Received July 28, 2020, accepted August 4, 2020, date of publication August 7, 2020, date of current version August 24, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3015096

Privacy and Security Management in Intelligent Transportation System

SURESH CHAVHAN[1], (Member, IEEE), DEEPAK GUPTA[2], (Member, IEEE), SAHIL GARG[3], (Member, IEEE), ASHISH KHANNA[2], (Member, IEEE), BONG JUN CHOI[4], (Senior Member, IEEE), AND M. SHAMIM HOSSAIN[5], (Senior Member, IEEE)

[1]Automotive Research Center, Vellore Institute of Technology, Vellore 632014, India
[2]Maharaja Agrasen Institute of Technology, Delhi 110086, India
[3]Electrical Engineering Department, École de technologie supérieure, Montreal, QC H3C 1K3, Canada
[4]School of Computer Science and Engineering, Soongsil University, Seoul 06978, South Korea
[5]Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia

Corresponding authors: Bong Jun Choi (davidchoi@soongsil.ac.kr) and M. Shamim Hossain (mshossain@ksu.edu.sa)

This work was supported in part by the National Research Foundation (NRF), South Korea, funded by the Ministry of Science and ICT (MSIT), South Korea, under Grant 2019R1C1C1007277, and in part by the Researchers Supporting Project number (RSP-2020/32), King Saud University, Riyadh, Saudi Arabia for funding this work.

ABSTRACT Metropolitan transportation is a dynamic and non-linear complex system. In such a system, there are possibilities of altering, monitoring, forging, and accessing private, public, and resource information of depot staff and communicating agents by unauthorized agencies the metropolitan area. Existing solutions for the management of security and privacy of communicating agents in an intelligent public transportation system (IPTS) do not adapt to the dynamic occurrence of real-time event information. Therefore, existing solutions are insufficient to address the randomness and other characteristics pertaining to a non-linear complex system such as an intelligent transport system (ITS). To this end, in this article, we propose a privacy and security management scheme for ITS depot staff in a metropolitan area. This scheme provides privacy and security management in the transportation industry during the exchange of information regarding vehicle allocation, dispatch, revocation, financial, and maintenance. Absence of such an aforementioned scheme leads to anomalies such as impersonation of genuine staff and malicious and greedy staff. We use the emergent intelligence (EI) technique to collect, analyze, and share information, and take dynamic decisions during the security and privacy management of the depot staff in transport industries. The EI technique provides autonomy, flexibility, adaptiveness, robustness, self-organization, and evolution to address the randomness and behavior of a non-linear complex system pertaining to the transportation system in metropolitan areas. The proposed scheme is implemented using the Crypto++ package, and the results indicate that the scheme efficiently manages the security and privacy in transportation industries in metropolitan areas.

INDEX TERMS Emergent intelligence, intelligent transportation systems, metropolitan area networks, privacy and security policy, pseudonyms, transport depot staff.

I. INTRODUCTION

Metropolitan areas which include urban areas, satellite cities, rural areas, etc., are highly congested. They are divided into regions, and each region is further subdivided into zones. A transportation depot is built (especially, in metropolitan cities in India) for each region to satisfy the commuting needs of people. Depots in transportation industries are premises where resources (e.g., vehicles, fuel, staff) are stored, managed, and allocated by the manager (e.g., agent). Owing to the dynamic arrival rates of the commuters, staff, and vehicles in transport depots [1], there may be possibilities of altering, monitoring, and forging the public and private information of transport depots and staff by third parties [2]. Moreover, the third parties can use the private and public data to create situations such as traffic congestion, underutilization of

The associate editor coordinating the review of this manuscript and approving it for publication was Rongxing Lu.

resources, and lane blocking. Therefore, the intelligent public transport system (IPTS) faces various privacy and security challenges in metropolitan cities [29], [30].

Owing to the advancement of various information and communication technologies (ICTs) [3], [4] and high penetration of their deployment, a greater threat of observing and analyzing communication entities by third parties arises. This problem can be mitigated by using privacy preservation techniques such as anonymity, mutual authentication, and cryptography [8], [11]. The anonymity technique hides the identification information of entities during their interactions with others by using pseudo-identity. These anonymous communicating entities can become malicious if they are compromised [3]–[5]. This is a severe security threat because it is difficult to recognize and revocate such entities from the group once they are compromised. Therefore, an intelligent privacy and security technique is needed to remove the privacy of such communicating entities, i.e., make them non-anonymous. This step is required on detection of the malicious entities.

Several existing works utilize public key infrastructure (PKI) for achieving anonymity. The PKI is based on cryptographic primitives such as Rivest-Shamir-Adleman (RSA) and elliptical curve cryptosystem (ECC). In the intelligent transportation system (ITS), ECC is considered to be more suitable than RSA owing to its lower computational cost and smaller key size, albeit the same level of privacy protection [4]–[6], [12], [17], [18]. To provide solutions to the privacy and security problems in the ad-hoc network, anonymous authentication schemes such as group signature [2], [3], [6] and pseudonym authentication [2], [4], [5], [7], [9], [10] are used. However, these schemes require high computational power and have bandwidth limitations.

Alternatively, the privacy-preserving ciphertext-policy attribute-based encryption (PP-CP-ABE) scheme [19] preserves the privacy of users using access policies. These access policies are formed using user attributes. Moreover, the privacy-preserving attribute-based broadcast encryption (PP-AB-BE) scheme uses hidden access policy, either with or without specifying the receivers. It has been observed that this scheme reduces the storage and communication overheads. The broadcast group key management (BGKM) scheme [20] was proposed for managing the key, wherein an attribute-based access control policy preserves the user's identity attributes while sharing documents in an untrusted cloud storage. This approach encrypts and decrypts the document if it satisfies the policy and keys.

These schemes face drawbacks such as high computation overhead, possibility of disclosing anonymity of communication entities, difficulty in identifying and revocating malicious communication entities, and vulnerability of roadside units (RSUs) to physical attacks. The generation of pseudonymous keys requires a considerable amount of resources. Moreover, such keys cannot preserve and disclose privacy as required, and are not efficient for distributed environments.

To this end, in this article, we propose a privacy and security management scheme for supporting IPTS depots in metropolitan areas using an emergent intelligence (EI) technique. The proposed scheme is based on the integration of the transport depot staff's policies, pseudonymous technique, cryptographic techniques, bilinear pairing, and EI technique. The IPTS depot staff is categorized into three levels to provide three different levels of privacy. Each level is determined by a policy managed by the regional trusted authority (RTA). These policies are formed using the depot staff's credentials that comprise the type of staff, working time, working place, authentication information, the signature of RTA, and pseudonyms. The proposed scheme provides accurate and reliable information (e.g., resource availability, resource allocated, traffic conditions) to the transport depot agents, which can be shared with the neighbor depot's agents.

The remainder of the paper is organized as follows. Section II presents the system model, assumptions, and preliminaries of the proposed scheme. Section III presents the principle of the EI technique. Sections IV and V discuss the principles of the privacy preservation scheme and policy-based transport depot staff. Section VI presents the performance analysis and results. Finally, Section VII concludes the paper.

II. SYSTEM MODEL

In this section, we present the necessary assumptions, definitions, communication network model, attack model, and background of the mathematical concepts.

A. PUBLIC TRANSPORT DEPOT

A public transport depot in a metropolitan area is the transport system's operating base [22]. The depot contains many administrative functions, engineering, and managerial functions for staff. There are three grades of the staff: depot manager (DM), operations and engineering manager (OEM), and administrative, personnel, and accounts staff (APAS). Each staff member discharges their respective duties and interacts with others. RTAs, who are responsible for issuing the initial security keys and parameters, are deployed at the depot. It is assumed that they can be trusted and cannot be compromised.

B. COMMUNICATION NETWORK MODEL

Fig. 1 shows the different communication entities and technologies in a metropolitan region. The communication network model comprises agents, RSUs, vehicles, and an RTA. RSUs cannot be fully trusted because they are installed in an open environment, making them more prone to physical breaches. The RTA continuously monitors the RSUs to detect any malicious behavior and sends revocation messages via vehicle to everything (V2X) communication using the dedicated short-range communication (DSRC) technology. The RSUs and agents are assumed to be time-synchronized.

