# PCCA: Position Confidentiality Conserving Algorithm for Content-Protection in e-Governance Services and Applications

Darshan Vishwasrao Medhane and Arun Kumar Sangaiah

***Abstract*—E-Governance or electronic governance is a procedure of public sector regulation and is a significant step in the transformation of municipal administration, with the intention of confiding and smoothing collaboration among the population and civic establishments through Information and Communications Technology-based applications. Content Confidentiality has become a serious anxiety for modern Information Societies. The sensitive nature of much of the private personal data that are exchanged or released to untrusted parties necessitates that liable administrations should embark on suitable content confidentiality protection mechanisms. Nowadays, many of these data are texts (e.g., emails, messages posted in social media, healthcare outcomes, etc.) that, because of their unstructured and semantic nature, constitutes a challenge for automatic data protection methods. In this paper, we present a solution for position confidentiality conserving content protection in e-Governance services through computational intelligence. We propose PCCA, a novel position confidentiality conserving algorithm for content protection in e-Governance. The proposed algorithm applies computational intelligence in e-Governance for content protection by means of rule-based approach from computational intelligence and users current position information. A simulation model has been implemented on a desktop PC and evaluation using roaming users real-time position-based information demonstrates that PCCA can efficiently conserve roaming users position confidentiality while accomplishing better performance, guaranteed position confidentiality, and better quality of service in e-Governance.**

***Index Terms*—Position confidentiality, content protection, computational intelligence, wireless search space area, e-Governance, quality of service.**

## I. Introduction

NOWADAYS, Information and Communications Technology (ICT) have cemented the method for universal scale content sharing in e-Governance. Fundamentally, e-Governance or electronic governance is the application of ICT to the various procedures of Government functioning so as to achieve smart governance. In general, e-Governance incorporates the use of ICTs by government organizations for: (a) give-and-take of information with people, industries or several government sectors, (b) user confidentiality conserved, faster and effective provision of municipal facilities, (c) refining the internal effectiveness and productivity, and (d) improving quality of services. Government releases and transmits large volumes of electronic contents on day-to-day basis. But, these contents indicate private features of people (e.g., individuals inclinations, identities, ideas, current positions, etc.), hence triggering a severe content confidentiality risk. In order to avoid this risk, suitable content protection measures should be commenced by the authorities so as to accomplish with existing rules and regulations on content confidentiality. Besides, users position plays a vital role in a rapid growth of ICT applications causing the development of emerging e-Governance services and applications. With the fusion of position-based services and e-Governance; conserving users position confidentiality is one of the most substantial objectives. To achieve this objective, we offer a confidentiality conserving position-based query handling framework for content-protecting in e-Governance. We identify several users of typical e-Governance services and applications which are, Citizens, Enterprises, Businesses and Government. On the basis of users, e-Governances applications are categorized into four wide groups: Government to Citizens (G-C), Government to Enterprises (G-E), Government to Businesses (G-B) and Government to Government (G-G).

It is important to use the aforementioned types of e-Governance services and applications through a secure mechanism. Hence, to achieve a users position confidentiality in e-Governance; we propose a Position Confidentiality Conserving Algorithm (PCCA) in this paper. Data corruption instances specify that even the most prevailing service providers are not completely trustworthy [1]–[3]. This articulates content protection concerns of users. Researchers and practitioners have come up with numerous solutions such as GCA [4], D-TC [5], AVD-DCA [6], DSDCA [7] and V-DCA [8] for effective position-based query and content protection.

In this paper, we present confidentiality conserving position-based query handling framework for content-protecting in e-Governance. The proposed framework can protect user confidentiality, however, simultaneously attaining extraordinary content protection in e-Governance. The proposed methodology is cluster-based where, roaming users in wireless search space areas are prearranged into clusters with assorted interests, to facilitate each user's personal interests. The individual users personal interests may be concealed amongst a group of

Manuscript received July 4, 2017; revised October 8, 2017 and September 11, 2017; accepted October 26, 2017. Date of current version May 23, 2018. *(Corresponding author: Arun Kumar Sangaiah.)*

The authors are with the School of Computing Science and Engineering, VIT University, Vellore 632014, India (e-mail: darshan.medhane@gmail.com; arunkumarsangaiah@gmail.com).

Digital Object Identifier 10.1109/TETCI.2017.2769110

roaming users against position server. A number of users are gathered in respective user clusters, individual user signifies a distinctive personal interest, and the unification of all users conceals all personal interests of an individual user cluster. The roaming users interconnect with the position server in support of the e-Governance service users. The e-Governance users can then procure customized endorsements on the basis of the position server's endorsements to the roaming users and their individual interest circulation amongst roaming users, without revealing any confidential data to the e-Governance access server. We propose a four-stage procedure for in-cluster calculations, which guarantee and confirm users position confidentiality from existing authorized members of the respective cluster in the process of content protection in e-Governance with great proficiency. To the best of our knowledge, this is the first comprehensive work that challenges the problem of confidentiality conserving position-based query handling in e-Governance services and applications through computational intelligence.

### A. *Research Objectives and Challenges*

Our research objectives are as follows:

1) To study Confidentiality Conserving Position Monitoring System (C2PMS) in wireless networks.
2) To achieve Source Node Position Confidentiality (SNPC) in wireless networks by means of two emerging trends in research studies namely: (a) Quantum Computational Theory and (b) Evolutionary Multi-Objective Optimization (EMO).
3) Effective use of computational intelligence for attaining Source Node Position Confidentiality.
4) To propose novel computational intelligence inspired strategy for achieving Source Node Position Confidentiality.
5) To map proposed computational intelligence inspired SNPC algorithm & strategy to EMO theory.
6) To introduce search space based evolutionary multi-objective algorithm for attaining Source Node Position Confidentiality.
7) To make use of proposed methodology for: (a) monotonous estimation of continuous position-based queries, (b) managing wide-ranging variety of continuous position-based queries, (c) handling huge incoming position-based queries data, and (d) large numbers of contemporary continuous position-based queries.
8) To analyze the performance of proposed strategy for achieving Source Node Position Confidentiality in wireless networks.

In our earlier works, we have suggested the confidentiality conserving position monitoring system architecture [9], [10] and offered novel algorithms using quantum-inspired computing theory [11]; evolutionary multiobjective optimization theory [12]; parallel computation theory [13]; and opacity and machine learning-based approach [38] (see Fig. 1).

