Multimedia Tools and Applications (2024) 83:7249–7272
https://doi.org/10.1007/s11042-023-15363-4

A nomadic multi-agent based privacy metrics for e-health care: a deep learning approach

Chandramohan Dhasarathan[1] · M. Shanmugam[2] · Manish Kumar[1] · Diwakar Tripathi[3] · Shailesh Khapre[4] · Achyut Shankar[5,6,7]

Received: 23 December 2021 / Revised: 7 March 2023 / Accepted: 15 April 2023 /
Published online: 6 June 2023

Abstract
In recent years, there has been a surge in the use of deep learning systems for e-healthcare applications. While these systems can provide significant benefits regarding improved diagnosis and treatment, they also pose substantial privacy risks to patients' sensitive data. Privacy is a crucial issue in e-healthcare, and it is essential to keep patient information secure. A new approach based on multi-agent-based privacy metrics for e-healthcare deep learning systems has been proposed to address this issue. This approach uses a combination of deep learning and multi-agent systems to provide a more robust and secure method for e-healthcare applications. The multi-agent system is designed to monitor and control the access to patients' data by different agents in the system. Each agent is assigned a specific role and has specific data access permissions. The system employs a set of privacy metrics to a substantial privacy level of the data accessed by each agent. These metrics include confidentiality, integrity, and availability, evaluated in real-time and used to identify potential privacy violations. In addition to the multi-agent system, the deep learning component is also integrated into the system to improve the accuracy of diagnoses and treatment plans. The deep learning model is trained on a large dataset of medical records and can accurately predict the diagnosis and treatment plan based on the patient's symptoms and medical history. The multi-agent-based privacy metrics for the e-healthcare deep learning system approach have several advantages. It provides a more secure system for e-healthcare applications by ensuring only authorized agents can access patients' data. Privacy metrics enable the system to identify potential privacy violations in real-time, thereby reducing the risk of data breaches. Finally, integrating deep learning improves the accuracy of diagnoses and treatment plans, leading to better patient outcomes.

Keywords Privacy Preserving · Deep learning system · Multi-Agent · Knowledgebase · Security

✉ Achyut Shankar
ashankar2711@gmail.com

Extended author information available on the last page of the article

1 Introduction

E-healthcare systems deal with sensitive and confidential information, making privacy protection a critical issue. Multi-Agent based Privacy Metrics for E-Healthcare Deep Learning Systems is an emerging field that involves the use of Multi-Agent Systems (MAS) for evaluating the privacy of healthcare data processed by Deep Learning algorithms. 1. In "Privacy-Preserving Deep Learning for Medical Imaging: A Meta-Analysis Approach," the authors propose a privacy-preserving framework for deep learning in medical imaging. They employ a federated learning model aggregating the local models from multiple hospitals without sharing sensitive data. The framework uses differential privacy to protect the confidentiality of the data. Agent-based privacy-preserving data sharing for collaborative healthcare approach to ensure data sharing in healthcare. The agents negotiate the data-sharing process between healthcare providers and patients, ensuring privacy and security. The proposed system employs encryption and blockchain technology to secure the data. A multi-agent reinforcement learning approach for a privacy-preserving deep learning system for e-healthcare using Multi-Agent Reinforcement Learning (MARL). The system uses agents to learn from data while preserving the privacy of the data. The agents interact with each other to make decisions based on their known policies. A multi-agent approach the research focuses on proposing a multi-agent approach to privacy-preserving deep learning in healthcare. The system employs a combination of homomorphic encryption, differential privacy, and federated learning to protect the confidentiality of the data. Multi-agent-based Privacy Metrics for E-Healthcare Deep Learning Systems is an essential field that aims to protect the privacy of sensitive healthcare data. The proposed approach uses federated deep learning, differential privacy, homomorphic encryption, and blockchain to secure the data. This paper presents a privacy-preserving multi-agent deep learning framework for healthcare data, which uses differential privacy techniques to protect patient privacy. Moreover, a multi-agent system distributes the deep learning tasks among the agents and uses secure aggregation to aggregate the results without revealing sensitive information. The proposed framework is evaluated using a real-world dataset, and the results show that it provides good privacy protection while maintaining high accuracy.

1.1 Privacy observation for multi-agent system using Deep Learning System(DPLS)

E-healthcare systems provide a platform for patients to access medical services without physical contact with their healthcare providers. However, using e-health care systems has privacy concerns that must be addressed. Multi-agent-based privacy metrics have emerged as a solution to privacy concerns in e-health care systems.

1.1.1 Multi-agent system design level for DPLS

$$Multi-Agent\ System\ desing\ level = size + component\ structure + complexity + function$$

$$Multi-Agent\ System\ desing\ level = \sum_{i=1}^{n} \left(act_a + mtr \right) + \left(org_{hr} + org_{fn} \right) + \{re, env, ph, soc\} + fn_{sreq}$$

In the contemporary scientific world, unforeseen health-related issues and tribulations are emerging into new diseases for the next generation. Medication and its treatment levels are advanced to the next level to support the human race. Patient's regular health check-ups in

hospices and continuous guidance from practitioners are added as habitual in a typical human life. However, it might not support the patients who arrive at critical care in a fraction of a minute. As a sustaining connotation for healthcare (HC), the body sensors (BS) have espoused regular monitoring of the patients, irrespective of patients daily activities BS would follow them as a shadow without their intervention. The sensed information is transmitted to the medication department exclusively and is expected to reach the concerned practitioner without delay and intervention. The collected health data is forwarded through a Smartphone or intelligent device capable enough to do the networking miniaturize. There are issues with data forecasting to the base station or healthcare management system. This paper mainly focuses the Coordinator Specific Optimized Healthcare Monitoring (CSOHM) on patient data forwarding during a routine, emergency, and critical cases. However, if every patient has their own device, bring your own devices (BYODs) then there comes a data privacy problem for sharing resources using BYODs. For organizing the competent device resources, there might be an optimization technique to do resource allocation in the network framed due to its mobility ad hoc nature. To do the resource allocation process, the proposed system adopts the artificial bee colony approach to evolve information collected from the patient's sensors for a pre-cautionary medication process. The efficiency of the proposed method is evaluated with existing techniques. The experimental result analysis shows that the proposed system performs comparatively high in all scenarios and maintains a high-reliability rate in delivering sensitive data more effectively.

1.2 Multi-agent system working level for DPLS

$$\begin{aligned} &Multi-Agent\ system\ working\ level \\ &\quad = communication + interaction + knowledge + lifeness + conflict\ management + community \\ &\quad + management + application + stability + performance + organization \end{aligned}$$

$$\begin{aligned} &Multi-Agent\ system\ working\ level = \\ &\quad = \left[\, lang\left(sof_a + other_a\right) + act\right] + md_{ty}\left(sof_a + other_a\right) + lear_{outc} + \left(adp_a + ssmain_{eff}\right) \\ &\quad + \left(neg_a + sys_{ts}\right) + \left[\left(comm_a\right)_0^n collb_a\right] + \left(coor_a\left(sstr_a\right)\right) + \left(appar + \left[coop\right]_0^n\right) + \sum selrp_a \\ &\quad + \left(perf + perf_a\right) + r(cu, pl, ar, md, comm, ob, dmk) \end{aligned}$$

It cannot organize and maintain the coordinators private information safety and trust. They are identifying appropriate users privilege, and their confidentiality level needs to be considered more concerned with the support of multi-level computing. A Peer to Peer opportunistic computing and routing system also socializes with tolerable message transmission with privacy metrics. Software interface for effective machine optimization would support the critical and emergencies of E-health monitoring. A crisis is caused in any circumstance to handle it with cooperative information sharing to the centralized system for the betterment of recovery. Monitor the regular activity with intensive care and react quickly to speed up the monitoring and medication process. The monitoring activity could be organized periodically to collect the patient medical data for appropriate treatment and action. The specified agent could regularize the movement of a patient to monitor the active process. Multiple agents cooperatively monitor the process for an organized medication process to prolong the integral e-health structure. E-health monitoring is a good activity for a balanced medication process for complex maintenance integrated by multiple cooperation. Each agent monitors the patient's health activity and periodically reports to the E-health centralized agent for medication by

appropriate experts in time. To collect a patient's regular exercise, the deployed agents always run as an active depict. The main proper treatment objective is the appropriate treatment at the right time to avoid a patient's critical situational cases, the medication must be processed with a cooperative multi-agent hierarchy approach. Emergency and essential E-health organizations with multi-agent unified monitoring by on-demand computing lead to a risk of collaborative device participation in communicating appropriate medication. The devices handling critical situations are provided by agreeing to the multi-agent terms and conditions. To develop a good trust for the devices participating in the cooperative task which handles the emergencies. Participative agent's personal data privacy preserving strategy by adopting the mathematical approach, statistical information, information policy act, and encryption techniques to ensure the multi-agent coordination with privacy metrics. Timestamp routing by swarm intelligence is expressed in Section 2. In Section 3 we designed and proposed a nomadic multi-agent privacy metric system using an optimization model incorporating the artificial bee colony approach in the framework. The need for a deep learning system for analyzing healthcare data under various sensor data and devices is formulated for a protective analysis. The analytical result analysis is discussed and the efficiency variations are illustrated and plotted respectively in Section 4. Section 5 concluded that the privacy metric needed for a healthcare system and enhancement features for future research are discussed.