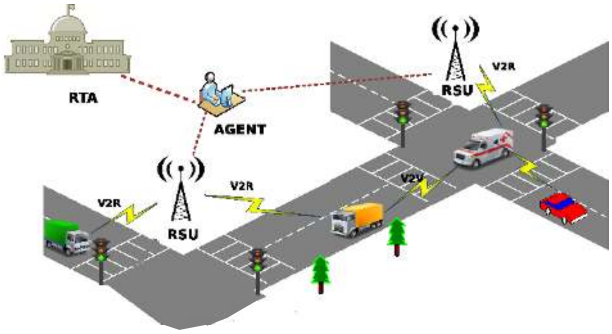


FIGURE 1. Communication network model in metropolitan area.

C. POLICY-BASED PRIVACY

A policy is a set of rules under which a specific action can be taken on a particular sensitive resource [24]. There are two cryptographic primitives for enabling privacy-aware policy enforcement.

1) *Policy-based encryption*: This cryptographic primitive requires data to be encrypted according to the policy such that only organizations compliant with the policy can successfully decrypt the plaintext data.
2) *Policy-based signature*: This cryptographic primitive uses the policy to generate digital signature. Only the entities that satisfy the policy can generate a valid digital signature.

These cryptographic primitives involve developing privacy policies, automated trust negotiation, trust establishment, access control, etc. In this article, we use the policy-based encryption cryptographic primitive for the privacy preservation of transport depot staff during the exchange and/or access of information about vehicle allocation, dispatch, revocation, financial transactions, and maintenance. In the absence of a privacy preservation scheme, anomalies such as impersonation, and malicious and greedy staff can be seen at the transport depot.

D. ATTACK MODEL

In a metropolitan area, various entities (e.g., vehicles, RSUs, agents) are connected via communication links. These links are highly vulnerable to attacks. Attackers can access, alter, monitor, and forge private information. These malicious tasks executed by the attackers can be classified into internal and external, depending on the attackers' locations [16].

An external attacker observes the ongoing communication and analyzes traffic-related data; however, they cannot decipher messages. On the contrary, internal attackers such as malicious agents and staff have full rights to access both public and private information of transport depots. Therefore, if compromised, they can become powerful attackers. Among the several possible attack scenarios in metropolitan areas, we consider the following attack scenarios in this study.

1) *Impersonation of Genuine Staff*: The attacker pretends to be the staff to fool others and access privileged information.
2) *Malicious Staff*: Malicious behavior can result in illegal access to data, which can have a dangerous impact during emergencies.
3) *Greedy Staff*: The greedy staff tries to use resources for their benefit. They may create unnecessary problems such as traffic jam, lane blocking, etc.

The proposed scheme assures privacy and security under the abovementioned scenarios, which are discussed in subsequent sections.

E. PRELIMINARIES

The proposed privacy preservation scheme uses the following basic mathematical concepts.

1) *Bilinear Pairing:* A bilinear mapping function pairs an element between two groups and another group [25]. *Definition:* Consider groups, g_1 *and* g_2 (multiplicative and additive), with the same order, p, where $p = q^n, n \in \mathbb{Z}^+$, and q is a prime number. The bilinear mapping $\hat{e} : g_1 \times g_1 \rightarrow g_2$ satisfies the following three properties.
   a) *Bilinearity:* $\forall M, N \in g_1$, $\forall a, b \in \mathbb{Z}_p^*$: $\hat{e}(aM, bN) = \hat{e}(M, N)^{ab}$, where $\mathbb{Z}_p^* = [1, 2, \ldots, p-1]$.
   b) *Non-degeneracy:* If M is a generator of g_1, then $\hat{e}(M, M)$ is a generator of g_2.
   c) *Computability:* The algorithm to compute bilinear map $\hat{e} : g_1 \times g_2$.
2) *Elliptic Curve Discrete Logarithm Problem (ECDLP) [21]:* Given points X and Y of the group, find the value of k such that $Xk = Y$.
3) *Bilinear Diffie-Hellman Problem (BDHP):* Given $(M, a.M, b.M, c.M)$ for $a, b, c \in \mathbb{Z}_p$, compute $e(M, M)^{abc}$.

III. EI TECHNIQUE

The EI methodology is an extension of the multi-agent system (MAS), in which agents are involved in group activities and individual decision-making. The EI strategy is one category of agents' mutual intelligence [23], [33]–[35]. This group of agents interacts cooperatively, coordinately, and collaboratively to provide dynamic independent decisions. The EI technique can be used to perform individual tasks and subtasks in parallel, thereby providing a partial (or complete) solution.

EI is the intelligence of a task-oriented group of agents [14]. Groups of agents interact periodically and on-demand in a dynamic and unpredictable environment to provide decisions to achieve the common goals of the system. Herein, the entities have a common interest, whereas the entities of a MAS may have diverging interests.

To illustrate the EI technique, consider task t_A in a 3-node network as shown in Fig. 2. Depending on its objectives, t_A is divided into sub-tasks: st_{A_1}, st_{A_2}, and st_{A_3}. These subtasks are respectively assigned to the three different agents and executed independently. The EI technique is deployed at node A, and the task is initiated. This technique generates and

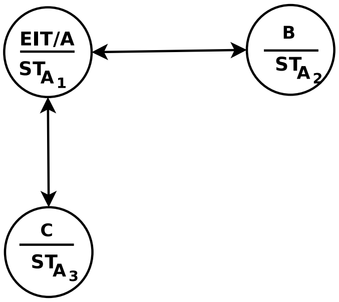


FIGURE 2. Scenario of a 3-node network with task and sub-tasks.

dispatches three agents (A_1, A_2, A_3) to nodes A, B and C, respectively. Furthermore, the three agents independently solve the assigned task using local and global knowledge. Finally, all the agents send their individual decisions to agent A_1. Agent A_1 uses the following equation to provide the collective intelligence of the group.

$$d(t_A) = d(st_{A_1}) + d(st_{A_2}) + d(st_{A_3}) \tag{1}$$

where $d(st_{A_1})$, $d(st_{A_2})$, and $d(st_{A_3})$ are the decisions of individual agents taken at nodes A, B, and C, respectively.

The ITS has several characteristics outlined below that make it suitable to be solved by the EI technique rather than by MAS or SI.

- Complexity: A transportation system's behavior is considerably complex to be modeled with the traditional approach, owing to the lack of synchronization among different components of the system. The EI technique, which is based on the observed and collected data is more suitable for modeling such complex systems.
- Qualitative data: A transportation system comprises both quantitative and qualitative data. A considerable amount of qualitative data must be dealt with in such a system, and the process can be facilitated using the EI technique.
- Non-linear and dynamic system: Transportation systems are non-linear, dynamic, and complex stochastic systems. Therefore, in their case, it is often not possible to find the optimal solution. The EI technique provides a natural alternative to obtain optimal or sub-optimal solutions.
- Simple model: Most of the methods of the ITS for metropolitan area are built upon precise analytical models. However, in reality, it is challenging to model the ITS traffic, security, and privacy accurately. However, the EI technique does not require a precise model.
- The EI technique is adaptable to the dynamic, uncertain, and complicated system under consideration and replenishes the environment by creating autonomous regenerating feedback loop through spontaneous interaction among a group of agents. Thereby, it allows to provide intelligent behaviors for transportation in metropolitan areas.

Some works attempted to use the EI technique for solving the problem [31], [32]. However, they have not provided a clear methodology to solve the assigned tasks in unpredictable environments. Therefore, in this research, for a metropolitan area, the acquisition, analysis, and sharing of transport depot staff information such as private, public, and transport resource information and dynamic decision information is done using the EI technique.

IV. PROPOSED POLICY-BASED PRIVACY PRESERVATION SCHEME FOR ITS

In this section, we present the policy-based privacy preservation system setup, three levels of depot staff privacy preservation, and EI technique-based privacy preservation for depot staff. Table 1 lists the symbols used in the paper and their descriptions.

TABLE 1. Symbols used.

Symbol	Description
k	Secret key
β	RTA's master key
C	Policy encryption
Pol_i	i-th policy
$\bar{C}$	Policy decryption
M	Message
$Cert_i$	Certificate of i-th level staff
CID_i	Certificate id of i-th level staff
MID	Manager id
$SigAlg$	Algorithm used to create signature
RID	RTA's id
Val	Validity of certificate
PK_{MID}	Public key of MID
RTA_{PK}	RTA's public key
RTA_{SK}	RTA's private key
$MType$	Message type: request or response

A. SYSTEM SETUP

The policy-based privacy-aware cryptosystem (PAC) setup is achieved by two randomizing algorithms: (1) PAC setup and (2) RTA setup algorithms.