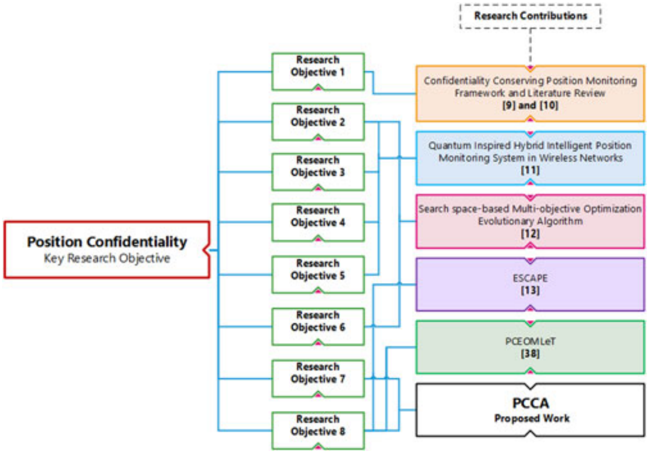
Research Contributions
Confidentiality Conserving Position Monitoring Framework and Literature Review [9] and [10]
Quantum Inspired Hybrid Intelligent Position Monitoring System in Wireless Networks [11]
Search space-based Multi-objective Optimization Evolutionary Algorithm [12]
ESCAPE [13]
PCEOMLeT [38]
PCCA Proposed Work
Position Confidentiality Key Research Objective
Research Objective 1
Research Objective 2
Research Objective 3
Research Objective 4
Research Objective 5
Research Objective 6
Research Objective 7
Research Objective 8

Fig. 1. Research objectives and novel research contributions.

All of these works converge on the aforementioned eight objectives. In continuation of these works, this time our focus is on conserving confidentiality of roaming users in e-Governance services. The position monitoring system has its particular features; a tradeoff occurs amongst position confidentiality conservation on the basis of effectiveness and quality in position monitoring services. Extracting possible fundamental features in the existing e-Governance services to protect the roaming users position confidentiality while offering superior e-Governance services will be a substantial challenge.

### B. *Research Contributions*

Compared with our previous works specifically, a quantum-inspired hybrid intelligent position monitoring system in wireless networks [11], a search space based multi-objective optimization evolutionary algorithm [12] and ESCAPE [13]; this work expands efficiency in the confidentiality conservation of position-based queries and offers a framework to rigorously safeguard user confidentiality in roaming users cluster formation and content protection in e-Governance. Our significant contributions in this paper are as follows:

1) We propose a confidentiality conserving position-based query handling framework for cluster-based roaming users of e-Governance services and applications, which can proficiently protect individual user's content confidentiality in the content retrieval process.
2) We offer four-stage secure procedure to accomplish competent confidentiality conserving operations in different circumstances of e-Governance services. The proposed procedure can be adopted by various e-Governance applications to accomplish effective position confidentiality conserving computation.
3) We suggest a novel solution to conserve roaming users position confidentiality and content protection in e-Governance services. E-Governance server is banned from getting authorized roaming users position information, whereas position anonymization server cannot get authorized roaming users content information in our proposed methodology. Additionally, roaming users position information cannot be retrieved by people who does not match their authorized e-Governance system access control.

4) We propose a Position Confidentiality Conserving Algorithm (PCCA) for content-protecting in e-Governance services and applications.
5) We focus on position confidentiality conservation of roaming users in e-Governance services; when roaming users make continuous queries and therefore propose position confidentiality conserved content retrieval by roaming users in wireless search space cloaked region.
6) We develop a simulation model to evaluate PCCA on a desktop PC using real-time position information.

### C. Organization of the Paper

The rest of this paper is organized as follows: Section II briefs related work. Section III introduces the system archetype, detailed problem definition, simple e-Governance service framework for position-based query handling and the proposed framework along with the position confidentiality model. Section IV explains the proposed algorithm (PCCA) in detail. Section V describes the detailed mathematical model. Section VI represents the complexity analysis of the proposed methodology. Section VII presents a performance evaluation, a simulation setup and performance metrics used. Limitations of the proposed work and future research directions are presented in Section VIII. Finally, Section IX concludes the paper.

## II. Related Work

In recent years, position-based services have been progressively incorporated into daily life and have subsequently conveyed people better convenience. To utilize position-based services, roaming users must send their service provider correct position information so as to accomplish the position-based query request. Generally, the position service providers server is incredible, and the position information of the roaming user is susceptible to theft [14]. Subsequently stealing the position information of a roaming user, the intruder, by means of position tracking or links to supplementary public information for an instance geographical database may be able to authorize the roaming users identity and achieve an improvement in extra confidential information [15]–[18]. Several techniques have been introduced recently to guarantee the confidentiality protection of roaming users. These techniques can be divided into two groups: false position [19]–[21] and spatial regions [22]–[24]. The model *k-*, earliest offered in the literature [25]–[27], denotes the anonymous position occurring when the position data of at least one other individual and the position information of *k-1* cannot be distinguished [14]. As a result, the individuals position to meet the position of k- turn out to be anonymous. The techniques discussed in [28], [29] makes use of a false position technique. In this paper, the proposed methodology is compared with existing position confidentiality conserving baseline techniques such as GCA [4], D-TC [5], AVD-DCA [6], DSDCA [7] and V-DCA [8]. Our aim is to build a system archetype that satisfies the criteria of users position confidentiality in the wireless search space area and allows users to query for e-Governance data on the basis of their current positions, while conserving their position confidentiality. In general, we want to support: 1) point query to query for e-Governance data allied with a specific position, 2) wireless search space area range query to query for e-Governance data allied with all positions in a specific range nearby the roaming user, and 3) adjacent neighbor query to query for e-Governance data allied with positions adjacent to a specified position.

### A. Computational Intelligence

The conventional definition of the term computational intelligence (CI) does not exist even though it is used in different circumstances [30]. CI is defined as a discipline of artificial intelligence comprised of computer systems that makes use of numeric data, recognize patterns, display computational adaptability and fault tolerance, and commit errors at a rate approximating human performance [31]. As per the directives from the IEEE Computational Intelligence Society, the conception of CI includes different topics of artificial intelligence covering the sub-areas of evolutionary multi-objective optimization, fuzzy inference systems, artificial neural networks and genetic algorithms. The proposed work can be explored with the concept of fuzzy logic for the users uncertain behavior and position-based decision making.

*1) Fuzzy Logic:* The fuzzy set theory was presented by Zadeh in 1965 as an extension of multi-valued logic. It has been termed as a specific logic of fuzziness and approximate reasoning. The shape of the membership function defines the fuzzy set and is dependent on the purpose of set [32], [33]. As far as the proposed work is concerned, we used fuzzy logic as a problem solving control system approach. Fuzzy logic offers a modest way of solving position-related queries containing ambiguous, vague, and imprecise input information [11]. Furthermore, instead of applying a mathematical model to a particular system, fuzzy logic integrates a rule-based IF A AND B THEN C approach to solve position-based queries [11]. So, in the proposed framework, we integrate a rule-based approach to solve users position-based queries in real time and to offer content protection in e-Governance. The position-based query forwarding and answering for content protection in e-Governance is implemented by means of the concept of a fuzzy inference system. We are using fuzzy logic as it is able to support real-time decisions about the context data of source nodes in wireless networks when such data has some degree of fuzziness and ambiguity. Consequently, conventional logic may lead to absolutely erroneous results owing to the ambiguity within context data. Fuzzy logic is a viable alternative to reasoning and making rational decisions with imprecision, uncertainty, incompleteness of information, conflicting information, partiality of truth and degrees of probability [33]–[37].

## III. System Archetype and Preliminaries

In this section, we first articulate our problem and then present the design of the proposed methodology.