2 Literature study and related work

A framework to collect patients' data in real time, perform appropriate nonintrusive monitoring, and propose medical and life style engagements in (Abdelghani et al., 2007 [5]) whenever needed and appropriate. The framework, which relies on service-oriented architecture (SOA) and the Cloud, allows seamless integration of different technologies, applications, and services. It also integrates mobile technologies to smoothly collect and communicate vital data from a patient's wearable biosensors while considering the mobile devices' limited capabilities and power drainage in addition to intermittent network disconnections. A cyber-physical co-design approach to structural health monitoring based on wireless sensor networks. The approach of (Gregory Hackmann et al., 2014 [22]) closely integrates 1) flexibility-based damage localization methods that allow a tradeoff between the number of sensors and the resolution of damage localization, and 2) an energy-efficient, multilevel computing architecture specifically designed to leverage the multi-resolution feature of the flexibility-based approach. An opportunistic ad hoc localization algorithm called Urban Pedestrians Localization (UPL) has been suggested in (Akire et al., 2013 [39]) for estimating locations of mobile nodes in urban districts and an algorithm to calculate the movable areas of mobile nodes considering obstacles for predicting the area of presence of mobile nodes accurately under mobility. Two opportunistic routing algorithms for intermittently connected mobile P2P networks, which exploit the spatial locality, spatial regularity, and activity heterogeneity of human mobility to select relays have been proposed by (Sheng,ling et al., 2013 [42]). The rapidly growing number of portable devices and the amount of transmitted data make routing even harder. Scalable, distributed, and lightweight intermittently connected mobile outperform the state-of-the-art in terms of delivery latency and delivery ratio. Opportunistic computing for on-demand resource computation can be effectively carried out as discussed by (Dhasarathan et al., 2018 [11] ; 2015 [10]) developed an opportunistic privacy-preserving framework for cloud-based services.

To derive the first upper bound on the flooding time, it is a decreasing function of the maximal speed of the nodes. The bound holds with high probability, and it is nearly tight

even if the network is sparse and disconnected, information spreading can be fast has been identified (Andrea et al., 2013 [13]). In heterogeneous distributed computing systems solving the problems for an effective task handlito (Qinma Kang et al.,2013 [23]) reduces the total execution and communication costs by using the honeybee mating optimization (HBMO) algorithm. Service integration would be reconfigured by (Frederico Lopes et al., 2014 [29]) the semantic integration of services provided with respect to distinct sources is handled by a middleware Open Context Platform Integration system. However, it is designed to support the service-oriented architecture based on the context-provision. It also maintains the reliability of the system with an adaptation mechanism to adapt service execution during failures. This system balances both the Quality of Service and the Quality of Context among various services. Identified the impact of topology changes in service communication (Groba et al., 2014 [19]), in order to reduce service failure a composition protocol is designed and it can able to allocate and minimize the service invoked at the provider's end. Moreover, its ability to choose appropriate services opportunistically at the time of the service requisition process. The service sequences and parallel service flows are supported from time to time. It also avoids deadlock occurrences and terminates the service to a valid end state by allocating the correct service response for requested sub-services.

A multi-user diversity is adopted to select node channels that gain more data rates from the listing (Mehta, N.B et al., 2013 [31]) channels to frame the highest channel power gain. A low feedback timer triggers to select the best node in a distributed fame. A mapping carried with respect to time value to evaluate the channels gain using a real values metrics. An optimal algorithm is designed for identifying the best node from the selected nodes using a pragmatic optimal mapping algorithm. A distributed optimal Community-Aware Opportunistic Routing (CAOR) algorithm was developed (Mingjun Xiao et al., 2014 [44]) to address the routing problems in a delay-tolerant network caused to frame of a Mobile social network. The focus on reducing the computational and maintenance cost with minimum delays of nodes in a home-aware community model. A reverse Dijkstra algorithm is used to improve the optimal opportunistic routing performance. A specific sensing mechanisms is in need to build under designed and opportunistic computing machines (Gupta, P et al., 2013 [21]) for sensing infrastructure and integrating to the software interface to improve the machine potentiality. To improve the machine computing effective optimization algorithm should be adopted for handling the sensing information which collected from industrial infrastructure.

The user activity monitoring by markov-reward model propagation in a primary network might support (Alcaraz, J.J et al., 2014 [2]) to improve the performance using secondary users 'activity. Through Bayesian estimation channel access technique an imperfect sensing can be remobilized to expect capacity and boost to improve the overall performance of a spectrum allocation for an effective utilization. Service suitability and sustainability to perform in a distributed environment with an customized framework designed by (Chandramohan et al., 2014 [9]). Through opportunistic resource utilization the potentiality of a network can be served under active sharing of recourses and infrastructure (Singh, C et al., 2012 [38]) by a multi hop routing. There are issues while sharing resources pertaining with personal information, theory of transferable payoff coalitional might limit the exchange of confidential information shared in a distributed computation as a preventive measure. In a pervasive computing environment a Smartphone-based sensor are used among humans (Josh Wall et al., 2011 [41]) in everyday life. Through automated computing smart phones energy management issues are increasing tremendously. An agent based approach might reduce the active promotion of serious issue among human intervention. The optimization techniques improvement by (Akira et al., 2013) for the vast development of industries and humanization particularly in urban region to

pinpoint a mobile node is critical task, to identify it, a pedestrians opportunistic localization algorithm for predicting the area of presence of mobile nodes in an urban region. The current location information of node is updated by its neighboring mobile nodes and also relies on obstacles as the nodes moves randomly. Identified the proactive source routing for opportunistic data forwarding might harmoniously integrated (Zehua Wang et al., 2011 [47]) to reduce the data overhead while discarding timestamp routing in wireless networks. Bio-inspired approach to preserve users information with artificial bee colony approach proposed by (Dhassrathan et al., 2021 [16]). Fog computing can be deployed closer to the users to meet the Vehicular Networks (VN) to deliver network services. Software Defined Networking (SDN) might support the use of large-scale fog-enabled VN services (Jeferson Nobre et al., 2018 [32]). The researchers are focusing to address the diversity of VN enabled fog applications. It is focusing on the perspectives of the systems, networking, and ubiquitous services. A real time scenario is taken into consideration for a fast traffic accident rescue management in a real-time trafficking data.

Interrelated structure for fault-location and classification technique for transmission lines (Ashok kumar et al., 2018 [4]) with distribution of good power quality. The synchrophasor measurements identify for the classification of regression modeling in all transmission line. The magnetic flux from the transmission line in ideal condition to the projects with faults location. Privacy preserving in a distributed web service environment with a framework dealt with an ad-hoc scenarios. The service requester's demands are not gets fulfilled by the quality of retrieved services (Dhasarathan et al., 2018). Privacy policy extensibility is applicable for the services providers in all constraint based satisfactions. It is validated by optimization algorithms to check the efficiency. In Fog enabled environmental services are gets Delayed and its Load is estimated (Nandor Verba et al., 2018 [40]) in a shared services. The requirements are tested in real-time test cases and industrial standards to check its efficiency. Virtual and physical validation is verified in a contemporary data environment. The delay in transmission gets improved and also the data delivery rate gets effectively improved based on the optimization approaches.

Patient-care amenities related healthcare services is taken into intensive are by Edge of Things (EoT) (Golam Rabiul et al., 2018 [1]) as a persuasive healthcare management. The edge computing service providers (ECSP) and cloud computing service provider (CCSP) observes the patients health in regular intervals and gets all health information using body area networks (BAN). The article proposed a portfolio optimization solution based on virtual mechanism (VM) with the deliverable cloud service. To achieve the service distribution a centralized service monitoring and portfolio optimization is introduced by EoT. It supports as a cost effective system in a personalized health care management system using VM supportable techniques to improve the smart health care services. Moreover, it improves the smart device and mobile applications to support the health care services in a secure and safe incarceration. The patient details would be categorized based on the data analytics techniques (D'Agostino, et al., 2018 [14]) for identifying the low power devices utilized in real-time environments for monitoring the microbiome. The portable devices are neutral in nature it have an ambiguous architecture which needs a ubiquitous analysis in all diversified environments. To process the data collectively integrated form resources of ubiquitous environment devices have huge amount of relevant and irrelevant data which needs to be communicated and gets convert into useful information. A scheduling mechanism is adopted for a reliable communication to pipeline the cloud based services and edge computing devices.

It is proposed an efficient information interaction, multimodal data fusion, and automatic production (Long Hu et al., 2018 [28]) to improve the edge computing. The interaction based systems are highly demand for utilizing the e-health services in a robotic

architectural neutral system management. The cognitive management of multimodal fusion is carried in both traditional and real-time scenarios. Resource scheduling is highlighted by the artificial intelligent driving force. All computing resources are expanded by edge computing techniques for promoting the economic growth. Sentimental analysis is endorsed as an unsupervised learning with AI as the core competitiveness. The efficiency of the cognitive manufacturing adopts a highly interconnected structure and composition for the significant improvement in chip assembly. The article discussed the need for a multi-agent based cloud service endorsement in ubiquitous computing scenarios (Chandramohan et al., [10]). The agents would analysis the possibilities of proper communications in all circumstances with minimum resource utilization. The cloud enabled devices would share the device information with all service providers on demand. It could increase the privacy issue of the device owners and put them at based service utilization with proactive privacy-preserving measures is taken into consideration in effective resource sharing and communication.

IoT-based learning for network communications to improve human-computer interaction (Rihab Boussada et al.,2019 [7]) for the betterment of service sharing and utilization. It involves huge sensible data processing and transformation in every service cattalos. The researchers are forecasting acceptable and rescindable research has been highlighted with limited privacy-preserving information. There is a need to concentrate on contextual and content-based privacy preservation in IoT-based communications. It is focused on identity-based encryption schemes based on the availability of resources for data transferring. Healthcare emergency monitoring using a bio-inspired approach has a predictive measure for the effective recovery of the patient from health risks as illustrated by (Dhasarathan et al., 2021). The existing study dealt with the contemporary computing and routing architecture which inculcate randomly and cannot develop trust in cooperative systems.