1) PAC SETUP

Given a secret key, k, as input parameter, execute the following.

1) The BDH algorithm generates $(p, g_1, g_2, \hat{e})$ parameters.
2) Randomly choose a generator, $X, \in g_1$.
3) n is a random number chosen from $\mathbb{N}^*$, and let $M = \{0, 1\}^n$.
4) Let $C = g_1 \times (\{0, 1\}^n)^* \times M$ and $S = (g_2)^* \times g_1$.
5) Hash functions: $h_0 : \{0, 1\}^* \rightarrow g_1$, $h_3 : \{0, 1\}^* \rightarrow \mathbb{Z}_p^*$, $h_4 : \{0, 1\}^* \rightarrow \{0, 1\}^n$, $h_5 : \{0, 1\}^n \rightarrow \{0, 1\}^n$, *and* $h_6 : \{0, 1\}^* \rightarrow \mathbb{Z}_p^*$.
6) $PubParam = (p, g_1, g_2, \hat{e}, n, X, h_0, h_3, h_4, h_5, h_6)$.

Public parameters describe the different groups and public functions that are used in the system.

2) RTA SETUP

The RTA chooses a random master-key, $s \in \mathbb{Z}_p^*$, and uses it to compute the corresponding public key, $RTA_{PK} = sX$. All system participants have access to the public key.

B. TRANSPORT DEPOT STAFF PRIVACY PRESERVATION MODEL

In this subsection, we discuss three different privacy policies for three levels of the depot staff. Here, we define a policy using logical expressions that comprise conjunctions ($\wedge$) and disjunctions ($\vee$) using the user credentials. We define an assertion for each staff member at the depot. An assertion provides information about the staff member's attributes, properties, capabilities, etc. It is encoded as a binary string, $A \in \{0, 1\}^*$. The details of the representations of assertions are out of scope of this article. Assertions are represented as credentials, and their validity is provided by the RTA using signature verification. These credentials are generated using the credential generation (CredGen) algorithm by the RTA whenever an assertion is valid.

CredGen: The CredGen algorithm takes the valid assertion, A, and RTA's master key, β as input, and outputs $\xi(RTA_{PK}, A) = (\beta, h_0(A))$.

The RTA defines the credentials and certifies their validity. The proposed policy-based privacy preservation scheme has three levels of depot staff depending upon their grades. As shown in Figure 3, the hierarchy of the depot staff is: (1) APAS, (2) OEM, and (3) DM.

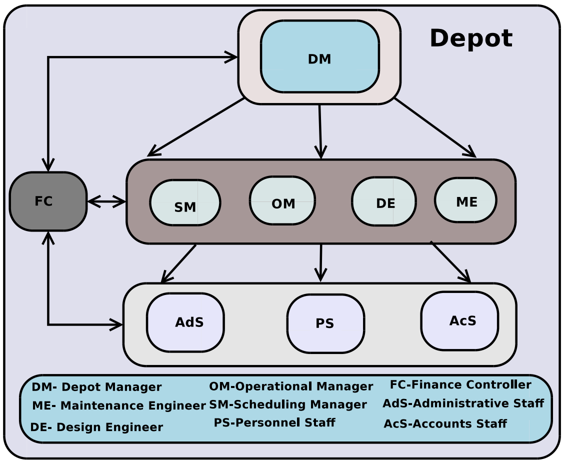


FIGURE 3. Hierarchy of staff at the transportation depot.

The proposed policy-based privacy preservation scheme provides different levels of privacy to each level in the staff hierarchy that runs at the transport depot depending upon the privacy parameters, as shown in Figure 4. The privacy preservation at levels 1, 2, and 3 are presented in the following subsections.

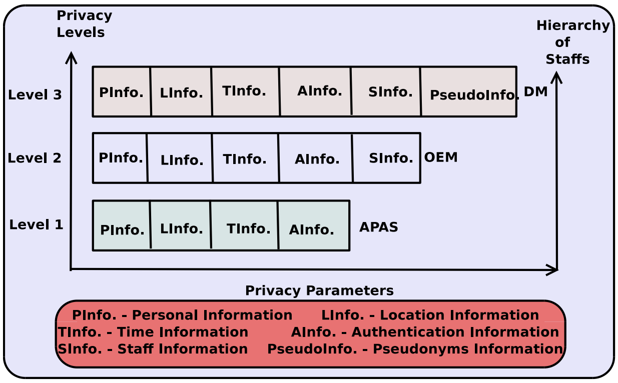

Privacy Levels
Hierarchy of Staffs
Level 3
PInfo.
LInfo.
TInfo.
AInfo.
SInfo.
PseudoInfo.
DM
Level 2
PInfo.
LInfo.
TInfo.
AInfo.
SInfo.
OEM
Level 1
PInfo.
LInfo.
TInfo.
AInfo.
APAS
Privacy Parameters
PInfo. - Personal Information
LInfo. - Location Information
TInfo. - Time Information
AInfo. - Authentication Information
SInfo. - Staff Information
PseudoInfo. - Pseudonyms Information

FIGURE 4. Privacy levels at the transportation depot.

C. PRIVACY PRESERVATION AT LEVEL 1

The APAS at the depot are registered with the RTA. During registration, the APAS provides their private information to the RTA. The RTA then encrypts and stores this information in its database. The RTA provides authentication information (Auth-Info) such as username/password. The level 1 policy (pol_1) is formed by the RTA at the depot using the credentials of APAS as:

$pol_1 =< Depot_i, x : Staff > \wedge < Depot_i, x : ID > \wedge < Depot_i, x : Time > \wedge < Depot_i, x : Location > \wedge < RTA_j, x : Auth - Info >$ where, $x \in$ {Administrative staff, Personnel staff, Accounts staff} and ID is the identity of staff member x.

TABLE 2. Notations used in the privacy policy execution.

Notation	Meaning
pol_1	Level 1 Policy
Auth-Info	Authentication Information
$Depot_i, x : Staff$	Staff x belongs to depot i
$Depot_i, x : ID$	Identity of staff x, who belongs to depot i
$Depot_i, x : Time$	Working time of staff x, who belongs to depot i
$Depot_i, x : Location$	Working location of staff x, who belongs to depot i
$staff \leftharpoonup \xi(RTA_{PK}, A)$	Credential of âĂIJStaffâĂİ was issued$\xi(RTA_{PK}, A)$
$staff \rightleftharpoons < RTA_{PK}, A >$	âĂIJStaffâĂİ fulfills condition $< RTA_{PK}, A >$
$staff \rightleftharpoons pol_1$	âĂIJStaffâĂİ satisfies policy 'pol_1'
$staff \rightleftharpoons pol_1 \Leftrightarrow staff \leftharpoonup \xi_{1,2,\ldots,j}(pol_1)$	Set of credentials fulfills policy 'pol_1'

The following steps are used to preserve the privacy of staff. The notations in Table 2 based on policy 1 issued by the RTA are used.

1) $staff \leftharpoonup \xi(RTA_{PK}, A)$.
2) The APAS encrypts message M according to pol_1, i.e., $C = PolEnc(M, pol_1)$ (given in algorithm 1) and sends it to the RTA.