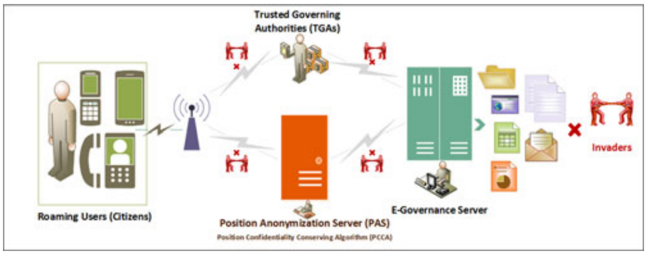
Trusted Governing
Authorities (TGAs)
Invaders
Roaming Users (Citizens)
Position Anonymization Server (PAS)
Position Confidentiality Conserving Algorithm (PCCA)
E-Governance Server

Fig. 2. Simple e-Governance service framework for position-based query handling.

### A. *Problem Definition*

In an e-Governance services, individuals may post, read or comment on online posts, like pictures, videos, music and articles published by government authorities or organizations by means of mobile devices or desktop PC. Initially, we need some assumptions about the invaders contextual facts. In view of this, the invader should know the position confidentiality conservation algorithm in advance and can acquire the number of e-Governance services in individual wireless search space range area. The problem definition is as follows: Suppose there is a request for position-based e-Governance service from a roaming userthe confidentiality of his or her position (k, Position, PositionMax). Then the position of the anonymous server must dictate how the roaming user discovers a concealed content set C and make the C specific position conceals user as well as to meet Position $\leq$ C . Position $\leq$ PositionMax, Ck $\geq$ k. Moreover, the invader cannot assume a precise position P from C with high probability. How do we infer the roaming users exact position after thieving the concealed content sets C? Usually, the invader consecutively assumes that the user is positioned in this concealed content set C for individual content set $C_i$ (i = 1, 2 L) of C. Then the invader will accomplish a position confidentiality conservation algorithm on the content set C and obtain a concealed section set C'. It compares C with C in order to reach the number of the identical contents of those two sets C and C; and the ratio of all contents of the C. In conclusion, the invader infers the possibility of U belonging to the content set $C_i$.

### B. *Simple e-Governance Service Framework for Position-Based Query Handling*

Fig. 2 shows the simple e-Governance service framework for position-based query handling. There are four building blocks involved in the system model: the roaming user (citizen), the e-Governance server, the position anonymization server (PAS) and the trusted governing authorities (TGAs). The roaming user (citizen) holds huge extent of confidential content that will be outsourced into the e-Governance server. The server situated at e-Governance service site offers huge storage space for the roaming users (citizens), which is controlled by e-Governance server all the way through PAS. The PAS, which has substantial communication and computation ability, is deputized by the roaming users (citizens) and TGAs to check the content tenure of the e-Governance server. The TGA is trusted by both the e-Governance server and roaming users (citizens) which can be a civic organization or a non-government private association.

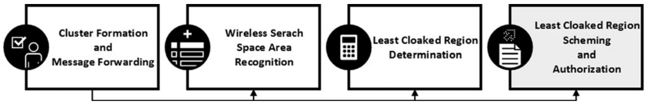

Fig. 3. Stages of proposed framework.

### IV *Proposed Framework and Position Confidentiality Model*

The proposed framework is a four-stage technique (see Fig. 3) for confidentiality conserving query handling in e-Governance services and applications.

Stage 1: Cluster formation and message forwarding
Stage 2: Wireless search space area recognition
Stage 3: Least cloaked region determination
Stage 4: Least cloaked region scheming and authorization

*Stage 1: Cluster formation and message forwarding:* This is the initial stage where all spatially dispersed roaming users comprised in a specific wireless range area send a simple message to their respective neighboring users. As it is mentioned, the message contains the unique id of an individual roaming user for determination of an individual user uniquely, the wireless range area, and the total count of corresponding neighbor users involved in that particular wireless range area. It is compulsory for all roaming users to have their personal neighbor users list and to form a cluster of corresponding neighbor users.

*Stage 2: Wireless search space area recognition:* The individual roaming user should conform their personal least cloaked region, which is basically the wireless range area that hides the confidentiality of the particular roaming user from illegal users (may be invaders). The position related information about a specific roaming user can be accessed by approved roaming users only which are contained within a particular least cloaked region. Therefore, it is crucial for all roaming users to arrange and conform their personal least cloaked region.

*Stage 3: Least cloaked region determination:* A cluster of authorized roaming users covered in the wireless search space area is treated as an input in this stage. This stage is meant for determination of the least cloaked region of a roaming user. It is important to check all the combinations and transformations of the roaming users in a wireless search space area. At least four roaming users should be grouped for the reason that a minimum of two roaming users is required to define the width of the least cloaked region and a minimum of two roaming users are required to define the height of the least cloaked region.

*Stage 4: Least cloaked region scheming and authorization:* Specific roaming user changes its wireless range area into a least cloaked region covering a minimum of *k* users for satisfying the prerequisite of k-anonymity confidentiality. Each roaming user arranges a search space area and determines a value for separate roaming user in its personal neighbor list. This value of roaming user is basically the ratio of the authorized neighbor users count of a specific roaming user to the distance amongst roaming user and individual authorized neighbor user. In conclusion, roaming user formulates its least cloaked region, and this least cloaked region hides the total count of authorized roaming users in the personal neighbor list and the wireless range area of roaming users in a particular wireless search space area.

## IV Algorithm

The complete algorithm is illustrated in this section (Refer Algorithm 1).

**Algorithm 1:** Position Confidentiality Conservation Algorithm (PCCA).

```
Input: Community Network CN, Roaming user R,
  Authorized roaming users A, Neighbor users list NL,
  Neighbor users N, Message M, Anonymity threshold
  value k, users count U, Roaming users count RC,
  Wireless Range Area WRA.
Output: A clustering of Roaming users into clusters of
  size $\leq k$, Wireless Search Space Area WSSA, Least
  Cloaked Region LCR, position confidentiality
  conserving content protection in e-Governance services
  and applications.
procedure CLUSTER FORMATION AND MESSAGE FORWARDING
Neighbor user list NL $\longleftarrow$ NULL
Forward a message with the unique identity of roaming
  user R (R.id), wireless range area (R.WRA) and roaming
  users count (R.RC) to all neighbors of roaming user R.
if authorized roaming users A receives a message M
  from specific roaming user R then add authorized
  roaming users A to Neighbor users list NL
if roaming user R acquired an adequate number of
  authorized roaming users A then broadcast a warning
  message to neighbor users N
if an adequate number of authorized roaming users A
  has not been found then send a message M to neighbor
  users N
procedure WIRELESS SEARCH SPACE AREA RECOGNITION
Wireless search space area WSSA $\longleftarrow$ NULL
Assess each neighbor user N appearing in Neighbor
  users list NL
Neighbor user N with maximum anonymity threshold
  value k from Neighbor users list NL to wireless search
  space area WSSA unless and until cumulative count of
  Neighbor users N in wireless search space area WSSA
  is nevertheless anonymity threshold value k
Recognize and estimate wireless search space area
  WSSA on the basis of anonymity threshold value k and
  Neighbor users list NL
procedure LEAST CLOAKED REGION DETERMINATION
Least cloaked region LCR $\longleftarrow$ NULL
Collect the information of authorized roaming users A
  situated in wireless search space area WSSA
Add individual authorized roaming user A situated in a
  particular wireless search space area WSSA to Least
  cloaked region LCR
```