It has crypto mechanisms for ensuring the handshake process between the devices. There is a need to develop a privacy metric with the collaboration of a mathematical approach, statistical data, a privacy policy customized, and an advanced encryption mechanism for the betterment of user trust. Shaoxin Li et al., 2019 [25] mining the storage region based on the frequent access utility to be reconstructed based on a maximum data request. Collecting data from various domains are manifested to build an effective protocol that can control the user's information on continuous monitoring was discussed by Haider Sajjad et al., 2019 [36]. To maintain the scalability of big data mining have filtered selective data streams that are eligible to prevent confidential data collection and its applicability was described by Chamikara et al., 2019 [8]. In the cloud, data effectiveness could be achieved by enabling the collaborative fusion of various resource providers and its monitoring privileges need to be organized with a proper verification process developed by Qiang Zhang et al., 2019 [48]. Network file tracking mechanisms and packet switching between different organizations' private information is kept in safe opportunistic coordination when it gets routed the personal data by Samaneh Rashidibajgan et al., 2019 [35]. Edge resources optimization from the various devices collected with respect to crowded data collection in different geographical regions is processed as per the task assigned and the system has scheduled completion management led by Hang Shen et al., [37].

Guoming Wang et al., 2019 [43] discussed that the electronic health monitoring and guidance of patients with primary symptoms and various clinical records must be prevented. Shangwei Guo et al., 2019 [20] image-based identification and classification of multimedia that focuses on data filtering as per the requirements and its descriptions to be prevented as confidential metadata. A neurocomputing for facial recognition-based privacy-preserving strategy was developed to prevent the third parties intrusion Yuancheng Li et al., 2019 [26]. The cloud services that fulfill encrypted mechanisms adopt homomorphic encryption

to ensure the confidentiality of uses information addressed by Mohammad Saidur Rahman et al., 2019 [34]. The vehicular network predicts the mobility of different vehicles that are collaborative with the base station for effective transportation in an optimized way of communication designed to minimize the overall burden of an intelligent transportation system Yousheng Zhou et al., 2019 [51]. In the era of information prevention various sectors become an unpredictable clash that would affect the economy of any nation that supports multi-party circular computation Zhiliang Deng et al., 2019 [15]. Dongmei Li et al., 2019 [27] Machine learning-based approach would help the beneficiary withdraw the offer issued by the feature extraction method. Rasim M et al., 2019 [3] a deep learning mechanism to preserve the identical information of a user to integrate data analysis with machine learning techniques for user privacy modeling. Michael Bewong et al., 2019 [6] high confidential transaction data have the potential to prevent serial communication in the information management system.

Alper Yargic et al., 2019 [46] information processing would develop a mechanism to do all comparative analyses to magnify multi-criteria collaborative filtering the unwanted request and allowing authenticated users. Tengfei Yang et al., 2019 [45] encrypted images are processed from various outsourced network that pinpoint the flaws in outsourcing computational resources. Zhuoran Ma et al., 2019 [30] machine learning mechanism to predict the decisions in the healthcare system with a distinct human-computer intervention as a unique computational machine. Ubiquitous computing for effective content collection that assists human in a directed information management developed to resolve automatic computation Xu Zheng et al., 2019 [49]. Map-reduce technology can join various data collected under a similar bucket for notable prevention Xiaofeng Ding et al., 2019 [18]. Anonymization of private data in healthcare management that finds the relationship between medication and transactions performed with patient's information might lead to privacy breaches in electronic monitoring Vartika Puri et al., 2019 [33]. The secret sharing authentication system that predicts remote monitoring with a biometric authentication process is developed bt H. Kaur et al., 2019 [24]. Information processing from the storage region would follow the aggregation of supervised data organization to test the authenticity of private information requestor's information management was discussed by Hong Zhong et al., 2018 [50]. Kongtao Chen et al. [12] tensor processing units follow various convolutional network statergies to model the structural components of data collected with respect to similar domains that could be monitored by a smart system. Chandramohan et al., 2023 [17] developed a framework that can predict the possibilities of data breaches that would cause series drawbacks in healthcare sectors by evaluating the COVID-19 patient's data illustrated.

3 Nomadic multi-agent privacy metric

The process of transmitting body sensor data thereby collected from the patients in a healthcare management system might lead to a critical case if the information handover gets delayed. Deployed sensors fuse the information collected periodically from the hostility through the devices they are connected with. It must maintain energy backup for data transmission to handle critical and emergency cases. Each and every device has limited battery backup, computing energy, bandwidth, memory, interoperability, mobility, etc. If any emergency situation takes place with wireless BSN, the next hop is the only choice to share and transmit the data collected from the BSN. The condition became horrible if the next hop could not participate in sharing its resource for certain period of time. Thereby, coordinator specific opportunistic computing technique is proposed to handle these situations and

provide an optimal solution to overcome the emergency and critical scenarios. A clustering concept is incorporated in the coordinator process and to take intelligent decisions the virtual coordinator it acts as a cluster head for effective task handling. It is suggested from the literature study that many more optimization models and systems are available to do these tasks. However, the proposed system follows the artificial bee colony approach due to it's constrain based optimization handling in wireless sensor networks.

3.1 Optimization model

To find the best nearest solution from a set of available solutions an optimization model is needed to identify an optimized time. Thereby enormous approaches and prerequisite techniques are available for improving the system efficiency and increasing its effectiveness comparatively high compared to traditional models. It might be applied to problems that are considered to be unsolvable in polynomial time. More specifically nature inspired algorithmic approach plays a decisive role in solving unpredictable combinations to frame a set of valid computing parameters. An ant colony, bee colony, particle swarm intelligence, bird intelligent, and even more are available to apply for finding the optimum solution for a given problem. However, it is identified from the literature study in wireless networking, sensor networking, body area networking, mobile networking, etc., solving problems in these areas artificial bee colony approach is widely applied to find the nearest possible solution. This work arrives at an initialization of adopting the artificial bee colony algorithm for searching and identifying the appropriate information which is expected for the collaborative task.

3.2 Artificial bee colony model

There presents one or more bee colony approaches to search and identify the optimum resource in a wireless environment. Whereas, Bee colony approach, honey bee matting algorithm, artificial bee colony algorithms are widely circulating in the information technology era. However, for wireless sensor& body sensor network artificial bee colony (ABC) approach is highly recommended by the academicians, practitioners and researchers. This research work aims to stall an iterative improvement in utilizing unused resources by adopting the ABC for finding the appropriate resources in right time and also for a cooperative task handling.

In the initialization of the algorithm, a set of solutions (food source positions) are randomly generated by the scout bees, let X i ={x_i1, x_i2, ... , x_in } represent the i^{th} food source in the population, and thereby each solution is generated by Eq. (1)

$$x_{ij} = x^{j}_{min} + \text{rand}\,(0,1)\left(x^{i}_{max} - x^{j}_{min}\right) \tag{1}$$

$$v_{ij} = x_{ij} + \phi_{ij}\left(x_{ij} - x_{kj}\right) \tag{2}$$

$$P_i = \frac{0.9 * fit_i}{fit_{best}} + 0.1 \tag{3}$$

$$fit_i = \frac{1}{1 + f_i} \tag{4}$$

Where x_{jmin} and x_{jmax} are the lower and upper bounds of the j^{th} parameters of the solution i. During initialization, the population is evaluated and then, is repeated with the search processes of the employed bees the onlooker bees and the scout bees. Each employed bee is associated with a particular food source and in each iteration; it searches a new food source in the neighborhood of the food source in her memory by using Eq. (2).Where ij is a random number between [1, 1], t_i is a candidate food source position, x^i is the current food source position, x^k is a neighbor food source position, and j 2{1, 2, ... , D } is randomly chosen index which represents a component of each food source position and D is the dimension of the problem. Once t^i is obtained and evaluated, it is compared to x^i. When t^i is better than x^i, it will replace with x^i and become a new member of the population. In other words, greedy selection process is applied; when the nectar amount of the new one is higher than that of the previous one, the bee memorizes the new position and forgets the old one; otherwise, she keeps the position of the previous one in her memory. After all employed bees complete the search process; they come into the hive and share the nectar information of their sources with onlooker bees by dancing. Then, each onlooker prefers a food source area depending on the nectar information distributed by the employed bees. The preference is carried out probabilistically, where the preference probability of the solution i, pi, depends on the nectar amount of food source i and pi is calculated by Eq. (3): where fi_t best is the quality of the best solution among the current solutions and fi_t is the quality of the solution i which is proportional to the nectar amount of the food source i, given as (4). Where fi is the objective function value of the associated solution i. In basic ABC, the onlooker bee selects a solution by roulette wheel selection method which provides better candidates to have a greater chance of being selected. Then, it searches new solution in the neighborhood of the selected solution by Eq. (2) and applies a greedy selection process to choose the new solution or to keep the old one. Static boundaries (SB) establishment may varies from 100m to few kilometers. Figure.1 shows the Dynamic membership (DM), each mobile opportunistic node (MON) registered with HMS and communicates via coverage specific intelligent agent (IA).Intelligent Agent IA= $\{IA_1, IA_2, IA_3, \ldots, IA_n\}$

Mobile Opportunistic Node MON= $\{MON_x, MON_y, . MON_\infty\}$

Coverage Specific Optimization Clustering (CSOC) = (Static Boundary * Dynamic Membership)

$$\mathrm{CSOC} = [\mathrm{IA1}, \mathrm{IA2}, \mathrm{IA3}, \ldots, \mathrm{IAn}] * \begin{bmatrix} MON_x & MON_y & MON_\infty \\ MON_{x1} & MON_{y1} & \vdots \\ MON_{x2} & MON_{y2} & \vdots \\ \vdots & \vdots & \vdots \\ MON_{xn} & MON_{yn} & MON_\infty \end{bmatrix}$$

The computing is carried out by identifying the right node which is ready for further sharing with HMS resource sharing policy. Figure.1 shows the coordinator specific Intracluster Information Updating for Health care Model. It is expressed with each cluster head and its nodes coordinates having limited reachable range and access capabilities.