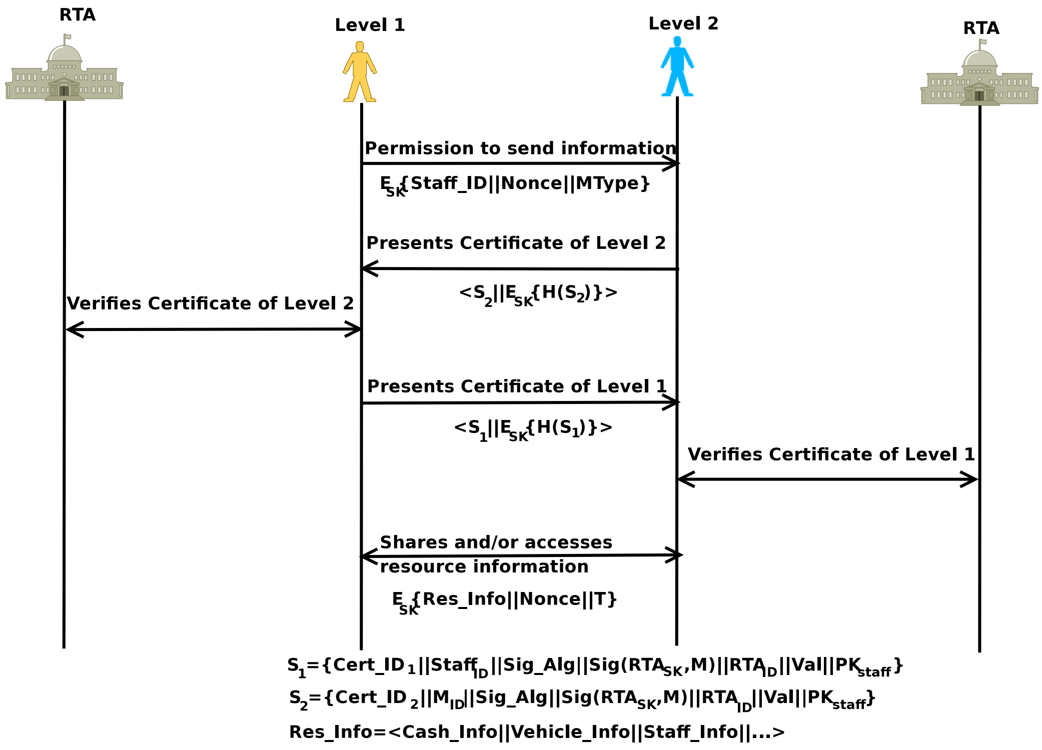

RTA
Level 1
Level 2
RTA
Permission to send information
E_SK{Staff_ID||Nonce||MType}
Presents Certificate of Level 2
<S_2||E_SK{H(S_2)}>
Verifies Certificate of Level 2
Presents Certificate of Level 1
<S_1||E_SK{H(S_1)}>
Verifies Certificate of Level 1
Shares and/or accesses resource information
E_SK{Res_Info||Nonce||T}
S_1={Cert_ID_1||Staff_ID||Sig_Alg||Sig(RTA_SK,M)||RTA_ID||Val||PK_staff}
S_2={Cert_ID_2||M_ID||Sig_Alg||Sig(RTA_SK,M)||RTA_ID||Val||PK_staff}
Res_Info=<Cash_Info||Vehicle_Info||Staff_Info||...>

FIGURE 5. Sequence diagram depicting mutual authentication between level 1 and 2's staff.

Algorithm 1 Encryption Based on Policy 1

```
Data: message $M$ and $pol_1$.
$t_i$ choose from $\{0, 1\}^n$.
Compute $t = \oplus_{i=1}^{a} t_i,\ r = h_3(M \parallel t \parallel pol_1),\ and\ U = rX$.
for i=1, 2, ..., a do
    $g_i = \prod_{k=1}^{a_i} \hat{e}(R_{i,k}, h_o(A_{i,k}))$
    $v_i = t_i \oplus h_4(g_i^r \parallel i)$
end for
Calculate $w = M \oplus h_5(t)$
Ciphertext $C = \left(U, [v_i]_{1 \leq i \leq a}, w\right)$
End
```

3) The RTA decrypts the received message using its secret credentials, $\bar{C} = PolDec(C, pol_1, \xi_{1,2,...,j}(pol_1))$ (given in algorithm 2).
4) The RTA checks $U = \bar{U}$, then $staff \rightleftharpoons < RTA_{PK}, A >$ and $staff \rightleftharpoons pol_1$ implies $staff \rightleftharpoons pol_1 \Leftrightarrow staff \leftharpoonup \xi_{1,2,...,j}(pol_1)$.
5) The APAS performs its job such as processing cash and vehicle and staff information.

Before the level 1 staff can share information such as processed cash and vehicle and staff information with the level 2 manager, both parties must mutually authenticate each other. We use a certificate-based authentication scheme, wherein certificates are issued by the RTA, as shown in Figure 5.

Algorithm 2 Decryption Based on Policy 1

```
Data: $C, pol_1, \xi_{1,2,...j}(pol_1)$.
for i=1,2, ..., a do
    Compute $\bar{g}_i = \hat{e}\left(U, \sum_{k=1}^{a_i}(\xi_{i,k}, A_{i,k})\right)$
    $\bar{t}_i = v_i \oplus h_4(\bar{g}_i \parallel i)$
end for
Compute $\bar{M} = w \oplus h_5(\oplus_{i=1}^{a} \bar{t}_i)$.
Compute $\bar{U} = h_3(\bar{M} \parallel \oplus_{i=1}^{a} \bar{t}_i \parallel pol_1).X$
End
```

The following steps are performed during mutual authentication.

1) Level 1's staff asks permission to send information such as processed cash and vehicle and staff information from Level 2's manager by sending a token that is represented as $token =< E_{SK}\{Staff_{ID}||Nonce||MType\} >$, where $MType$ is the message type with a value of either 1 (request or permission message) or 2 (response message).
2) Level 2's manager presents their certificate, $Cert_2$, which is given as $Cert_2 =< S_2||E_{SK}\{H(S_2)\} >$, where $S_2 =< \{CID_2||MID||SigAlg||Sig(RTA_{SK}, M)||RID||Val||PK_{MID}\} >$, where CID_2 represents the certificate id of level 2, MID is the manager id, $SigAlg$ is the algorithm used to create the signature, $Sig(RTA_{SK}, M)$ is the actual signature of the RTA to authenticate the

entity, RID is the RTA id, Val is the validity of the certificate, and PK_{MID} is the public key of MID.

3) Level 1's staff sends this certificate to the RTA for verification.
4) On successful verification, level 1's staff sends the certificate, $Cert_1 =< S_1||E_{SK}\{H(S_1)\} >$, to level 2's manager.
5) Level 2's manager sends this certificate to the RTA for verification.
6) If successful, the level 2's manager grants permission to the level 1's staff to send information.

D. PRIVACY PRESERVATION AT LEVEL 2

The OEM at the depot registers with the RTA. During registration, the OEM provides their private information to the RTA. The RTA then hides and stores this information in its database. The RTA provides authentication (username/password) and confidential information (signature from the RTA). The level 2 policy (pol_2) is formed by the RTA at the depot using the credentials of the OEM as $pol_2 =< Depot_i, y : Manager > \wedge < Depot_i, y : ID > \wedge < Depot_i, y : Time > \wedge < Depot_i, y : Location > \wedge < RTA_j, y : Auth - Info > \wedge < RTA_j, y : Sig(\beta, M) >$, where $y \in \{Operation\ manager, Engineering\ manager\}$, ID represents manager identity information, β is RTA's private key, and M is the message.

To preserve the privacy of depot staff at level 2 using pol_2, the steps described in IV-C must be repeated. However, in these steps, the privacy-preserving policy must be changed from pol_1 *to* pol_2, although with the same parameters. Before level 2's manager starts sharing information such as allocated buses and crews, dispatched, and maintenance with level 3's DM, they must mutually authenticate each other using the procedure described in IV-C for level 1 staff by changing level 1 to 2, level 2 to 3, and pol_1 *to* pol_2.

E. PRIVACY PRESERVATION AT LEVEL 3

The DM, who is an agent at the depot, registers with the RTA. The private information provided by the DM to the RTA during registration is encrypted and stored in its database by the RTA. The RTA provides authentication information (username/password), confidential information (signature from RTA), and a pseudonym. The level 3 policy is formed by the RTA at the depot using the credentials of the DM as:

$pol_3 =< Depot_i, z : DM > \wedge < Depot_i, z : Time > \wedge < Depot_i, z : Location > \wedge < RTA_j, z : Auth - Info > \wedge < RTA_j, z : Sig(\beta, M) > \wedge < RTA_j, z : Pseudonym >$ where pseudonym is a pseudo-identity given by the RTA to the DM or agent using their credential data.

For preserving the privacy of the depot staff at level 3 using pol_3, the steps described in IV-C must be repeated. However, in the steps, the privacy-preserving policy must be changed from pol_1 *to* pol_3. The DM has the right to access information at levels 1 and 2. The privacy-preserved information exchange is presented in the following subsections.

F. TRANSPORT DEPOT STAFF's PUBLIC/PRIVATE DATA COLLECTION AND SHARING

In this subsection, we discuss the EI technique-based depot staff information collection, sharing, and common decision-making in a metropolitan area. Additionally, we discuss the degree of depot staff privacy preserved and disclosed in a metropolitan area.