**Algorithm 1:** (Continued).

```
Add authorized roaming user A to Neighbor users list
  NL
    for $x = 1; x \leq 4; x$++ do
        for Neighbor users list $NL = \{ R_1, .. R_n \}$ in in
            least cloaked region $LCR[x]$ do
            if WRA ( LCR ( NL ) ) < WRA ( LCR ) then
                if RC ( LCR ( NL ) ) >= k then
                    $LCR \longleftarrow \{ NL \}$
                    Remove NL from $LCR[x]$
            else
                Remove NL from $LCR[x]$
procedure Least cloaked region scheming and
  authorization
    if $x < 4$ then
        for each NL; $L = \{ l_1, l_2 .. l_{x+1} \}$, $M = \{ m_1, m_2 .. m_{x+1} \}$ in $LCR[x]$ do
            if $l_1 = m_1 .. l_x = m_x$ and $l_{x+1} \neq m_{x+1}$ then
                Add NL $\{ l_1, m_1 .. l_{x+1}, m_{x+1} \}$ to
                $LCR[x+1]$
    Wireless range area WRA $\longleftarrow$ Least cloaked region
    LCR
    RC $\longleftarrow$ Total number of roaming users R in least
    cloaked region LCR
    Send message M to all authorized roaming users A
    within wireless range area WRA and the position
    anonymous server (PAS)
```

## V. Mathematical Model

This section describes the mathematical model of the proposed framework for content-protection in e-Governance.

1) *Variables:*
   a) R, the roaming users position $[r = 1, 2 ... R] \geq 0$
   b) P, position $[p = 1, 2 ... P] \geq 0$
   c) B, bits $[b = 1, 2 ... B] \geq 0$
   d) T, time $[t = 1, 2 ... T] \geq 0$
   e) C, roaming users current position $[c = 1, 2 ... C] \geq 0$
2) *Decision Variable:*
   a) $A_m$ = if position p is nominated; value is 1; otherwise 0.
3) *Autonomous Function:*
   a) $NC_{ab}$, net confidentiality attained;
   b) $I_a$, inference value for the PCCA.
4) *Factors:*
   a) $CC_{bpt}$, communication cost per unit of *b*th bit at position *p* in time *t*;
   b) $B_{bpt}$, number of bits in association with position *p* in time *t*;
   c) $CC_{bt}$, communication cost of a single bit *b* in time *t*;
   d) $B_t$, number of bits sent at time *t*;
   e) $CTP_{bt}$, consistent time production of the *b*th bit at time *t*;
   f) $MTV_t$, maximum threshold value deliberated for generation of fake records at time *t* in order to achieve content confidentiality in e-Governance;

g) CTP$_{bpct}$, consistent time production of the *b*th bit produced in the *p*th position for current position *c* of the roaming user at time *t*;

h) R$_{bct}$, request for position-based bit *b* from current position *c* of roaming user at time *t*;

i) CAP$_{pt}$, capability of position *p* at time *t*;

j) PROCAP$_{b}$, processing capability for bit *b*;

k) TCAP$_{p}$, total capability of the position *p*;

l) EGSU$_{t}$, e-Governace service use per bit by roaming users at time *t*;

m) TRU$_{t}$, total number of roaming users in the e-Governance scenario at time *t*;

n) UCC$_{bpct}$, unit communication cost of *b*th bit from position *p* to current position *c* of the roaming user at time *t*;

o) A$_{bpct}$, total number of bits from position *p* to current position *c* of roaming user at time *t*;

p) TE$_{bct}$, total communication cost of bit *b* to current position *c* of roaming user at time *t*;

q) UCC$_{rpt}$, unit communication cost of the required contents position *r* to position *p* at time *t*;

r) TB$_{rpt}$, total number of bits sent from the required contents position *r* to position *p* at time *t*;

s) TCT$_{rt}$, total transportation cost of the required contents position at time *t*;

t) IC$_{bt}$, investment cost of bit *b* at time *t*.

5) *Limitations:*

$$\text{Max} \sum_{x=1}^{P} I_x A_x + \sum_{x=1}^{P} \sum_{y=1}^{B} NC_{xy} A_x \tag{1}$$

$$\text{subject} \, to \sum_{x=1}^{P} \sum_{y=1}^{B} CC_{bpt}.B_{bpt} \leq \sum_{y=1}^{B} CC_{bt}.A_x \tag{2}$$

$$\sum_{y=1}^{B} [B_t.CTP_{bt}].A_x \leq MTV_t, t = 1, 2...T \tag{3}$$

$$\sum_{x=1}^{P} \sum_{y=1}^{B} CTP_{bpct} > R_{bct}, t = 1, 2...T, c = 1, 2...C \tag{4}$$

$$TCAP_p >= CAP_{pt} - \sum_{y=1}^{B} [PROCAP_b.B_{bpt}], t = 1, 2...T \tag{5}$$

$$TRU_t >= \sum_{y=1}^{B} [EGSU_t.CTP_{bt}].A_x \tag{6}$$

$$\sum_{y=1}^{B} \sum_{z=1}^{C} [UCC_{bpct}.A_{bpct}] \leq \sum_{y=1}^{B} TE_{bct}.A_x \tag{7}$$

$$\sum_{l=1}^{R} [UCC_{rpt}.TB_{rpt}] \leq TCT_{rt}.A_x, t = 1, 2..T, l = 1, 2..R \tag{8}$$

$$\sum_{t=1}^{T} [TCT_{rt} + TE_{bct}].A_x \leq TCT_{rt} \tag{9}$$

$$\sum_{y=1}^{B} [CC_{bt} + TE_{bt}] \leq IC_{bt}.A_x \tag{10}$$

The autonomous function (1) exploits the net position confidentiality accomplished and qualitative factor of the contents position on the basis of quantitative factors in e-Governance services. Limitations (2) to (10) determine the communication cost, maximum anonymity threshold value, appeal for position-based queries, the capability of a specific position, count on online roaming users, the total communication cost of a specific position-based query, unit communication cost of roaming users perception, unit communication cost from position-based query perception and total investment cost of position-based queries.