Privacy Cluster (PC), Privacy Coordinator Agent= $\{PC_1, PC_2, PC_3 \ldots, PC_n\}$, Private User (PU), Emergency Privacy Node (PN). Mobile node distance 'd', computing power 'p', bandwidth 'b' and memory available 'm' as shown in Fig. 1 follows a deep learning based approach to frame the static boundary with the dynamic nodes in and around the region.

Emergency Private Iinformation= Privacy cluster (Emergency Node)

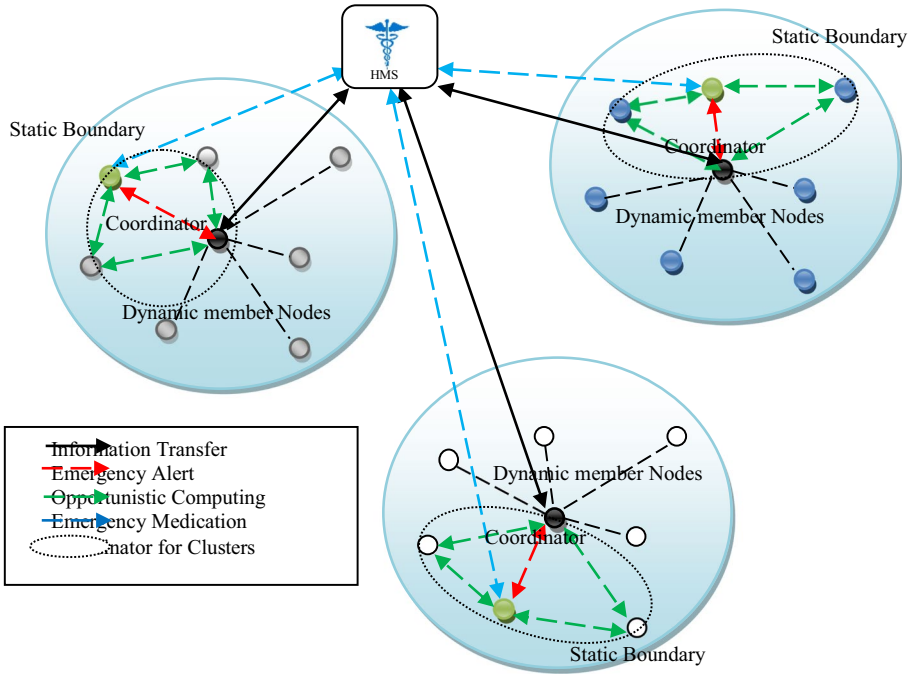

Fig. 1 A Deep learning based Static Boundary clustering of coordinator specific Intra-cluster Information mobile nodes

$$\Rightarrow \mathrm{PC}\left(PU_1, PU_2, PU_3, \ldots, PU_{\mathrm{n}}\right)$$

$$\Rightarrow \text{Where, } PU_{\mathrm{n}} = PU_{\mathrm{x}} * \begin{bmatrix} PU_{x11} & PU_{x12} & PU_n \\ PU_{x21} & PU_{x22} & \vdots \\ PU_{x31} & PU_{y32} & \vdots \\ \vdots & \vdots & \vdots \\ PU_{xm} & \ldots & PU_{mn} \end{bmatrix} * [\mathrm{d, p, b, m}]$$

$$PU_{x_{ij}} * \begin{bmatrix} PU_{d11} & PU_{p12} & PU_{b13} & PU_{m14} \\ PU_{d21} & PU_{p22} & PU_{b23} & PU_{m24} \\ PU_{d31} & PU_{p32} & PU_{b33} & PU_{m34} \\ \vdots & \vdots & \vdots & \vdots \\ PU_{dm1} & PU_{pm2} & PU_{bm3} & PU_{mm} \end{bmatrix} \begin{bmatrix} PU_{d11} & PU_{p12} & PU_{b13} & PU_{m14} \\ PU_{d21} & PU_{p22} & PU_{b23} & PU_{m24} \\ PU_{d31} & PU_{p32} & PU_{b33} & PU_{m34} \\ \vdots & \vdots & \vdots & \vdots \\ PU_{dm1} & PU_{pm2} & PU_{bm3} & PU_{mm} \end{bmatrix} \cdots \begin{bmatrix} PU_{d1} & \cdots & PU_{m1} \\ \vdots & \ddots & \vdots \\ PU_{dm} & \cdots & PU_{mm} \end{bmatrix} n$$

$$\mathrm{EPN} = PU_{x_{ij}} [\because (\mathrm{x_i})_{\mathrm{j}} => \mathrm{i} = \{\mathrm{d,p,b,m}\} \text{and } \mathrm{j} = \{\text{number of mobile opportunistic nodes}\}]$$

$$\begin{bmatrix} MON_x & MON_y & MON_\infty \\ MON_{x1} & MON_{y1} & \vdots \\ MON_{x2} & MON_{y2} & \vdots \\ \vdots & \vdots & \vdots \\ MON_{xn} & MON_{yn} & MON_\infty \end{bmatrix} \begin{bmatrix} PU_{d11} & PU_{p12} & PU_{b13} & PU_{m14} \\ PU_{d21} & PU_{p22} & PU_{b23} & PU_{m24} \\ PU_{d31} & PU_{p32} & PU_{b33} & PU_{m34} \\ \vdots & \vdots & \vdots & \vdots \\ PU_{dm1} & PU_{pm2} & PU_{bm3} & PU_{mm} \end{bmatrix} \begin{bmatrix} PU_{d11} & PU_{p12} & PU_{b13} & PU_{m14} \\ PU_{d21} & PU_{p22} & PU_{b23} & PU_{m24} \\ PU_{d31} & PU_{p32} & PU_{b33} & PU_{m34} \\ \vdots & \vdots & \vdots & \vdots \\ PU_{dm1} & PU_{pm2} & PU_{bm3} & PU_{mm} \end{bmatrix} \cdots \begin{bmatrix} PU_{d1} & \cdots & PU_{m1} \\ \vdots & \ddots & \vdots \\ PU_{dm} & \cdots & PU_{mm} \end{bmatrix} n$$

$$\Rightarrow EON_{x_{ij}}\left(\mathrm{x_{dpbm}}\right)_{\mathrm{n}}\left[\because(\mathrm{xi})\mathrm{j}\right]$$
$$\Rightarrow PC_n.\prod_{n=1}^{\infty} PU_n$$
$$\therefore Emergency\ Health\ Information = PC_n.\prod_{n=1}^{\infty} PU_n$$

In Fig. 2 shows the structure of collective on-demand classification of nodes with the help of Multi-Agent system working level deals with the agent communication, level of agent interaction, knowledge, lifeness, conflict management, community, management, application, stability, performance and organization. Agent communication is stated as the various communication languages of other agent and its action to be carried. *communication* $comm=[\ lang(sof_a+other_a)+act]$. Interaction states the type of interaction with software agent and other agent, *interaction* $int=md_{ty}(sof_a+other_a)$. Knowledge of refers to the outcome of agent learning *knowledge* $kng=lear_{outc}$. Lifeness refers to the adaptation of agent and symbolizes system maintenances efforts *lifenes* $lif=(adp_a+ssmain_{eff})$. Conflict management deals with the agent negotiation and system tasks. *conflict mangement* $conf_{mg}=(neg_a+sys_{ts})$. Community refers to the different levels of agent communication in regards to agent collaboration. *community* $cmty=\left[\left(comm_a\right)_0^n collb_a\right]$. Management level refers to the various level of agent coordination with respect to agent system structures. *management level* $mg=(coor_a(sstr_a))$. Application level refers to the application area and different agent role cooperation. *application level* $app=\left(appar+\left[coop\right]_0^n\right)$. Stability level states the measure of agent self-reproduction. *stability level* $stb=\sum selrp_a$. Performance level states the performance and performance of an environment. *performance level* $prf=(perf+perf_a)$. Organization level parameters

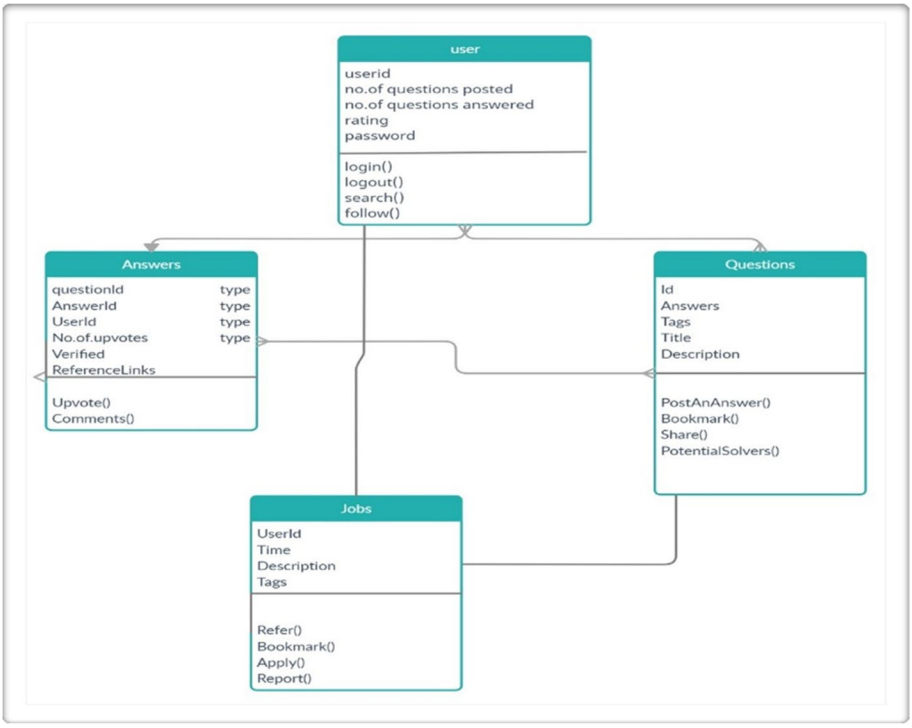

Fig. 2 Deep Learning Based UML Classification for Privacy Preserving System

deals with the various roles of agent such as customer, planner, archivist, mediator, communicator, observer and decision maker. *organization level* $org = r(cu, pl, ar, md, comm, ob, dmk)$.