The steps in the EI technique-based decision-making at a metropolitan area depot are as follows.

(1) Initiator depot's agent uses staff, RSUs, agents, and vehicles to form a cluster or group.
(2) The required resources are analyzed and estimated, and it is decided whether private or public information needs to be exchanged among them. The waiting time required at each depot is estimated.
(3) During emergencies, the history and analyzed information is used to estimate the resources needed, traffic jams, waiting time, etc.
(4) The information regarding the estimations is used to decide the staff' cooperative, negotiative, and competitive interaction.
(5) During these interactions, a certain degree of private and/or public information of the same or other levels of staff and depots is shared and accessed.
(6) Finally, the EI technique at the initiator depot decides (i) an accurate percentage of the type of information that must to be shared with the staff of particular depots and (ii) the revocation of malicious depot staff from the depot.

The static agent (SA) deployed at each metropolitan area depot manages the DM functions. It creates and dispatches mobile agents (MA) to the level 1 and 2 staff. These MAs collect and analyze public data of depot and private data of depot staff, and share them with the SA. The SA analyzes the information collected from a group of the depot staff and takes dynamic decisions to achieve a common goal. During decision-making, there is a possibility of the of occurrence emergency incidents or a change in the depot staff's levels. These sudden changes are incorporated into the privacy preservation scheme. This proves that the EI technique is adaptable. During adaptation, the scaling factors to disclose a certain percentage of information based on the depot staff level and type of emergency incidents are defined.

The EI technique forms groups comprising mutually authenticated depot staff. This depot staff shares information with some constraints that are defined by the EI technique based on the depot staff level, sudden occurrence of emergency events, etc. These constraints are used to define the values of scaling parameters such as α, β, γ, λ, μ, and ζ; they take values in the range of [0, 1]. Three key parameters are described in Table 3.

The EI technique uses the probabilistic model to define the extent of privacy that must be disclosed and preserved among the depot staff level. Let i, j, and k indicate APAS, OEM, and DM, respectively. The probabilistic privacy model that defines the extent of privacy preservation and disclosure

TABLE 3. Level of privacy preservation of transport depot staff.

Scaling Parameter Value	Description	Level of Privacy Preservation
1	Transport depot staff completely discloses both private and public information	0 (privacy is disclosed)
0	Transport depot staff does not disclose both private and public information	1 (complete privacy is preserved)
(0,1)	Transport depot staff partially discloses both private and public information	(0,1) (partial privacy is preserved and/or disclosed)

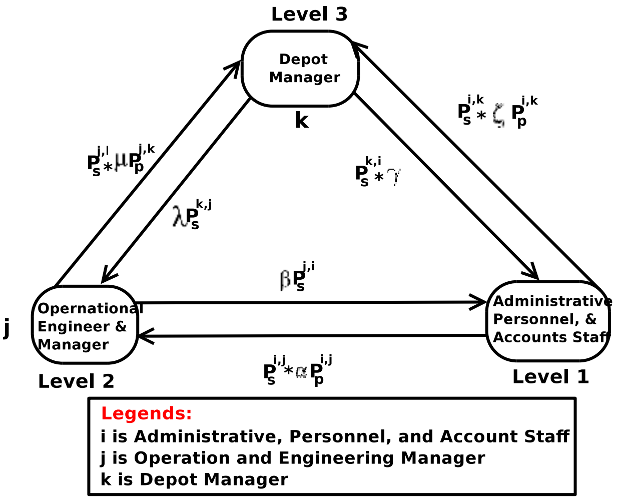

Level 3
Depot Manager
k
$P_s^{j,l} * \mu P_p^{j,k}$
$P_s^{i,k} * \zeta\, P_p^{i,k}$
$P_s^{k,i} * \gamma$
$\lambda P_s^{k,j}$
$\beta P_s^{j,i}$
j
Opernational Engineer & Manager
Administrative Personnel, & Accounts Staff
i
$P_s^{i,j} * \alpha P_p^{i,j}$
Level 2
Level 1
Legends:
i is Administrative, Personnel, and Account Staff
j is Operation and Engineering Manager
k is Depot Manager

FIGURE 6. Privacy model of depot staff.

of private and public data of the depot staff level, is shown in Figure 6.

The level i depot staff's probabilities of disclosing private and public (shareable) data to j and k are denoted as $P_d^{i,j}$ and $P_d^{i,k}$, respectively, and they are given as

$$\begin{aligned} P_d^{i,j} &= Pol_i \times Pol_j \times P_s^{i,j} \times \alpha P_p^{i,j}, \\ P_d^{i,k} &= Pol_i \times Pol_k \times P_s^{i,k} \times \zeta P_p^{i,k}, \end{aligned} \tag{2}$$

where P_s and P_p denote the public or shareable and private data of staff i, respectively.

Similarly, probabilities of not disclosing private and public data are given as follows.

$$P_{nd}^{i,j} = 1 - P_d^{i,j}, \quad P_{nd}^{i,k} = 1 - P_d^{i,k}. \tag{3}$$

The probabilities of disclosing private and public or shareable data of OEM level j to i and j to k are denoted as $P_d^{j,i}$ and $P_d^{j,k}$, respectively. They are given as follows.

$$\begin{aligned} P_d^{j,i} &= Pol_j \times Pol_i \times \beta P_s^{j,i}, \\ P_d^{j,k} &= Pol_j \times Pol_k \times P_s^{j,k} \times \mu P_p^{j,k}. \end{aligned} \tag{4}$$

Similarly, the probabilities of not disclosing private and public data are given as follows.

$$P_{nd}^{j,i} = 1 - P_d^{j,i}, \quad P_{nd}^{j,k} = 1 - P_d^{j,k}. \tag{5}$$

The probabilities of disclosing private and public or shareable data from the depot staff and DM (level k to i and k to j) are denoted as $P_d^{k,i}$ and $P_d^{k,j}$, respectively, and they are given as follows.

$$\begin{aligned} P_d^{k,i} &= Pol_k \times Pol_i \times \gamma P_s^{k,i}, \\ P_d^{k,j} &= Pol_k \times Pol_j \times \lambda P_s^{k,j}. \end{aligned} \tag{6}$$

Similarly, the probabilities of not disclosing private and public data are given as follows.

$$P_{nd}^{k,i} = 1 - P_d^{k,i}, \quad P_{nd}^{k,j} = 1 - P_d^{k,j}. \tag{7}$$

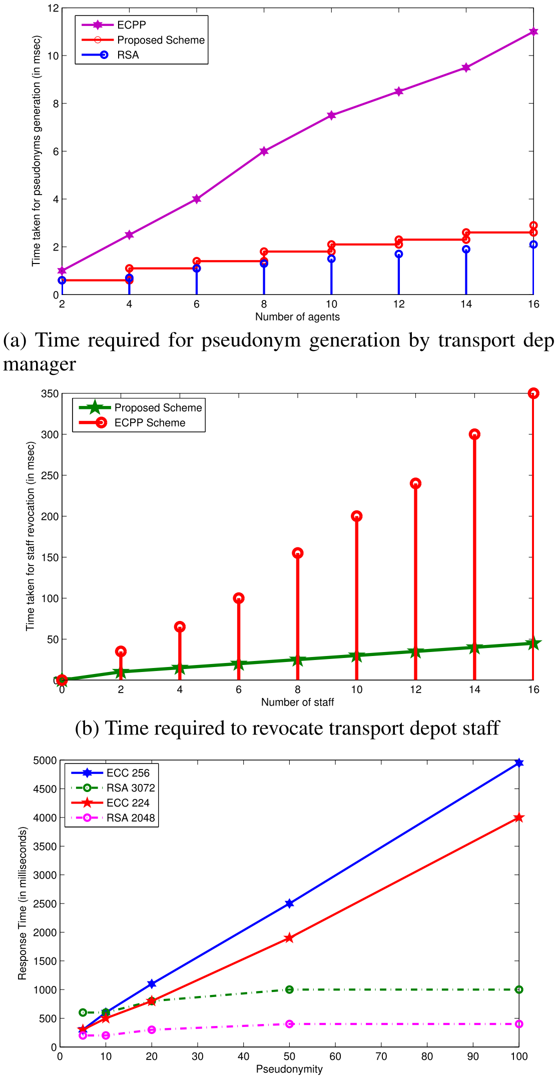
G. TRANSPORT DEPOT STAFF REVOCATION

Identification of misbehavior of legitimate staff (i.e., insiders) at a metropolitan area transport depot is considerably difficult and complex. Insiders possess the credentials and policies issued by the RTA to perform authentication and their respective functions; therefore, the misbehavior of legitimate staff needs to be revocated by revealing the confidential information.