## VI. Complexity Analysis

If there are an *R* number of roaming users in a specific wireless range area. As, every roaming user has *R-1* peers, we have to consider,

$$\sum_{m=1}^{R-1} \text{Communication Cost} = 2^{R-1} - 1 \tag{11}$$

wireless search space areas for finding out the least cloaked area. In the proposed algorithm (PCCA), the second stage (wireless search space area recognition) defines a wireless search space area *WSSA* and reduces the count of roaming users situated external to the wireless search space area *WSSA*. Let *A* be the authorized roaming users in the wireless search space area *WSSA* satisfying the condition $A \leq R\ 1$. Therefore, the communication cost may be reduced to

$$\sum_{m=1}^{A} \text{Communication Cost} = A - 1 \tag{12}$$

In stage 3 and 4 of PCCA, it is demonstrated that; the least cloaked region *LCR* can be defined by means of maximum four roaming users. As, we have to consider the arrangements of at the most four roaming users; the communication cost is again reduced to

$$\sum_{m=1}^{4} \text{Communication Cost} = (A^4 - 2A^3 + 11A^2 + 14A)/24$$
$$= O(A^4). \tag{13}$$

In the proposed PCCA, the wireless range area *WRA* is reduced to the wireless search space area comprising only three wireless objects; consequently, it requires to calculate and figure out $2^3$ 1 = 7 least cloaked areas.

## VII. Performance Analysis

The proposed framework is examined in terms of number of position-based queries in real time and confidentiality requirements, number of roaming users in the wireless range

TABLE I
PARAMETERS AND THEIR VALUES

| Sr. No. | Parameter | Value |
|---|---|---|
| 1 | Simulation area | 2 km × 2 km |
| 2 | No. of roaming users | 500 |
| 3 | No. of roaming queries | In a range of 15 500 |
| 4 | User mobility technique | Plus mobility |
| 5 | Time interval | 2 Hours |
| 6 | Anonymity threshold value | Low (5), Medium (7) and High (10) |

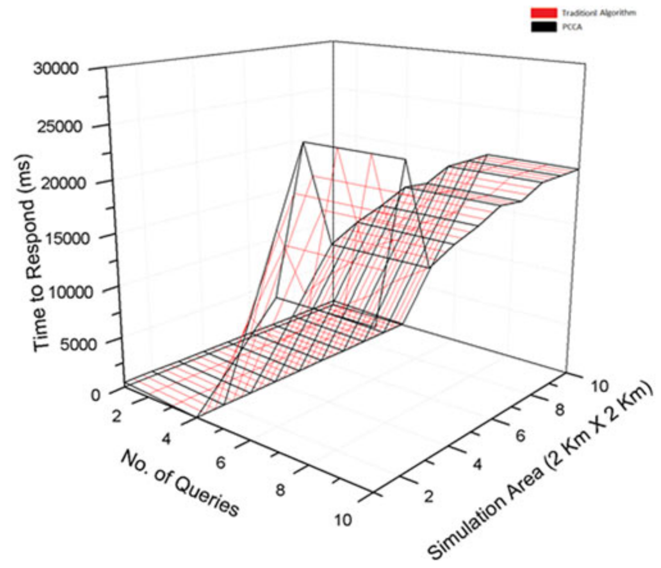

Fig. 4. Impact of PCCA on number of position-based queries, simulation area and time to respond (ms).

area, roaming users mobility and anonymity threshold value. These bound factors and their values are provided as an input to the simulation setup and results obtained are discussed in this section.

### A. Simulation Setup and Performance Bounds

We have implemented the PCCA in Java to simulate the proposed system framework and compare it with the traditional algorithms. All these works are run on a Windows 10 laptop. To simulate our proposed work, 500 roaming users are considered within the simulation area of 2 km × 2 km. Table 1 describes the parameters and their resultant substantial values. Furthermore, to achieve scalability in real-world implementation of the proposed system, we may make use of approach mentioned in ESCAPE [13].

*1) Number of roaming position-based queries and confidentiality requirements:* In the beginning, we calculate the average size of the least cloaked region (in km) and the number of position-based queries by varying the anonymity threshold value k in the range of 5 to 10. The number of roaming users is fixed to 500 while executing each dataset of simulations. In Fig. 4, we confirm that the number of position-based queries within a specific least cloaked region is considerably affected by the anonymity threshold value $k$ and is less affected by number of fake records created.

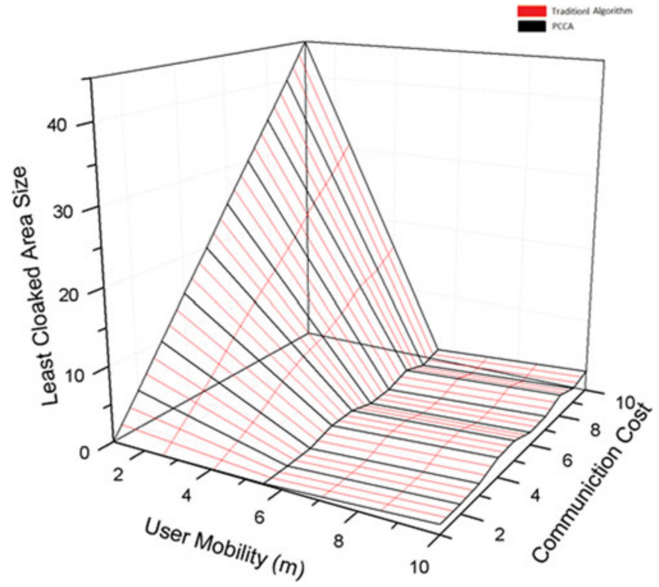

Fig. 5. The performance of PCCA with respect to cumulative roaming users mobility within a definite wireless range area.

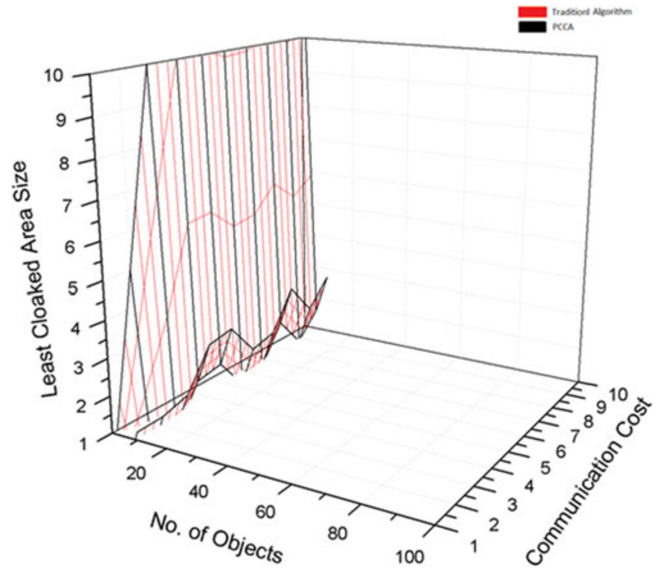

Fig. 6. The performance of PCCA relating to increase in the number of roaming users (objects) from 50 to 500.

*2) Roaming users mobility:* Fig. 5 shows the performance of PCCA with respect to cumulative roaming users mobility within a definite wireless range area. The results show that, the cumulative roaming users mobility affects the least cloaked region size and the communication cost of PCCA to some extent. Therefore, there is a very small effect on wireless search space area scheming and least cloaked region conformation.

*3) Number of roaming users in wireless range area:* Fig. 6 shows the performance of PCCA relating to increase in the number of roaming users from 50 to 500. As depicted in Fig. 6, the communication cost considerably increases when the number of roaming users in wireless search space area increases.