3.2.1 Multi-agent system description level for DPLS

$$Multi - Agent\ system\ description\ level = development + application + publication$$
$$Multi - Agent\ system\ description\ level = \left(id_a + \ dyn + doc \right) + [doc]_0^n + \left(mk_{as} + acc_{user} \right)$$

3.2.2 Agent development life cycle for DPLS

$$Agent\ development\ life\ cycle = phase\ level + milestone\ level + requirement\ workflow\ level$$

$Agent\ development\ life\ cycle = \{ str, sz, c \} + \sum_{i=1}^{n} ms_a + \left[req_a \right]$Agent development method level states about the various stages involved in the development method level, and its parameters such as methodology level, paradigm level and case level. Methodology level tries to find out suitable development method for agent implementationDmd_a.*methodolgy level* $mth = \prod Dmd_a$. Paradigm levels used to identify the relevance of selected development paradigmDmd_{pard}, *paradigm level* $= \prod Dmd_{pard}$.Case level parameters state the tools support-$tl_{sp}$for the agent implantation (Tables 1, 2 and 3).

3.2.3 Agent development method level for DPLS

Agent development method level $=$ *methodology level* $+$ *paradigm level* $+$ *case level*; *Agent development method level* $= \prod Dmd_a + \prod Dmd_{pard} + tl_{sp}$ Agent development management level metric deals with the all management level activity and the parameters are project management level, configuration management level and quality management level. Project management level state the developer risksdev_{rs} and the method $m_a$involved in the agent development.*project mangement level* $proj_{mgl} = dev_{rs} + m_a$. Configuration management level states the success of the version control with respect to the agent and thus*configuration management level* $= \left(\frac{n}{k} \right) p^k q^{n-k}$, wheren stands for number of trails, k denotes the number of success , n − k represents the number of failures, p denotes the probability of success of version control based on agent in one trails, $q = 1 - p$ probability of failures in one trail. Quality management level parameter state the quality assurance techniqueqtec$_a$ involves in software agent. *quality management level* $q_{mgl} = [\text{qtec}_a]$.

3.2.4 Agent development management level DPLS

Agent developer level metric state the parameters involved in the development of agent such as skill level, communication level and productivity level. Agent skill level involves the developer skill dev_{sk} and implementation of agentimp_a. *skill level* $sk_l = (\ dev_{sk} + imp_a)$. Agent communication level parameter deals with the work advance based on collaboration *collb* and cooperation *coop* . *communication level* $comm_l = wk_{adv}(collb + coop)$. Productivity level states the amount of work done $w = f * d$.

$$Agent\ development\ management\ level = project\ management\ level + configuration\ management\ level + quality\ management\ level$$
$$Agent\ development\ management\ level = \left(dev_{rs} + m_a \right) + \left(\frac{n}{k} \right) p^k q^{n-k} + \left[\text{qtec}_a \right]$$

Table 1 Privacy Metrics for DPLS

Sl. No	Factors	Privacy Brooding Metric	Metric Observation
1.	Performance of Agent and Non-Agent	Energy consumption and overall response time $E_{total_{agent}} = \sum_{i=1}^{N} E_{SN\_Agent_i}$ $T_{responsetime_{non-agent}} = T_{tans_{non-agent}} + T_{tans_{MAC}}$	$T_{tans_{non-agent}}$ time consumed to transfer data to the sink
2.	Ad-hoc Networking	Wireless-Network 1. Bandwidth 2. Computation required. Agent $T_I = \frac{D}{B_I}$ Server $T_s = \sum_{i=1}^{n} \sum_{j=1}^{m_i} \frac{C_{ij}\left(D, F'_{\varepsilon ij}, F_{ij}\right)}{\alpha^s S^s} + \frac{rtC_{init}}{\alpha^s S^s}$ Wireless network $T_w = \frac{\sum_{i,j} D, F'_{\varepsilon ij}, F_{ij}}{B_a}$ Communication Overhead $\beta = \frac{B_a}{B}$	Needed capacity in the server and in the network. T_I – Time for transmission across the internet. D – Size of data arriving during time period t.B_I - Bandwidth available in theserver's wired internet connection T_s - Time for processing on server.C_{ij}- Computational complexity of task j on client i.$F'_{\varepsilon ij}$ - Fraction of the total data D processed by task j on client i.F_{ij} - fraction of the data processed by task j on client i,r – Arrival rate of new agents uploaded from the client to the server.t – Time interval.C_{init} - Average no of operations needed for a new agent to start and exist.α^s - Performance efficiency of the software platform on the server.S^s - Performance of the server machine.T_w - Transmission across the wireless network. B_a - Effective bandwidth available for agent messages.B_a - Effective bandwidth available for broad castB – wireless channel.
3.	Privacy Utility Metrics	$U = \sum_{j=1}^{m} w_j X_{ij}$	Value of j decision attribute , w is the psychological weighting
4.	Placeholder Utility	$UF_1 = (ax \pm b$ Or $UF_5 = (ax^2 \pm bx \pm c)$	UF_1 – utility function x – placeholder variable for a value, range a,b& c represent arbitrary, nonnegative constant
5.	Privacy Goal Evaluation	$EVAL(s) = \sum_{i=1}^{n} w_i f_i(s)$	w_i – weight f_i - feature
6.	Adoption Fitness	$fitness = fitness_{t-1} + V_t$	V_t - Feedback value related to time
7.	Calculative and targeted	$f(A_i) = \left\{ 1 - \frac{no.of\ steps\ before\ reproduction}{-1, life\ span\ of\ A_i} \right.$	$f(A_i)$Denotes the function of fitness of an agent.

Table 1 (continued)

Sl. No	Factors	Privacy Brooding Metric	Metric Observation
8.	Big Data Coalition	$C_p = \frac{S_c}{\|c\|}$, $w_i = \frac{P_i}{\sum_{i=1}^{\|c\|} P_i}$, $S_c = \sum_{i=1}^{\|c\|} P_i * w_i$	C_p - Coalition value as the average payoff by the corresponding confidence of agents that participate in the coalition. S_c – Sum of the coalition payoff. w_i - Weight vector of the each agent.
9.	Communication learning	$d(m,n) = \frac{1}{\|m\|+1} \sum_{i=1}^{\|m\|} d(m,n)$If m=n ;	m= message sequences
10.	Process Communication	$comm\_index(X,A_1,A_2 \ldots A_c) = C - \sum_{i=1}^{C} \left(Poss(X,A_i)\right)$	X - Input information granule. $A_1, A_2 \ldots A_c$ – Collection of information granules to the agent. $Poss(X,A_i)$ - Possibility measure of communication.
11.	Intelligence Communication	$IQ \leq \sum IFQ_i$	IFQ_i - Intelligent Factor Quotient of IF
12.	Trust worthiness	$T = 5 * \frac{\sum_{c=1}^{N} Commit_{cr\_c} * Clear_{cr\_c} * Inf_{cr\_c}}{\sum_{c=1}^{N} 5 * Clear_{cr\_c} * Inf_{cr\_c}}$	$Commit_{cr\_c}$ - measures how much of the criterion defined in the service agreement has been fulfilled by the delivered service. $Clear_{cr\_c}$ - Clarity of each criterion. Inf_{cr_c} - Influence of each commitment of the service agreement.
13.	Data Replication and optimization	$nb_i = rounded\left(rm + w_i * \frac{Rm}{W}\right)$	w_i - Agent criticality. W - Sum of domain agents criticality. rm – Minimum no. of replicas. Rm – Maximum no. of replicas.
14.	Data Uncertainty	$C = (1 - AAD^n * \delta) * E(n)$	C= certainty, n= number of agents and δ = maximum allowed conflict, AAD (Average Absolute Deviation

Table 2 Deep Learning based privacy metrics system tested under different scenario

No.of Tags	precision	recall	f1-score	support
01 to 50	0.64	0.33	0.42	3682.44
51 tp 100	0.63	0.33	0.42	835.68
101 t0 150	0.52	0.24	0.31	541.76
151 to 200	0.56	0.28	0.36	429.34
201 to 250	0.51	0.23	0.30	336.60
251 to 300	0.50	0.22	0.29	334.80
301 to 350	0.43	0.17	0.23	239.12
351 to 400	0.48	0.20	0.27	203.72
401 to 450	0.45	0.18	0.24	186.42
451 to 500	0.47	0.21	0.28	174.26
501 50 550	0.55	0.23	0.31	155.76
551 to 600	0.47	0.18	0.25	143.42

3.2.5 Agent developer level for DPLS

$$Agent\ developer\ level = skill\ level + communication\ level + productivity\ level$$
$$Agent\ developer\ level = \left(dev_{sk} + imp_{a} \right) + wk_{adv}(collb + coop) + (f * d)$$

Agent software resource level state the necessary resource required for the development of agent software and it's based on the following parameter such as paradigm level, performance level and replacement level. Paradigm level states the relevance of selected development paradigmdev_{prg}. *paradigm level* $prg_l = \prod dev_{prg}$. Performance level represents the component *comp* and effectiveness *eff*.*performance level* $perf_l = (comp + eff)$. Replacement level parameter states the version of adaptation *adp* when using varies software's. *replacement level* $rep_l = [adp]_{vr}$.