Malicious behavior of the legitimate staff is observed during interactions by the upper, lower, and peer level staff at the metropolitan area depot. The observing staff uses their policies to identify the misbehavior of legitimate staff. It then records the misbehavior events and creates a misbehavior of legitimate staff report (MSR), i.e., $MSR = < MIS, Pol_i, ID_x >$, where MIS is the misbehavior information, Pol_i is the policy of i-th level and ID_x is the identity of misbehaving legitimate staff, x. The observing staff sends the encrypted MSR to the RTA. The RTA decrypts the message and considers the average of all the reports collected from the observing staff. Then it considers the average feedback from all and uses ID_x and Pol_i to make a decision regarding the revocation of staff x.

V. PERFORMANCE ANALYSIS

In this section, we analyze the performance of the proposed system by considering performance measures such as latency of schemes, revocation latency, response time, and execution time. The proposed scheme has been scripted and implemented in C++—we used the pairing-based cryptography (PBC) library [28] for the elliptical curve and pairing operations and the Crypto++ package [27] for implementation of the proposed schemes. The implementation was performed on a desktop computer (dual-CPU Intel Core, i5 processor) with 12 GB RAM. The performance measures' results were averaged over 500 randomized simulation runs. For the comparative analysis of the simulation results, we used the ECC and RSA algorithms. The critical sizes of ECC: 224 and RSA: 2048; and ECC: 2048 and RSA: 3078 bits provide the same security level.



(a) Time required for pseudonym generation by transport depot manager

(b) Time required to revocate transport depot staff

(c) Response time with varying number of pseudonyms

FIGURE 7. Comparison with existing schemes.

Figure 7(a) presents the comparative results of ECPP [15], RSA, and the proposed scheme. The proposed privacy preservation scheme requires lesser pseudonym generation time for the transport DM as compared to that of ECPP. RSA performs better than the proposed scheme; however, it provides a lower level of privacy than provided by the proposed scheme.

Figure 7(b) shows the time required to revocate the malicious transport depot staff in the metropolitan area. Let T_A^{IM} denote the time to identify malicious staff by neighbor staff, S, T_S^{MSR} denote the time required by S to prepare MSR, T_S^E denote the MSR encryption time required by S, T_{RSU}^D denote the MSR decryption time required by RSU, T_{RTA}^{ID} denote the time required to obtain the identity from RTA, T_{RTA}^{RL} denote the revocation list transmission time required by RTA, and T^{TTL} denote the expiry time of the generated pseudonyms. The neighborhood depot staff's agents estimate the time fields. In the simulation, the time fields count the time from the start of the process execution till the process ends. Analytically, these time fields are used to calculate the actual revocation time required to revocate the malicious behavior of the transport depot staff from the formed network. The revocation time that is denoted by T^{RL} is given as follows.

$$T^{RL} = T_S^{IM} + T_S^{MSR} + T_S^E + T_{RSU}^D + T_{RTA}^{ID} + T_{RTA}^{RL} + T^{TTL}. \quad (8)$$

TABLE 4. Notations and estimated execution time for cryptographic operations.

Symbol	Description	Execution Time
T_{mul}	Time required for 1-point multiplication in g_1	0.6 ms
T_{pair}	Time required for one pairing operation	4.5 ms
T_{xor}	Time required for XOR operation	0.7 ms
T_{canct}	Time required for concatenation operation	0.1 ms
T_{cred}	Time required for issuing credentials	3.5 ms
T_{verf}	Time required to verify the policy with staff	6.5 ms

As observed from literature, the ECPP scheme is the only scheme used to revoke nodes, and we compare the proposed scheme with it. In the proposed scheme, the RTA and RSUs in the metropolitan area require considerably lesser time than the ECPP scheme to search and revoke the agent, because the ECPP scheme requires more time for pairing and multiplication operations. Consequently, the transport depot staff privacy scheme is faster than the existing ECPP scheme.

The response time of the transport depot staff privacy scheme is shown in Fig. 7(c). To improve the response time, minimize communication delay, and minimize computational delay, we use the elliptic curve public-key cryptography (i.e., ECC) instead of the RSA cryptography. ECC can provide the same level of security as the RSA, while using a smaller key. RSA-based authentication generates considerably larger packets compared to those generated by the ECC-based authentication. The response times for different schemes for different numbers of pseudonyms and key sizes are presented in Fig. 7(c).

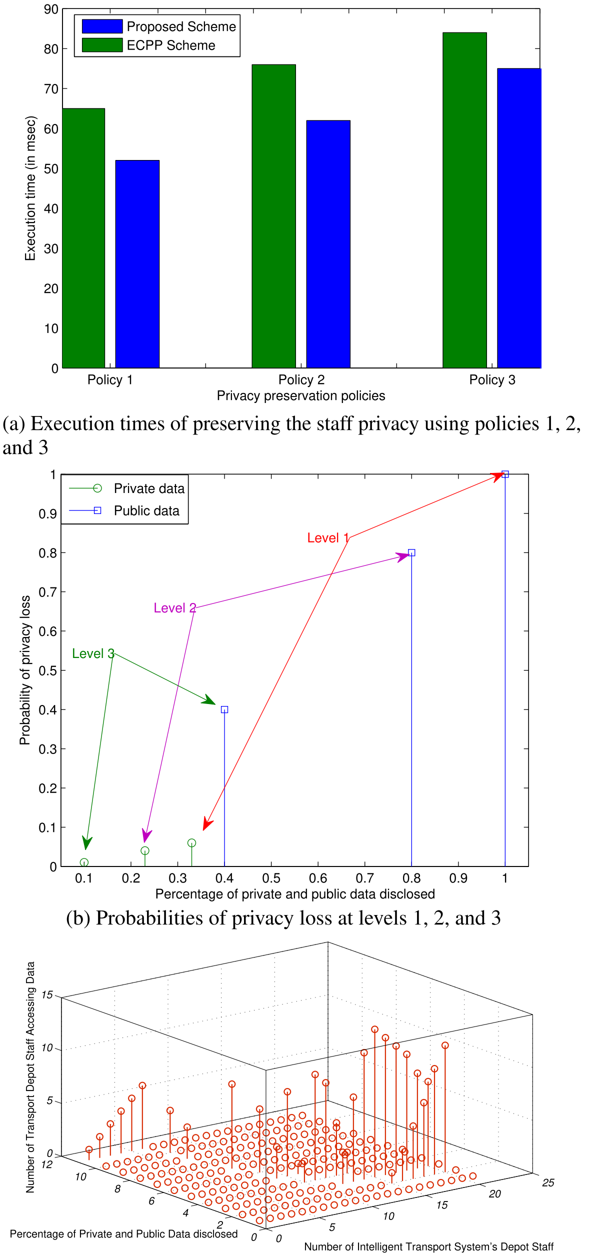
Execution time is the time required to verify the staff privacy preservation based on policies 1, 2, and 3. Table 3 lists the execution times of different cryptographic operations. Let $T_{priv}^{pol_1}$ be the execution time required to verify the privacy preservation based on policy 1, $T_{cred}^{pol_1}$ be the time required to issue staff credentials, $T_{enc}^{pol_1}$ be the time required to encrypt the message based on policy 1, $T_{dec}^{pol_1}$ be the time required to decrypt the message based on policy 1, and $T_{ver}^{pol_1}$ be the time required to verify policy 1. Table 4 presents the different cryptographic operations required during policy execution.

The $T_{priv}^{pol_1}$ is given as follows.

$$T_{priv}^{pol_1} = T_{cred}^{pol_1} + T_{enc}^{pol_1} + T_{dec}^{pol_1} + T_{ver}^{pol_1}, \quad (9)$$

where,

$$\begin{aligned} T_{enc}^{pol_1} &= T_{XOR} + T_{cant} + T_{mul} \\ &\quad + a(a_i T_{pair} + 2T_{XOR} + T_{cant}), \quad (10) \\ T_{dec}^{pol_1} &= T_{cant} \\ &\quad + a(T_{pair} + T_{XOR} + T_{XoR}^2 + T_{cant} + T_{XOR} T_{cant}). \quad (11) \end{aligned}$$



(a) Execution times of preserving the staff privacy using policies 1, 2, and 3

(b) Probabilities of privacy loss at levels 1, 2, and 3

(c) Percentages of private and public data access by transport depot staff

FIGURE 8. Comparison of execution time, privacy loss, and data access.