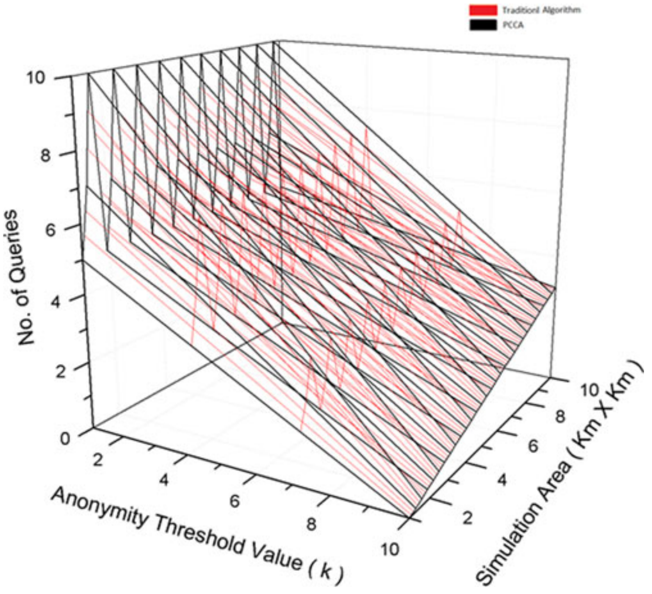

Fig. 7. Impact of the anonymity threshold value (k) on the simulation area and the total number of Queries from roaming users.

*4) Anonymity threshold value:* Additionally, the performance of PCCA is analyzed by means of anonymity threshold value $k$. Several least cloaked regions and value of $k$ varies from 5 to 10 in order to authorize the total number of roaming users in a specific least cloaked region that contains at least $k$ roaming users declared in the proposed framework. In all situations, the average number of roaming users every time exceeds the anonymity threshold value $k$. In case of a simulation area 2 km × 2 km, the number of roaming users is approximately hundred times more than $k$ as it is shown in Fig. 7.

### *B. Performance Metrics*

In addition to the performance bounds mentioned above, we define three performance metrics to measure the effectiveness of our proposed methodology. These performance metrics are: 1) Quality of Service (QoS), 2) Performance (P), and 3) Position Confidentiality Guarantee (PCG).

*1) Quality of Service (QoS):* The QoS is analyzed using the average wireless search space area for the duration of the active lifetime of position-based query as, the roaming users residing in remote places can reduce the general correctness of the results. For a position-based query $Q_{PBS}$, $WSSA_i$ is the wireless search space area of $Q_{PBS}$ at time $t$, the average wireless search space area $WSSA_{iavg}$ $(Q_{PBS})$ is the mean of all the wireless search space areas involved in the given scenario and is estimated as,

$$WSSA_{iavg} Q_{PBS} = \frac{\sum_{i=1}^{n} WSSA_i}{C_{achieved}} \tag{14}$$

Fig. 8 shows the test of QoS. The graph represents a variation of the wireless search space area against the total number of position-based contents. The wireless search space area varies inversely with the number of position-based content until when the number of position-based contents, is about forty, therefore the wireless search space area has virtually remained constant.

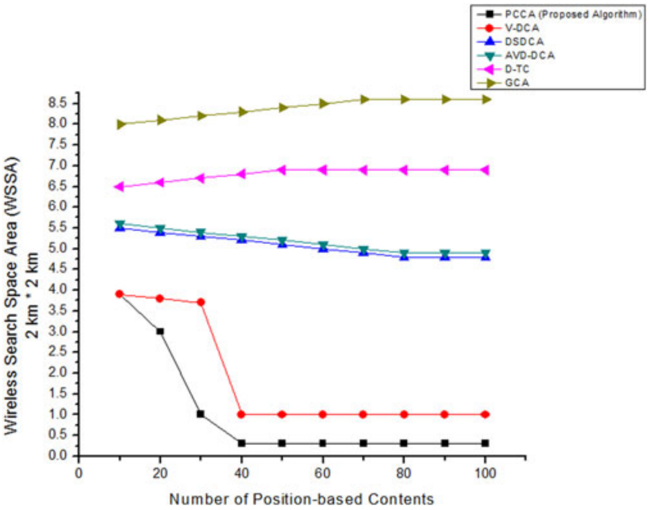

Fig. 8. Quality of Service (QoS) test.

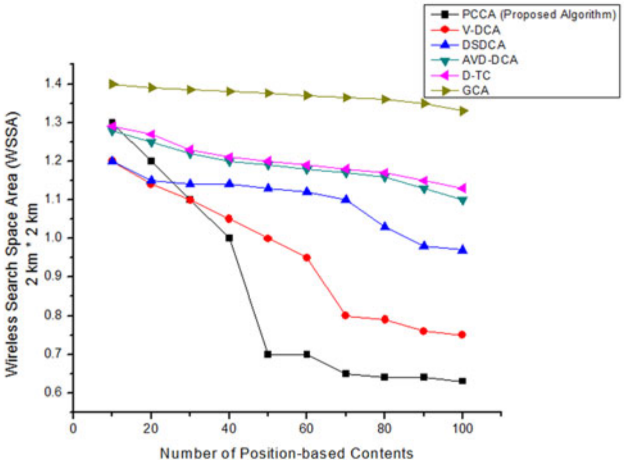

Fig. 9. Performance (P) test.

Usually, as the position-based content increases, the wireless search space area decrease thus improving the QoS. This tendency of improving QoS continued until it becomes almost constant after the 40th number of position-based contents. Using GCA, D-TC, AVD-DCA, DSDCA and V-DCA; QoS practically remains constant at all values of position-based content however the proposed methodology shows varied QoS.

*2) Performance (P):* The performance of proposed methodology is evaluated as the capability of proposed methodology to determine the $k_{resident}$ *1* roaming neighbor users. The wireless search space cloaking time is the time taken by proposed methodology to interrupt usual position-based query request. The average wireless search space cloaking time $WSSCT_{avg}$ for a position-based query that has pass its lively period for a position-based query containing $C_{achieved}$ position-based contents can be estimated as,

$$WSSCT_{avg} = \frac{\sum_{i=1}^{n} CT_{WSSA_i}}{C_{achieved}}. \tag{15}$$

Here, $\mathrm{CT}_{WSSAi}$ is the cloaking time of the position-based query with wireless search space area $WSSA_i$. Fig. 9 depicts

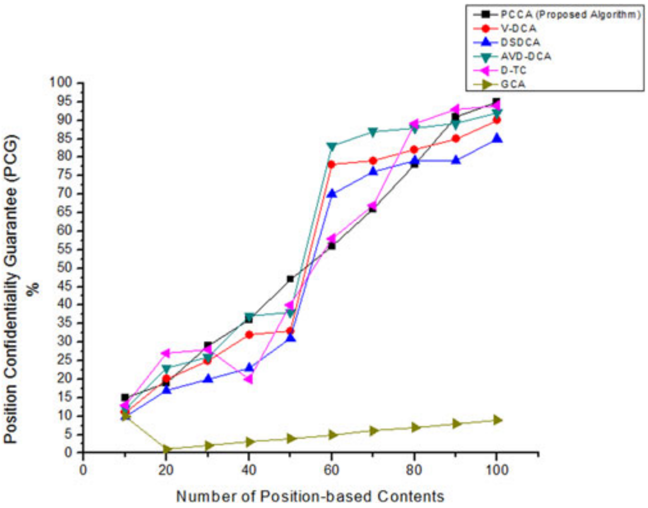

Fig. 10. Position Confidentiality Guarantee (PCG) test.

the performance test of the proposed methodology. The graph shows a variation of wireless search space area against the total number of position-based contents. The wireless search space area varies inversely with the number of position-based contents until about the 40th position-based content when the wireless search space area is almost constant at about 80 ms.