3.2.6 Agent software resource level for DPLS

Agent hardware resource level metric deals with reliability, performance and availability level. Reliability level states the reliable hardware $plaf_a$ required for running an agent. *relaiblity level* $rel_l = \left[plaf_a\right]_0^n$. Figure 3 shows the performance level deals with the various platform used by the software agent$performance\ level = \left[plat\right]_{a=1}^{n}$. Availability level states the available of the various platforms *avil*.*availablity level* $= [avil]_{plat}$

Table 3 Privacy metrics evaluation of cooperative system tested in healthcare system

X	y1	y2	y3	y4
x1	0	1	1	0
x2	1	0	0	0
x3	0	1	0	0

Accuracy : 0.081965

Macro f1 score : 0.0963020140154

Micro f1 score : 0.374270748817

Hamming loss : 0.00041225090909090907

$$Agent\ software\ resource\ level = paradigm\ level + performance\ level + replacement\ level$$

$$Agent\ software\ resource\ level = \prod dev_{prg} + (comp + eff) + \left[adp\right]_{vr}$$

$$Agent\ hardware\ resource\ level = Realibility\ level + Performance\ level + Availability\ level$$

$$Agent\ hardware\ resouce\ level = \left[plaf_{a}\right]_{0}^{n} + \left[plat\right]_{a=1}^{n} + [avil]_{plat}$$

3.2.7 Multi-agent system development life cycle for DPLS

$$Multi-Agent\ System\ development\ life\ cycle = phase\ level + milestone\ level + requirement\ workflow\ level$$

$$Multi-Agent\ System\ development\ life\ cycle = \{str, sz, c\} + \sum_{i=1}^{n} ms_{mas} + \left[req_{mas}\right]$$

3.2.8 Multi-agent system development method level for DPLS

$$Multi-Agent\ System\ development\ method\ level = methodology\ level + paradigm\ level + case\ level$$
$$Multi-Agent\ System\ development\ method\ level = \prod Dmd_{mas} + \prod Dmd_{pard} + tl_{sp}$$

3.2.9 Multi-agent system development management level for DPLS

$$Multi-Agent\ System\ \ development\ management\ level = project\ management\ level + configuration\ management\ level + quality\ management\ level$$

$$Multi-Agent\ System\ \ development\ management\ level = \ \left(dev_{rs} + m_{mas}\right) + \left(\frac{n}{k}\right)p^{k}q^{n-k} + \left[\mathrm{qtec}_{mas}\right]$$

The coordinator specific intra-cluster information system for a health management system is demonstrated in Fig. 3. The virtual coordinators have a limitation with static boundaries for communication. It searches for an appropriate resource for the effective communication in deprived regions.

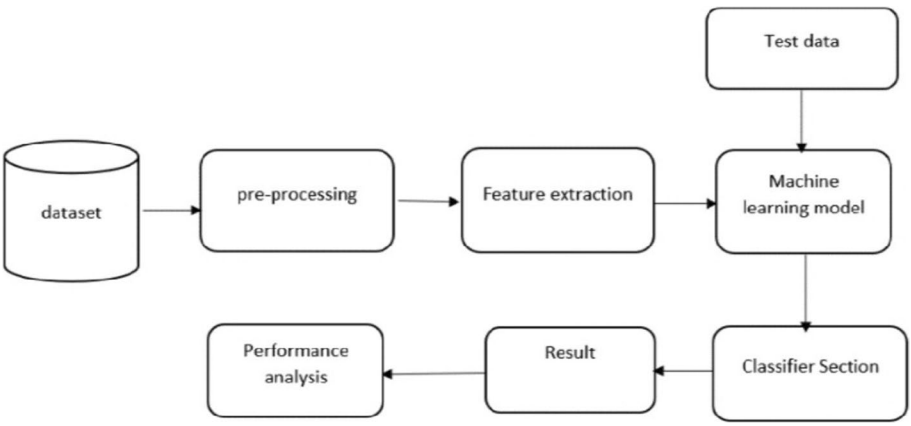

Fig. 3 Classifier and Preprocessor for Intra-cluster Information Updating system

4 Participative node selection process for E-health using PPBOC

4.1 Appropriate resource computing procedure using PPBOC

```
Begin
    P_mon( )
    P_mon, Pstart time, Pendtime, Pdate, Plocation;
    if resource constrain identified then
        do PM= P_s((PBs_i * PS_j)DM);
            then C_p = {PM_i, 1≤ i ≤ m};
    else if eligible devices are filtered and processed until
        Process time={PST_i - PET_i},
        do 1 ≤ i ≤ m;
            }
    HMS= P_s (BS_i) ; //Reading and collecting appropriate information form
Body Sensors (BS)
    }
    if  check HMS= PHc then
        perform P_s = PC(PH_c *PH_s *PH_w );   //medication by physician and
specialist
    else
    Es= Normal;
    }
    End P_mon;
End;

HCM (Patient EM_i, int Process time)
{
    E_starttime = Ø;
    While (HC ≤ Normal ) do
    {
    For j= 1; to Ps
    {
    E_L = BS_i (sensor data);// Health Log
    Switch (HS_i = (HC ≤ (C * E ) )) do
        Case: Critical
            GL_i = E_location;// Patient location
            EH_i = PC_j;
            Return;
        Case: Serious
            EP_i = P_j; // Indicate patient to concern a physician;
            EP_i = HEP_j; // Healthcare supporting with an  expert physician;
            Break;
        Case: Warning
            EP_i= M_j; //Send appropriate emergency care medication to  patient
            Break;
        Default ; PH= normal;
    if ( E_wait time ≥ 0) Repeat: procedure HCM( );
End HCM;

do
{
B_{h+1}← Ø;
            For each g Ɛ B_h
            {
            For each (side node g' of g in FS)
            {
            if (d (g) + W ≤ Vmax. Δt_j) then
                        {
                         B_{h+1} = B_{h+1}∪ {g'}; d (g') ← d (g) + w;
                        FS← FS-g';
                        }
            }
            For each (diagonal node g'' of g in FS)
            {
            if (d (g) + √2w ≤ Vmax. Δtj) then,
                        {
                        B_{h+1}= B_{h+1}∪ {g''}; d (g'') = d (g) + √2w;
                        FS= FS-g'';
                        }
            }
            }
R_j^l←R_j^l∪ B_{h+1}; h← h+1;
} while (B_h≠ 0)
```

```
Update the cluster head with the neighbor set available nodes
do
For each node j holding the data do
            do for each node i= Nj do

                        if i=d then,
                        Send (B, i, 1) return
                        End if;
            End for
            if Qj>1 ∃i Ɛ Nj, (s.t |Hi-Hd | ≤ L Λ I;
            If active (if opp node became deactivate /removed from the
operation)
            go to step1: return (1); else
            Send (B, I, (Qj/2))
            Qj ← (Qj /2);
            End if;
    End for; While (Repeat until the data expires)
```

5 Experimental setup and result analysis

The proposed coordinator specific optimized healthcare monitoring (CSOHM) system whistle ahead of many challenges in patient health monitoring. However, handling a critical and emergency scenarios are more complicated issues in the contemporary healthcare management process. The wireless body sensors system and its technology integrate with smart devices to compete right through un-anticipating cases by handling issues in a collaborative resource sharing mechanism. This system efficiency plotted in Fig. 4 is adopted from the natural behavior of bee, to fame a coordinator specific artificial bee colony approach for resource identification and sharing among the network framed during health emergency cases.

Figure 5a, b Critical scenarios, Fig. 5c, d Clustering multi-agent, Fig. 5e, f Deep-learning approach for prediction, Fig. 5g, h Cost effective performance illustration. In recent years, e-health care has become a significant part of the healthcare industry. The growing adoption of e-health systems has brought significant benefits such as easy accessibility, cost-effectiveness, and improved quality of care. However, these systems pose significant privacy risks to patients' sensitive information. This has led to an increased need for privacy-preserving techniques that can protect patients' sensitive information from unauthorized access. One such technique is the use of multi-agent based privacy metrics in deep learning systems.

The existing research on multi-agent based privacy metrics for e-health care deep learning systems. The experimentation result analysis reviewed with various proposed approaches for modeling the interactions between the different agents in the e-health care system and evaluating the privacy of the system. Overall, multi-agent based privacy metrics can provide a comprehensive evaluation of the privacy of e-health care deep learning systems, taking into account the privacy preferences of the different stakeholders in the healthcare ecosystem. However, the validation of the proposed approach to evaluate their effectiveness in real-world scenarios is comparatively high.