Similarly, the execution times required to verify the privacy preservation based on policies 2 and 3 are $T_{priv}^{pol_2}$ and $T_{priv}^{pol_3}$, respectively. They are given as follows.

$$T_{priv}^{pol_2} = T_{cred}^{pol_2} + T_{enc}^{pol_2} + T_{dec}^{pol_2} + T_{ver}^{pol_2}, \tag{12}$$

$$T_{priv}^{pol_3} = T_{cred}^{pol_3} + T_{enc}^{pol_3} + T_{dec}^{pol_3} + T_{ver}^{pol_3}. \tag{13}$$

TABLE 5. Estimated execution time of preserving the depot staff privacy for different policies.

Symbol	Description	Execution Time
$T_{priv}^{pol_1}$	Execution time of preserving the staff privacy using policy 1	52 ms
$T_{priv}^{pol_2}$	Execution time of preserving the staff privacy using policy 2	62 ms
$T_{priv}^{pol_3}$	Execution time of preserving the staff privacy using policy 3	75 ms

Table 5 shows the execution times with policies 1, 2, and 3 for preserving the metropolitan area depot staff privacy. The execution time of Policy 3 is higher than that of the others and that of the ECPP scheme, as shown in Figure 8(a). This is because of the pseudonyms of the DM, i.e., agent that periodically changes its value.

We estimate the probability of privacy loss of levels 1 to 3 with different percentages of private and public data disclosed at the metropolitan area depot as shown in Table 6.

TABLE 6. Estimation of probability of privacy loss of levels 1 to 3 with percentages of private data disclosed (P_{PDD}) and public data disclosed (P_{PuDD}).

Level	P_{PDD}	P_{PuDD}
1	0.06	1.0
2	0.04	0.8
3	0.01	0.4

Figure 8(b) shows the probability of privacy loss of different levels of depot staff with varying amounts of private and public data disclosed at the metropolitan area depot. The proposed scheme preserves the privacy of the private data of depot staff and shows flexibility with the public data. Privacy disclosure is done depending upon the depot staff levels and the type of data, i.e., private or public; this is shown in Figure 8(b). Figure 8(c) shows the percentages of the staff's private and public data disclosed and protected from other staff.

VI. CONCLUSION

In this article, we proposed a novel security and privacy management scheme for the intelligent public transportation industry in a metropolitan area. The proposed scheme provides privacy to the depot staff depending upon the policy issued by the RTA using the staff's credentials. It protects the public and private data of transport depots and staff. It outperforms the existing scheme, ECPP, on the following measures: (i) reduces the time taken for pseudonym generation (2 ms versus 11 ms of ECPP), (ii) improves revocation time of the misbehaving legitimate staff from the transport depot (40 ms versus 350 ms of ECPP), and (iii) reduced the execution time of policies 1, 2, and 3 (52 ms versus 65 ms of ECPP). The results demonstrate that the proposed scheme is a more efficient and accurate real-time implementation in a metropolitan area.

REFERENCES

[1] R. Du, C. Chen, B. Yang, N. Lu, X. Guan, and X. Shen, "Effective urban traffic monitoring by vehicular sensor networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 1, pp. 273–286, Jan. 2015.

[2] F. Qu, Z. Wu, F. Wang, and W. Cho, ''A security and privacy review of VANETs,'' *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, Dec. 2015.

[3] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, ''ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications,'' in *Proc. IEEE INFOCOM - 27th Conf. Comput. Commun.*, Phoenix, AZ, USA, Apr. 2008, pp. 1229–1237.

[4] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, ''An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications,'' *IEEE Trans. Veh. Technol.*, vol. 59, no. 7, pp. 3589–3603, Sep. 2010.

[5] J. Li, H. Lu, and M. Guizani, ''ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs,'' *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 4, pp. 938–948, Apr. 2015.

[6] I. F. Blake and P. Gadiel Seroussi Nigel Smart, *Advances in Elliptic Curve Cryptography*, vol. 317. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[7] L. Hu, Y. Qian, M. Chen, M. S. Hossain, and G. Muhammad, ''Proactive cache-based location privacy preserving for vehicle networks,'' *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 77–83, Dec. 2018.

[8] S. Chavhan, D. Gupta, C. B. N, A. Khanna, and J. J. P. C. Rodrigues, ''Agent pseudonymous authentication-based conditional privacy preservation: An emergent intelligence technique,'' *IEEE Syst. J.*, early access, Jun. 1, 2020, doi: 10.1109/JSYST.2020.2994631.

[9] Y. Qian, Y. Jiang, L. Hu, M. S. Hossain, M. Alrashoud, and M. Al-Hammadi, ''Blockchain-based privacy-aware content caching in cognitive Internet of vehicles,'' *IEEE Netw.*, vol. 34, no. 2, pp. 46–51, Mar. 2020.

[10] M. Raya, P. Papadimitratos, and J.-P. Hubaux, ''Securing vehicular communications,'' *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 8–15, Oct. 2006.

[11] S. Chavhan, D. Gupta, B. N. Chandana, A. Khanna, and J. J. P. C. Rodrigues, ''IoT-based context-aware intelligent public transport system in a metropolitan area,'' *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6023–6034, Jul. 2020.

[12] Zwierko, Aneta, and Zbigniew Kotulski, ''Mobile agents: Preserving privacy and anonymity,'' in *Intelligent Media Technology for Communicative Intelligence*. Berlin, Germany: Springer, 2005, pp. 246–258.

[13] R. Cissée and S. Albayrak, ''An agent-based approach for privacy-preserving recommender systems,'' in *Proc. 6th Int. Joint Conf. Auto. Agents Multiagent Syst.*, 2007, pp. 1–8.

[14] S. Chavhan and P. Venkataram, ''Transport management for evacuation of victims,'' *IEEE Trans. Emerg. Topics Comput. Intell.*, early access, Sep. 27, 2019, doi: 10.1109/TETCI.2019.2940832.

[15] N.-W. Lo and J.-L. Tsai, ''An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings,'' *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 5, pp. 1319–1328, May 2016.

[16] S. Garg, A. Singh, G. S. Aujla, S. Kaur, S. Batra, and N. Kumar, ''A probabilistic data structures-based anomaly detection scheme for software-defined Internet of vehicles,'' *IEEE Trans. Intell. Transp. Syst.*, 2020, doi: 10.1109/TITS.2020.2988065.

[17] Y. Qian, M. Chen, J. Chen, M. S. Hossain, and A. Alamri, ''Secure enforcement in cognitive Internet of vehicles,'' *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1242–1250, Apr. 2018.

[18] K. Lin, J. Luo, L. Hu, M. S. Hossain, and A. Ghoneim, ''Localization based on social big data analysis in the vehicular networks,'' *IEEE Trans. Ind. Informat.*, vol. 13, no. 4, pp. 1932–1940, Aug. 2017.

[19] Z. Zhou, D. Huang, and Z. Wang, ''Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption,'' *IEEE Trans. Comput.*, vol. 64, no. 1, pp. 126–138, Jan. 2015.

[20] M. Nabeel, N. Shang, and E. Bertino, ''Privacy preserving policy-based content sharing in public clouds,'' *IEEE Trans. Knowl. Data Eng.*, vol. 25, no. 11, pp. 2602–2614, Nov. 2013.

[21] A. J. Menezes, T. Okamoto, and S. A. Vanstone, ''Reducing elliptic curve logarithms to logarithms in a finite field,'' *IEEE Trans. Inf. Theory*, vol. 39, no. 5, pp. 1639–1646, Sep. 1993.

[22] *Information About Bus Depot*. Accessed: Jan. 25, 2016. [Online]. Available: http://www.ppiaf.org/sites/ppiaf.org/files/documents/toolkits/UrbanBusToolkit/assets/3/3.1/35(vii)b.html

[23] S. Chavhan and P. Venkataram, ''Emergent intelligence based QoS routing in MANET,'' *Procedia Comput. Sci.*, vol. 52, pp. 659–664, Dec. 2015.

[24] A. Yung and S. P. Moti, *Financial Cryptography and Data Security*. Berlin, Germany: Springer, 2005.