*3) Position Confidentiality Guarantee (PCG):* The position confidentiality of roaming users depends on $k_{universe}$. The position confidentiality of an individual user is always guaranteed as the value of $k_{universe}$ is always superior to $k$. To avoid position-based query conquest, we present a metric called position confidentiality guarantee (PCG). This metric is the ratio of the number of position-based query comprising $C_{achieved}$ position-based contents to the total number of cloaking regions produced within an active query time $CLOAKS_{total}$.

$$PCG = \frac{C_{achieved}}{CLOAKS_{total}}. \tag{16}$$

Fig. 10 depicts the test of position confidentiality guarantee. The graph shows a variation of the position confidentiality guarantee against the number of position-based contents. Generally, the tendency of the graph shows the number of position-based contents vary directly with position confidentiality guarantee.

## VIII. Limitations of Proposed Work and Future Research Directions

The proposed work has some limitations. First, a confidentiality conserving position-based query handling framework for cluster-based roaming users of e-Governance services and applications must be designed and the overall performance of the proposed algorithm (PCCA) must be analyzed and verified with the help of simulation setup as well as a real e-Governance system. Second, problems regarding how each of the e-Governance service providers produce the list of position-based query results with the help of PAS and how the PCCA improves the position-based query results acknowledged from several e-Governance service providers must be addressed. Meanwhile, new challenges associated with content confidentiality issues in e-Governance have been recognized. Alternatively, the confidential content overload and the risk of confidential data revelation are progressively critical [39], [40]. To the extent that we know, some testified works interrelated to e-Governance [41], [42] have suggested a complete solution for conserving roaming users position confidentiality. Then again, protection of sensitive contents on the basis of users position information is correspondingly a challenging and interesting problem. Solutions to prevent invaders from obtaining sensitive information on roaming users through the connections between the position information and e-Governance service-related contents must be studied thoroughly.

## IX. Conclusion

In this paper, we study the problem of conserving roaming users position confidentiality in e-Governance content protection. In an e-Governance services and applications, it is critical to secure and authenticate the citizens personal contents and information. Existing methodologies do not consider this issue. We propose a novel confidentiality conserving position-based query handling framework for cluster-based roaming users of e-Governance services and applications. Then, we offer a Position Confidentiality Conserving Algorithm (PCCA) for content protection in e-Governance services using rule-based approach in computational intelligence. PCCA can organize roaming users into clusters with miscellaneous content interests, hence conserving their position confidentiality in e-Governance services and applications. The experimental results prove that PCCA achieves better performance, guarantees better position confidentiality and offers a quality of service more efficiently in comparison with the state-of-the-art confidentiality conserving position-based query handling algorithms while conserving roaming users content confidentiality in e-Governance services and applications.

## References

[1] K. Yang and X. Jia, "Data storage auditing service in cloud computing: challenges, methods and opportunities," *World Wide Web*, vol. 15, no. 4, pp. 409–428, 2012.

[2] R. Cellan-Jones, "The sidekick cloud disaster," *BBC News*, vol. 1, 2009.

[3] R. Miller, "Amazon addresses EC2 power outages," *Data Center Knowledge*, vol. 1, 2010.

[4] X. Pan, X. Meng, and J. Xu, "Distortion-based anonymity for continuous queries in location-based mobile services," in *Proc. 17th ACM SIGSPATIAL Int. Conf. Adv. Geographic Inf. Syst.*, 2009, pp. 256–265.

[5] L. Stenneth and S. Y. Phillip, "Global privacy and transportation mode homogeneity anonymization in location based mobile systems with continuous queries," in *Proc. 6th Int. Conf. Collaborative Comput., Netw., Appl. Worksharing*, 2010, pp. 1–10.

[6] D. M. Kamenyi, Y. Wang, F. Zhang, I. Memon, and Y. H. Gustav, "Authenticated privacy preserving for continuous query in location based services," *J. Comput. Inf. Syst.*, vol. 9, no. 24, pp. 9857–9864, 2013.

[7] Y. H. Gustav, Y. Wang, M. K. Domenic, F. Zhang, and I. Memon, "Velocity similarity anonymization for continuous query location based services," in *Proc. Int. Conf. Comput. Problem-Solving*, 2013, pp. 433–436.

[8] Y. Wang, L.-p. He, J. Peng, T.-t. Zhang, and H.-z. Li, "Privacy preserving for continuous query in location based services," in *Proc. IEEE 18th Int. Conf. Parallel Distrib. Syst.*, 2012, pp. 213–220.

[9] D. V. Medhane and A. K. Sangaiah, "Source node position confidentiality (SNPC) conserving position monitoring system for wireless networks," in *Proc. Emerging ICT Bridging Future-Proc. 49th Annu. Convention Comput. Soc. India CSI*, 2015, vol. 2, pp. 347–355.

[10] D. V. Medhane and A. K. Sangaiah, “Source node position confidentiality aspects in wireless networks: An extended review,” *Int. J. High Perform. Syst. Archit.* vol. 6, no. 2, pp. 61–81, 2016.

[11] D. V. Medhane and A. K. Sangaiah, “A quantum inspired hybrid intelligent position monitoring system,” in *Proc. Wireless Netw., Quantum Inspired Comput. Intell., Res. Appl.*, 2016, pp. 417–452.

[12] D. V. Medhane and A. K. Sangaiah, “Search space-based multi-objective optimization evolutionary algorithm,” in *Proc. Comput. Elect. Eng.*, vol. 58, 2017, pp. 126–143.

[13] D. V. Medhane and A. K. Sangaiah, “ESCAPE: Effective scalable clustering approach for parallel execution of continuous position-based queries in position monitoring applications,” *IEEE Trans. Sustain. Comput.*, vol. 2, no. 2, pp. 49–61, Apr./Jun. 2017.

[14] K. Gao, Y. Zhu, S. Gong, and H. Tan, “Location privacy protection algorithm for mobile networks,” *EURASIP J. Wireless Commun. Netw.*, vol. 2016, no. 1, pp. 205:1–205:15, 2016.

[15] Z. Xu *et al.*, “Crowdsourcing based description of urban emergency events using social media big data,” *IEEE Trans. Cloud Comput.*, to be published.

[16] Z. Xu, Y. Liu, J. Xuan, H. Chen, and L. Mei, “Crowdsourcing based social media data analysis of urban emergency events,” *Multimedia Tools Appl.*, vol. 76, no. 9, pp. 11567–11584, 2017.