E-health care is a rapidly growing area of research, where deep learning algorithms have been widely applied for the prediction, diagnosis, and treatment of various medical conditions. However, with the increasing use of e-health care systems, there is a growing concern over the privacy and security of patient information. Multi-agent based privacy metrics have been proposed to evaluate the privacy of e-health care deep learning systems. In this literature survey, we review the existing research on this topic. Multi-agent systems (MAS) are a type of artificial intelligence that consists of multiple agents that interact with each other to achieve a common goal. In the context of e-health care, MAS can be used to model the interactions

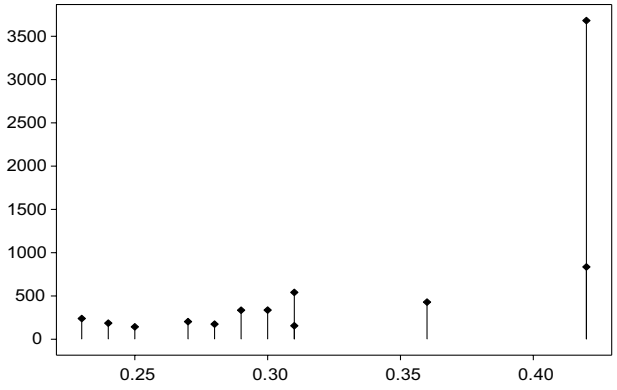

Fig. 4 Privacy breach classification identifier using Deep learning model

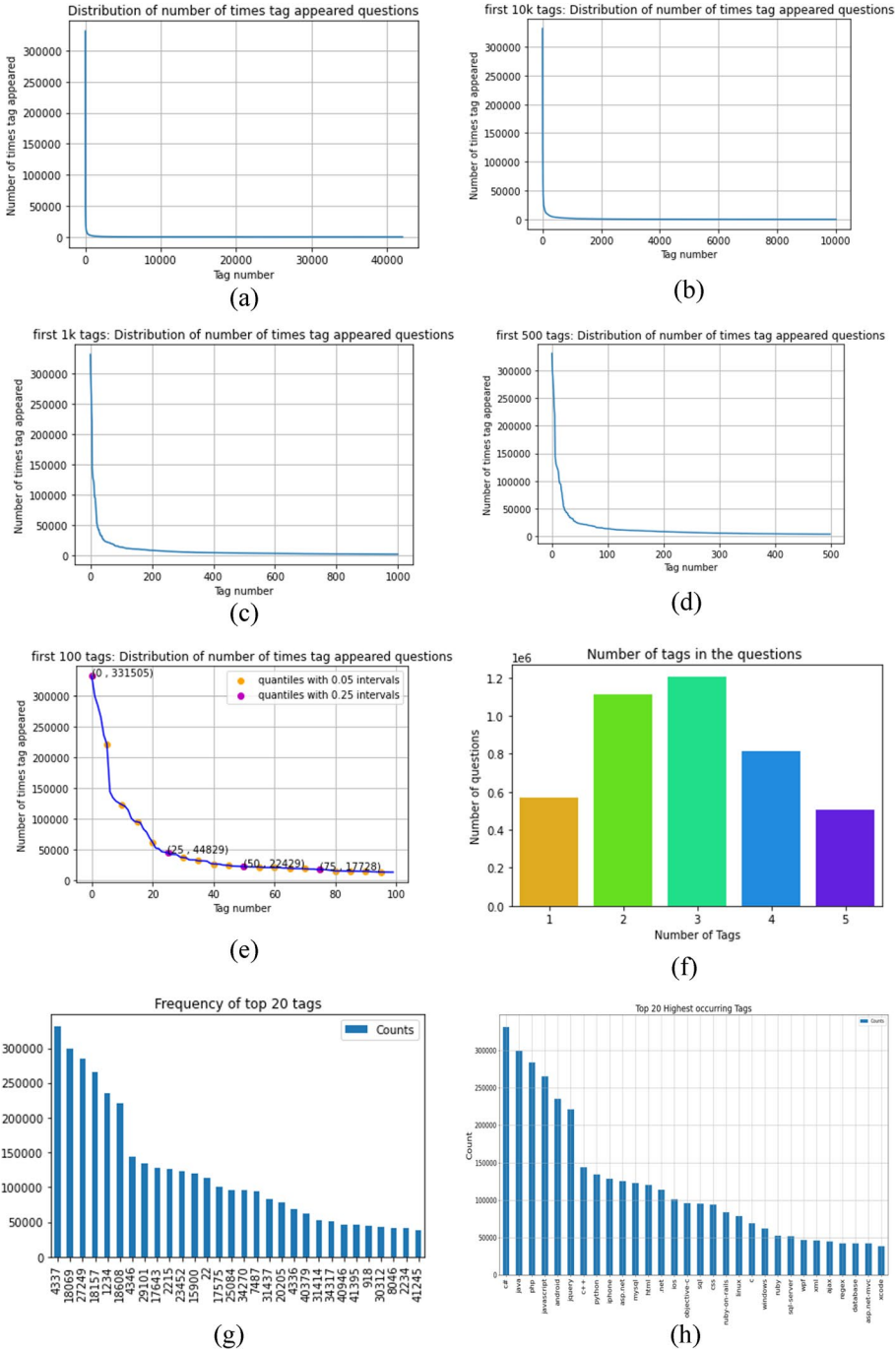

Fig. 5 **a**, **b** Critical scenarios **c**, **d**. Clustering multi-agent **e**, **f**. Deep-learning approach for prediction **g**, **h**. Cost effective performance illustration

between healthcare providers, patients, and other stakeholders in the healthcare ecosystem. Deep learning is a subset of machine learning that uses artificial neural networks to learn from large datasets. Deep learning algorithms have been shown to be effective in a wide range of medical applications, including image analysis, disease diagnosis, and drug discovery. Privacy is a critical concern in e-health care systems, as patient information is often sensitive and confidential. Privacy metrics are used to evaluate the privacy of e-health care systems and ensure that patient information is not compromised. Multi-agent based privacy metrics have been proposed to evaluate the privacy of e-health care deep learning systems.

There are several privacy metrics that can be used to evaluate the privacy of e-health care systems. One common approach is to use information theoretic metrics, such as entropy and mutual information, to quantify the amount of information leakage in a system. The multi-agent based privacy metrics for e-healthcare deep learning system approach provides a robust and secure system for e-healthcare applications while improving the accuracy of diagnoses and treatment plans. This approach has significant potential to revolutionize the e-healthcare industry by ensuring that patients' sensitive data is kept secure while still benefiting from the advances in deep learning technology.

6 Conclusion

Multi-agent based privacy metrics involve the use of multiple agents to evaluate the privacy level of a deep learning system. These agents analyze various aspects of the system, such as the data inputs, the algorithms used, and the output generated. The agents then generate a privacy score for the system based on their analysis. This score can be used to identify the privacy risks associated with the system and to implement appropriate measures to mitigate them. The use of multi-agent based privacy metrics in e-health care deep learning systems has several benefits. Firstly, it allows for a more comprehensive evaluation of the system's privacy level. This is because the different agents can analyze different aspects of the system, providing a more detailed assessment. Secondly, it enables the identification of specific privacy risks associated with the system. This information can then be used to implement targeted measures to mitigate these risks. Finally, it ensures that the system complies with relevant privacy regulations and standards. The use of multi-agent based privacy metrics is an effective technique for enhancing the privacy of e-health care deep learning systems. It provides a comprehensive and targeted approach to privacy evaluation, allowing for the identification and mitigation of specific privacy risks. As e-health systems continue to grow in popularity, the adoption of such privacy-preserving techniques will become increasingly important to protect patients' sensitive information.

Authors' contributions This article focuses on electronic health monitoring on the patient medical data preserving and prediction using opportunistic computing based deep learning system. It could be addressed various deep learning and Multi-agent based design level metrics.

Funding This Research Received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Data availability The data will be provided based on data request by the evaluation team.

Declarations

Ethical approval and consent to participate Not applicable

Consent for publication All the authors of this paper have shown their Participation voluntarily.

Competing interests The authors of this research article declares that no conflict of interest in preparing this research article.

References

1. Alam GR, Shirajum, M, Uddin Z (2018) "Edge-of-things computing framework for cost-effective provisioning of healthcare data", J Parallel Distrib Comput,pp.1-20
2. Alcaraz, J.J.; Lopez-Martinez, M.; Vales-Alonso, J.; Garcia-Haro, J., "Bandwidth Reservation as a Coexistence Strategy in Opportunistic Spectrum Access Environments," Selected Areas Commun IEEE J , vol.32, no.3, pp.478,488, March 2014.
3. Alguliyev RM, Aliguliyev RM, Abdullayeva FJ (n.d.) "Privacy-preserving deep learning algorithm for big personal data analysis", J Indust Inf Integration,https://doi.org/10.1016/j.jii.2019.07.002
4. Ashok Kumar S, Chandramohan D (2018) "Fault Test Analysis in Transmission Lines Throughout Interfering Synchrophasor Signals", Elsevier- ICT Express. https://doi.org/10.1016/j.icte.2018.03.003
5. Benharref A, Serhani MA (2014) Novel Cloud and SOA-Based Framework for E-Health Monitoring Using Wireless Biosensors. IEEE J Biomed Health Inf 18(1):46–55
6. Bewong M, Liu J, Liu L, Li J (2019) Privacy preserving serial publication of transactional data. Inf Syst 82:53–70
7. Boussada R, Hamdane B, Elhdhili ME, Leila Azouz Saidane (2019) Privacy-preserving aware data transmission for IoT-based E-health, Comput Netw, https://doi.org/10.1016/j.comnet.2019.106866
8. Chamikara MAP, Bertok P, Liu D, Camtepe S, Khalil I (2019) An EfÞcient and Scalable Privacy Preserving Algorithm for Big Data and Data Streams, Comput Secur, https://doi.org/10.1016/j.cose.2019.101570
9. Chandramohan D, Vengattaraman T, Dhavachelvan P, Baskaran R, Venkatachalapathy VSK (2014) Fewss- Framework to Evaluate the Service Suitability and Privacy in a Distributed Web service Environment. Int J Model Simul Sci Comput (World Scientific) 5(1):1350016. https://doi.org/10.1142/S1793962313500165 pp.1-37. ISSN: 1793-9615
10. Chandramohan D, Sathian D, Rajaguru D, Vengattaraman T, Dhavachelvan P (2015) A Multi-Agent Approach: To Preserve User Information Privacy for a Pervasive & Ubiquitous Environment. Egypt Inf J (Elsevier) 16:151–166. https://doi.org/10.1016/j.eij.2015.02.002. ISSN: 1110-8665
11. Chandramohan D, Rajaguru D, Vengattaram T, Dhavachelvan P (2018) "A Coordinator-specific privacy-preserving model for e-health monitoring using artificial bee colony approach", John Wiley: Security and Privacy. https://doi.org/10.1002/spy2.32
12. Chen K, Franko K, Sang R (n.d.) "Structured Model Pruning of Convolutional Networks on Tensor Processing Units", Mach Learn, https://doi.org/10.48550/arXiv.2107.04191
13. Clementi A, Pasquale F, Silvestri R (2013) Opportunistic MANETs: Mobility Can Make Up for Low Transmission Power. IEEE/ACM Trans Netw 21(2):610–620
14. D'Agostino D, Morganti L, Corni E, Cesini D, Merelli I (2018) "Combining edge and cloud computing for low-power, cost-effective metagenomics analysis", Futur Gener Comput Syst, https://doi.org/10.1016/j.future.2018.07.036
15. Deng Zhiliang,Ying Zhang, Xiaorui Zhang, Lingling Li,"Privacy-preserving quantum multi-party computation based on circular structure", J Inf Secur Appl47 (2019), pp.120–124.
16. Dhasarathan, C., Kumar, M., Srivastava, A.K. et al. (2021) A bio-inspired privacy-preserving framework for healthcare systems. J Supercomput. https://doi.org/10.1007/s11227-021-03720-9
17. Dhasarathan C, Hasan MK, Islam S, Abdullah S, Mokhtar UA, Javed AR, Goundar S (2023) COVID-19 health data analysis and personal data preserving: A homomorphic privacy enforcement approach. Comput Commun 199:87–97, ISSN 0140-3664. https://doi.org/10.1016/j.comcom.2022.12.004
18. Ding Xiaofeng,Wanlu Yang, Kim-Kwang Raymond Choo, Xiaoli Wang, Hai Jin,"Privacy preserving similarity joins using MapReduce", Inf Sci493 (2019), pp.20–33.
19. Groba C, Clarke S (2014) Opportunistic Service Composition in Dynamic Ad Hoc Environments. Service Comput IEEE Trans 7(4):642–653
20. Guo S, Xiang T, Li X (2019) Towards efficient privacy-preserving face recognition in the cloud. Signal Process 164:320–328. https://doi.org/10.1016/j.sigpro.2019.06.024
21. Gupta P, Agarwal Y, Dolecek L, Dutt N, Gupta RK, Kumar R, Mitra S, Nicolau A, Rosing TS, Srivastava MB, Swanson S, Sylvester D (2013) Underdesigned and Opportunistic Computing in Presence of Hardware Variability. Comput-Aid Des Integrate Circ Syst IEEE Trans 32(1):8–23

