2015) Implementation of HMAC-SHA256 algorithm for hybrid routing protocols in MANETs. In: 2015 International conference on electronic design, computer networks and automated verification (EDCAV). IEEE, pp 154-159

Satyanarayanan M, Bahl V, Caceres R, Davies N (2009) The case for vm-based cloudlets in mobile computing. IEEE Pervasive Comput 8(4):14–23

Scalable Network Technologies (2018) QualNet - Network Simulation. https://www.scalable-networks.com/qualnet-network-simulation. Accessed Feb 2019

Sen A, Madria S (2017) Risk assessment in a sensor cloud framework using attack graphs. IEEE Trans Serv Comput 10(6):942–955

Stark E, Hamburg M, Boneh D (2009) Symmetric cryptography in javascript. In: Computer security applications conference, pp 373–381

Venticinque S, Amato A (2019) A methodology for deployment of IoT application in fog. J Ambient Intell Human Comput 10(5):1955–1976

Wang SL, Chen YL, Kuo AMH et al (2016) Design and evaluation of a cloud-based Mobile Health Information Recommendation system on wireless sensor networks. Comput Electr Eng 49:221–235

Xiang Y, Balasubramanian B, Wang M et al (2013) Self-adaptive, deadline-aware resource control in cloud computing. In: 2013 IEEE 7th international conference on self-adaptation and self-organizing systems workshops (SASOW). IEEE, pp 41–46

Xie YX, Chen X G, Zhao J (2011) Data fault detection for wireless sensor networks using multi-scale PCA method. In: 2011 2nd international conference on artificial intelligence, management science and electronic commerce (AIMSEC). IEEE, pp 7035–7038

Yan L, Rong C, Zhao G (2009) Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography. In: IEEE international conference on cloud computing. Springer, Berlin, pp 167–177

Yaqoob S, Ullah A, Akbar M, Imran M, Shoaib M (2019) Congestion avoidance through fog computing in internet of vehicles. J Ambient Intell Human Comput. https://doi.org/10.1007/s12652-019-01253-x

Zhang Q, Cheng L, Boutaba R (2010) Cloud computing: state-of-the-art and research challenges. J Internet Serv Appl 1(1):7–18

Zhang P, Zhou M, Fortino G (2018) Security and trust issues in Fog computing: a survey. Future Gener Comput Syst 88:16–27

Zhu C, Leung VC, Wang K et al (2017) Multi-method data delivery for green sensor-cloud. IEEE Commun Mag 55(5):176–182