[17] S. H. Altman, N. T. Sivo, E. D. Tana, and B. R. Knapp, “Location-based advertising message serving for mobile communication devices,” U.S. Patent 8 682 350, Mar. 25, 2014.

[18] Z. Xu, H. Zhang, V. Sugumaran, K.-K. R. Choo, L. Mei, and Y. Zhu, “Participatory sensing-based semantic and spatial analysis of urban emergency events using mobile social media,” *EURASIP J. Wireless Commun. Netw.*, vol. 2016, no. 1, pp. 1–9, 2016.

[19] Joseph, Barry LEWIS II, B. Patel, and S. Sivalingham, “Location-aware instant messaging,” U.S. Patent 8 655 960, Feb. 18, 2014.

[20] H. Hu, J. Xu, Q. Chen, and Z. Yang, “Authenticating location-based services without compromising location privacy,” in *Proc. ACM SIGMOD Int. Conf. Manage. Data*, 2012, pp. 301–312.

[21] A. Havlark, V. Burton, and J. Ahrens, “Wireless telecommunications location based services scheme selection,” U.S. Patent 9 599 717, issued Mar. 21, 2017.

[22] W. Enck *et al.*, “TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones,” *ACM Trans. Comput. Syst.*, vol. 32, no. 2, pp. 5:1–5:15, 2014.

[23] Y.-A. De Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, “Unique in the crowd: The privacy bounds of human mobility,” *Sci. Rep.*, vol. 3, 2013, Art. no. 1376.

[24] T. Qiu, Y. Zhang, D. Qiao, X. Zhang, M. L. Wymore, and A. K. Sangaiah, “A robust time synchronization scheme for industrial internet of things,” *IEEE Trans. Ind. Inf.*, to be published, 2017.

[25] K. Li and Timon C. Du, “Building a targeted mobile advertising system for location-based services,” *Decision Support Syst.*, vol. 54, no. 1, pp. 1–8, 2012.

[26] I. Leontiadis, C. Efstratiou, M. Picone, and C. Mascolo, “Don’t kill my ads!: Balancing privacy in an ad-supported mobile application market,” in *Proc. 12th Workshop Mobile Comput. Syst. Appl.*, 2012, Art. no. 2.

[27] A. N. Khan, M. L. M. Kiah, S. U. Khan, and S. A. Madani, “Towards secure mobile cloud computing: A survey,” *Future Gener. Comput. Syst.* vol. 29, no. 5, pp. 1278–1299, 2013.

[28] M. R. Rahimi, J. Ren, C. H. Liu, A. V. Vasilakos, and N. Venkatasubramanian, “Mobile cloud computing: A survey, state of art and future directions,” *Mobile Netw. Appl.*, vol. 19, no. 2, pp. 133–143, 2014.

[29] K. P. N. Puttaswamy *et al.*, “Preserving location privacy in geosocial applications,” *IEEE Trans. Mobile Comput.*, vol. 13, no. 1, pp. 159–173, Jan. 2014.

[30] B. Craenen and A. Eiben, “Computational intelligence,” in *Encyclopedia Life Support Sciences*, Paris, France: EOLSS Publ., 2009, Art. no. 142.

[31] J. C. Bezdek What is computational intelligence?. No. CONF-9410335. USDOE Pittsburgh Energy Technology Center, PA, USA; Oregon State Univ., Corvallis, OR, USA. Dept. of Computer Science; Naval Research Lab., Washington, DC, USA; Electric Power Research Inst., Palo Alto, CA, USA; Bureau of Mines, Washington, DC, USA, 1994.

[32] M. R. Przybylek, “Skeletal algorithms in process mining,” *Stud. Comput. Intell.*, vol. 465, pp. 119–134, 2013.

[33] L. A. Zadeh, “Is there a need for fuzzy logic?” *Inf. Sci.*, vol. 178, no. 13, pp. 2751–2779, 2008.

[34] C.-S. Tseng, B.-S. Chen, and H.-J. Uang, “Fuzzy tracking control design for nonlinear dynamic systems via TS fuzzy model,” *IEEE Trans. Fuzzy Syst.*, vol. 9, no. 3, pp. 381–392, Jun. 2001.

[35] C. O. Rolim *et al.*, “Situation awareness and computational intelligence in opportunistic networks to support the data transmission of urban sensing applications,” *Comput. Netw.*, vol. 111, pp. 55–70, 2016.

[36] P. Trebatick, “Prediction of dynamical systems by recurrent neural networks,” *Inf. Sci Technol. Bull. ACHM Slovakia*, vol. 1, no. 1, pp. 47–56, 2009.

[37] Z. Xiang and X. Deyun, “Fault diagnosis based on the fuzzy recurrent neural network,” *Asian J. Control*, vol. 3, no. 2, pp. 89–95, 2001.

[38] M. D. Vishwasrao and A. K. Sangaiah, PCEOMLeT: Position confidentiality enforcement through opacity and machine learning techniques,” *IEEE Trans. Serv. Comput.*, to be published.

[39] Z. Liu, J. Luo, and L. Xu, “A fine-grained attribute-based authentication for sensitive data stored in cloud computing,” *Int. J. Grid Utility Comput.*, vol. 7, no. 4, pp. 237–244, 2016.

[40] X. Xiao, C. Chen, A. K. Sangaiah, G. Hu, R. Ye, and Y. Jiang, “CenLocShare: A centralized privacy-preserving location-sharing system for mobile online social networks,” *Future Gen. Comput. Syst.*, 2017.

[41] D. Li, Q. Lv, L. Shang, and N. Gu, “Efficient privacy-preserving content recommendation for online social communities,” *Neurocomput.*, vol. 219, pp. 440–454, 2017.

[42] T. Ishida, *et al.*, “The digital contents management system based on position information initiate fusion of AR and sensor technology,” *Int. J. Space-Based Situated Comput.*, vol. 6, no. 1, pp. 31–42, 2016.

**Darshan Vishwasrao Medhane** received the Graduate degree in information technology engineering from the University of Pune, Pune, India. He received the Master of Engineering degree in computer networks from the University of Pune, Pune, India. He is currently working toward the Ph.D. degree at the VIT University, Vellore, India. He has authored eight books and twelve publications in international journals and conferences. His areas of interest are security in wireless networks, quantum computational intelligent systems, and position monitoring system.

**Arun Kumar Sangaiah** received the M.E. degree in computer science and engineering from the Government College of Engineering, Tirunelveli, Anna University, India. He received the Ph.D. degree in computer science and engineering from the VIT University, Vellore, India. He is currently working as an Associate Professor in the School of Computer Science and Engineering, VIT University, India. He has authored more than 100 publications in different journals and conference of national and international repute. His current research work includes global software development, wireless ad hoc and sensor networks, machine learning, cognitive networks and advances in mobile computing and communications. Also, he has registered a one Indian patent in the area of Computational Intelligence. Besides, he is responsible for Editorial Board Member/Associate Editor of various international journals.