22. Hackmann G, WeijunGuo GY, Sun Z, Lu C, Dyke S (2010) Cyber-physical codesign of distributed structural health monitoring with wireless sensor networks. In: Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS '10). Association for Computing Machinery, New York, pp 119–128. https://doi.org/10.1145/1795194.1795211
23. Kang Q, He H (2013) Honeybee mating optimization algorithm for task assignment in heterogeneous computing systems. Intell Autom Soft Comput 19(1):69–84. https://doi.org/10.1080/10798587.2013.771438
24. Kaur H, Khanna P (2019) Privacy preserving remote multi-server biometric authentication using cancelable biometrics and secret sharing, Futur Gener Comput Syst, https://doi.org/10.1016/j.future.2019.07.023
25. Li S, Nankun M, Le J, Liao X (2019) Privacy Preserving Frequent Itemset Mining: Maximizing Data Utility Based On Database Reconstruction, Comput Secur ,https://doi.org/10.1016/j.cose.2019.03.008
26. Li Y, Wang Y, Li D (2019) "Privacy-preserving lightweight face recognition, Neurocomputing" ,https://doi.org/10.1016/j.neucom.2019.07.039
27. Li D, Dong X, Cao Z, Wang H (2019) Privacy-preserving outsourced image feature extraction. J Inf Secur Appl 47:59–64
28. Long H, Miao Y, Gaoxiang W (2018) "An intelligent robot factory based on cognitive manufacturing and edge computing", Futur Gener Comput Syst, https://doi.org/10.1016/j.future.2018.08.006
29. Lopes F, Delicato FC, Batista T, Cavalcante E, Pereira T, Pires PF, Ferreira P, Mendes R (2014) OpenCOPI: middleware integration for Ubiquitous Computing. Taylor Francis-Int J Parallel, Emerg Distribut Syst 29 Issue.2:178–212
30. Ma Z, Ma J, Miao Y, Liu X (2019) Privacy-preserving and high-accurate outsourced disease predictor on random forest. Inf Sci 496:225–241
31. Mehta NB, Talak R, Suresh AT (2013) Interplay Between Optimal Selection Scheme, Selection Criterion, and Discrete Rate Adaptation in Opportunistic Wireless Systems. Commun IEEE Trans 61(7):2735–2745
32. Nobre J,Allan M (2018) "Vehicular Software-Defined Networking and Fog Computing: Integration and Design Principles", Ad Hoc Networks-Elsevier, pp.1-30
33. Puri V, Sachdeva S, Kaur P (2019) Privacy preserving publication of relational and transaction data:Survey on the anonymization of patient data. Comput Sci Rev 32:45–61
34. Rahman MS, Khalil I, Alabdulatif A, Yi X (2019) Privacy preserving service selection using fully homomorphic encryption scheme on untrusted cloud service platform. Knowl-Based Syst 180:104–115
35. Rashidibajgan S, Doss R (2019) Privacy-Preserving history-based routing in Opportunistic Networks. Comput Secur 84:244–255
36. Sajjad H, Kanwal T, Anjum A, Malik SR, Khan A, Khan A, Manzoor U (2019) An efficient privacy preserving protocol for dynamic continuous data collection. Comput Secur 86:358–371
37. Shen H, Bai G, Yujia H, Wang T (2019) "P2TA: Privacy-Preserving Task Allocation for Edge Computing Enhanced Mobile Crowdsensing, J Syst Archit .https://doi.org/10.1016/j.sysarc.2019.01.005
38. Singh, C.; Sarkar, S.; Aram, A.; Kumar, A., "Cooperative Profit Sharing in Coalition-Based Resource Allocation in Wireless Networks," Netw IEEE/ACM Trans , vol.20, no.1, pp.69,83, Feb. 2012
39. Uchiyama Akira, SaeFujii, Kumiko Maeda, TakaakiUmedu, Hirozumi Yamaguchi and Teruo Higashino "UPL: Opportunistic Localization in Urban Districts", IEEE Trans Mob Comput, VOL. 12, NO. 5, pp.1009-1022, MAY 2013.
40. Verba N, Chao K-M, Lewandowski J (2018) "Modelling industry 4.0 based fog computing environments for application analysis and deployment", Futur Gener Comput Syst, pp.1-31
41. Wall Josh, John K. Ward and Luis Castro, "Large-Scale Opportunistic Sensing", Pervasive Comput IEEE , vol.10, no.4, pp.54,58, April 2011.
42. Wang S, Liu M, Cheng X, Li Z, Huang J, Chen B (2013) Opportunistic Routing in Intermittently Connected Mobile P2P Networks. IEEE J Select Areas Communications/Supplement 31(9):369–379
43. Wang Guoming,Rongxing Lu, Cheng Huang, Yong Liang Guan," An efficient and privacy-Preserving pre-clinical guide scheme for mobile eHealthcare", J Inf Secur Appl Vol.46 (2019),pp.271–280.
44. Xiao M, Wu J, Huang L (2014) Community-Aware Opportunistic Routing in Mobile Social Networks. Comput IEEE Trans 63(7):1682–1695
45. Yang T, Ma J, Miao Y, Liu X, Wang X, Meng Q (2019) "PLCOM: Privacy-Preserving Outsourcing Computation of Legendre Circularly Orthogonal Moment over Encrypted Image Data", Inf Sci, https://doi.org/10.1016/j.ins.2019.07.078.
46. Yargic A, Bilge A (2019) Privacy-preserving multi-criteria collaborative filtering. Inf Process Manag 56:994–1009
47. Zehua Wang, Yuanzhu Chen, Cheng Li, "A New Loop-Free Proactive Source Routing Scheme for Opportunistic Data Forwarding in Wireless Networks," Commun Lett, IEEE , vol.15, no.11, pp.1184,1186, November 2011.

48. Zhang Q, Wang G, Liu Q (2019) Enabling Cooperative Privacy-preserving Personalized search in cloud environments. Inf Sci 480:1–13
49. Zheng X, Chen A, Luo G, Tian L, Cai Z (2019) Privacy-preserved distinct content collection in human-assisted ubiquitous computing systems. Inf Sci 493:91–104
50. Zhong H, Han S, Cui J, Zhang J, Xu Y (2018) "Privacy Preserving Authentication Scheme with Full Aggregation in VANET", Inf Sci. https://doi.org/10.1016/j.ins.2018.10.021
51. Zhou Y, Long X, Chen L, Yang Z (2019) Conditional privacy-preserving authentication and key agreement scheme for roaming services in VANETs. J Inf Secur Appl 47:295–301

Authors and Affiliations

Chandramohan Dhasarathan[1] · M. Shanmugam[2] · Manish Kumar[1] · Diwakar Tripathi[3] · Shailesh Khapre[4] · Achyut Shankar[5,6,7]

Chandramohan Dhasarathan
pdchandramohan@gmail.com

M. Shanmugam
shaninfo247@gmail.com

Manish Kumar
mk9309@gmail.com

Diwakar Tripathi
diwakarnitgoa@gmail.com

Shailesh Khapre
shailesh@iiitnr.edu.in

1 Computer Science and Engineering Department, Thapar Institute of Engineering and Technology, Patiala, Punjab, India

2 Department of Computer Science, School of Engineering and Technology, Pondicherry University, Puducherry, India

3 Computer Science and Engineering Department, Indian Institute of Information Technology, Sonepat, Hariyana, India

4 Department of Data Science & Artificial Intelligence, Dr. S. P. Mukherjee IIIT, Naya Raipur, Chhattisgarh, India

5 WMG, University of Warwick, Coventry, UK

6 Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, 248002, India

7 School of Computer Science Engineering, Lovely Professional University, Phagwara - 144411, Punjab, India