[25] L. Martin, *Introduction to Identity-Based Encryption* Norwood, MA, USA: Artech House, 2008.

[26] M. SS and S. Tangade, ''A survey on authentication schemes in VANETs for secured communication,'' *Vehicular Commun.*, vol. 5, pp. 19–30, Mar. 2017.

[27] W. Dai. *Cryptopp Library*. Accessed: Jul. 18, 2020. [Online]. Available: https://www.cryptopp.com/wiki/Linux

[28] B. Lynn. *The Pairing-Based Cryptography Library*. Accessed: Jul. 18, 2020. [Online]. Available: http://crypto.stanford.edu/pbc/

[29] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, ''VANet security challenges and solutions: A survey,'' *Veh. Commun.*, vol. 7, pp. 7–20, Jan. 2017.

[30] S. S. Karanki and M. S. Khan, ''SMMV: Secure multimedia delivery in vehicles using roadside infrastructure,'' *Veh. Commun.*, vol. 7, pp. 40–50, Jan. 2017.

[31] W. D. Hillis, ''Intelligence as an emergent behavior; Or, the songs of Eden,'' *Daedalus*, vol. 5, pp. 175–189, Oct. 1988.

[32] T. Wolf, ''Analyzing and engineering self-organizing emergent applications,'' Ph.D. dissertation, Katholieke Univ. Leuven, Leuven, Belgium, May 2007.

[33] S. Chavhan and P. Venkataram, ''Emergent intelligence: A novel computational intelligence technique to solve problems,'' in *Proc. 11th Int. Conf. Agents Artif. Intell.*, 2019, pp. 93–102.

[34] S. Chavhan and P. Venkataram, ''Emergent intelligence technique-based transport depot resource management in a metropolitan area,'' *J. Vehicle Routing Algorithms*, vol. 2, nos. 1–4, pp. 23–40, Dec. 2019.

[35] M. A. Rahman, M. S. Hossain, G. Loukas, E. Hassanain, S. S. Rahman, M. F. Alhamid, and M. Guizani, ''Blockchain-based mobile edge computing framework for secure therapy applications,'' *IEEE Access*, vol. 6, pp. 72469–72478, 2018.

SURESH CHAVHAN (Member, IEEE) received the B.E. degree from SDMCET Dharwad, in 2011, the M.Tech. degree from NIT Karnataka, Surathkal, in 2013, and the Ph.D. degree from IISc Bengaluru, India, in 2019. He is currently working as a Senior Assistant Professor with the Automotive Research Center, Vellore Institute Technology, Vellore, Tamil Nadu, India. He has published over 20 research publications in reputed International /National Journals/Conferences and a book chapter, which includes ten SCI Indexed Journals. His research interests include ad-hoc networks, autonomous and electric vehicles, smart grid computing, and intelligent transportation systems.

DEEPAK GUPTA (Member, IEEE) received the Ph.D. degree from Dr. A. P. J. Abdul Kalam Technical University. He is currently an Eminent Academician; plays versatile roles and responsibilities juggling between lectures, research, publications, consultancy, and community service. With 12 years of rich expertise in teaching and two years in the industry, he focuses on rational and practical learning. He has actively been an organizing end of various reputed International conferences. He held a postdoctoral position with Inatel, Brazil. He has authored/edited 37 books with National/International level publishers. He has published 92 research publications in reputed International Journals and Conferences, including 45 SCI Indexed Journals. He has invited as the Faculty Resource Person/Session Chair/Reviewer/TPC member in different FDP, conferences, and journals. He has served as the Editor-in-Chief, a Guest Editor, an Associate Editor in SCI, and various other reputed journals.

SAHIL GARG (Member, IEEE) received the Ph.D. degree from the Thapar Institute of Engineering and Technology, Patiala, India, in 2018. He is currently a Postdoctoral Research Fellow with the École de technologie supérieure, Université du Québec, Montreal, Canada. He has many research contributions in the area of machine learning, big data analytics, security and privacy, the Internet of Things, and cloud computing. He has over 50 publications in high-ranked journals and conferences, including more than the 25 IEEE TRANSACTIONS/journal articles. He is a member of ACM. He received the IEEE ICC Best Paper Award, Kansas City, MO, in 2018. He serves/served as the Workshop Chair/Publicity Co-Chair for the several IEEE/ACM conferences, including the IEEE INFOCOM, IEEE GLOBECOM, IEEE ICC, ACM MobiCom, and more. He serves as the Managing Editor for *Human-Centric Computing and Information Sciences* journal (Springer). He is also an Associate Editor of the IEEE NETWORK, the IEEE SYSTEMS JOURNAL, *Applied Soft Computing* (Elsevier), *Future Generation Computer Systems*, and the *International Journal of Communication Systems* (Wiley). In addition, he also serves as a Workshops and Symposia Officer of the IEEE ComSoc Emerging Technology Initiative on Aerial Communications. He has guest-edited a number of Special Issues in top-cited journals, including the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE INTERNET OF THINGS JOURNAL, the IEEE NETWORK, *Computer Networks*, and *Future Generation Computer Systems*.

ASHISH KHANNA (Member, IEEE) received the B.Tech. and M.Tech. degrees from GGSIPU, Delhi, and the Ph.D. degree from the National Institute of Technology, Kurukshetra, in March 2017. He was a Postdoctoral Fellow with the Internet of Things Laboratory, Inatel, Brazil. He has expertise in Teaching, Entrepreneurship, and Research and Development. He has around 90 accepted and published research works in reputed SCI, Scopus journals, conferences, and reputed book series, including around 40 articles in SCI-indexed journals with a cumulative impact factor of above 100. He has authored, edited, and editing 20 books. His research interests include image processing, distributed systems, and its variants (MANET, FANET, VANET, and the IoT), machine learning, evolutionary computing, and many more. He is a Series Editor of the *Intelligent Biomedical Data Analysis* series (Germany: De Gruyter).

BONG JUN CHOI (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees in electrical and electronics engineering from Yonsei University, South Korea, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Canada. He was an Assistant Professor with the Department of Computer Science, State University of New York Korea, South Korea, and a Research Assistant Professor with the Department of Computer Science, Stony Brook University, USA. He is currently an Associate Professor with the School of Computer Science and Engineering and jointly the School of Electronic Engineering, Soongsil University, Seoul, South Korea. His current research interests include energy-efficient networks, distributed mobile wireless networks, smart grid communications, and network security. He is a member of the ACM.

M. SHAMIM HOSSAIN (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Ottawa, Canada, in 2009. He is currently a Professor with the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. He is also an Adjunct Professor with the School of Electrical Engineering and Computer Science, University of Ottawa, Canada. His research interests include cloud networking, smart environment (smart city, smart health), AI, deep learning, edge computing, the Internet of Things (IoT), multimedia for health care, and multimedia big data. He has authored or coauthored more than 260 publications, including refereed journals, conference papers, books, and book chapters. He is a senior member of the ACM. He was a recipient of a number of awards, including the Best Conference Paper Award and the 2016 *ACM Transactions on Multimedia Computing, Communications, and Applications* (TOMM) Nicolas D. Georganas Best Paper Award. He has served as the Co-Chair, the General Chair, the Workshop Chair, the Publication Chair, and TPC for over 12 IEEE and ACM conferences and workshops. He is also the Co-Chair of the 3rd IEEE ICME Workshop on Multimedia Services and Tools for smart-health (MUST-SH 2020). He also co-edited a book *Connected Health in Smart Cities* (Springer). He is on the Editorial Board of the IEEE TRANSACTIONS ON MULTIMEDIA, the IEEE MULTIMEDIA, the IEEE NETWORK, the IEEE WIRELESS COMMUNICATIONS, IEEE ACCESS, the *Journal of Network and Computer Applications* (Elsevier), and the *International Journal of Multimedia Tools and Applications* (Springer). He also serves as a Lead Guest Editor for the IEEE NETWORK, the *ACM Transactions on Internet Technology*, the *ACM Transactions on Multimedia Computing, Communications, and Applications* (TOMM), and *Multimedia Systems* journal. He serves/served as a Guest Editor for the *IEEE Communications Magazine*, the IEEE NETWORK, the IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE (currently JBHI), the IEEE TRANSACTIONS ON CLOUD COMPUTING, *Future Generation Computer Systems* (Elsevier), the *International Journal of Multimedia Tools and Applications* (Springer), and *Cluster Computing* (Springer).