IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received July 13, 2016, accepted August 9, 2016, date of publication August 18, 2016, date of current version September 16, 2016.

Digital Object Identifier 10.1109/ACCESS.2016.2601442

Location-Aware Authorization Scheme for Emergency Response

HAMIDREZA GHAFGHAZI[1], (Student Member, IEEE), AMR ELMOUGY[2], HUSSEIN T. MOUFTAH[1], (Fellow, IEEE), AND CARLISLE ADAMS[1]
[1]Department of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON K1N 6N5, Canada
[2]German University in Cairo, Cairo 11432, Egypt

Corresponding author: H. Ghafghazi (hamidreza.ghafghazi@uottawa.ca)

ABSTRACT Effective emergency (such as a hurricane, a building on fire, and so on) response requires accurate, relevant, timely, and location-aware information (e.g., environmental information, health records, and so on). Acquiring information in such critical situations encounters substantial challenges, such as large volume of data processing, unstructured data, privacy, authorized data access, and so forth. Among the issues, access authorization has received little attention. Existing solutions for data authorization either do not scale well or merely consider a Break-the-Glass concept in which a master key is provided to the first responders (FRs) to decrypt the corresponding ciphertext. This may not only enable unauthorized users to access information, but it may also overwhelm FRs by the large volume of accessible data. To jointly address the aforementioned issues, this paper proposes a location-aware authorization scheme that enables FRs to access information provided that they are within a predefined distance from data owners at the time of an emergency. We innovatively integrate attribute-based encryption with broadcast encryption to incorporate dynamic attributes (i.e., location and time) into an access policy. Such attributes act as filters to eliminate data irrelevant to an ongoing emergency. As a result, our scheme provides authorized access to accurate, relevant, timely, and location-aware information. We provide extensive security analysis and performance evaluations to demonstrate the effectiveness of our scheme. The analysis shows that the scheme imposes constant communication and decryption computation overheads. Furthermore, the proposed scheme is proven chosen plain-text attack selectively secure based on $m-$bilinear Diffie–Hellman exponent assumption. It also addresses the key escrow problem.

INDEX TERMS Emergency response, access authorization, location-aware data filtering, data privacy.

I. INTRODUCTION

A key aspect of effective emergency response is information availability. The more information that is available to First Responders (FRs), the higher level of situational awareness is achievable for them [1]. Dreadful experiences such as the 7.0 magnitude Haiti earthquake in January 2010, the Boston bombing in April 2013, and the recent Paris attacks in November 2015 have shown the criticality of information [1], [2]. In this regard, after incident reports have concluded that effective emergency response requires accurate, relevant, timely, and location-aware information (e.g., environmental information, identification information, health records, last known location of endangered individuals, etc.) [2]–[5].

Unfortunately, acquiring such information encounters substantial challenges. First, there are unstructured and heterogeneous data sources, which indicates that data may be in many forms like text, photo, etc. [1], [2]. Second, there can be very large data volumes, e.g., 3.2 million tweets were sent in 24 hours after hurricane Sandy hit the US [6]. The obtained data should also be processed and filtered to become relevant information to prevent FRs from getting overwhelmed [2]. Third, unavailability of data sources because a disaster like an earthquake may destroy communication infrastructure and data centers [1], [2], [7], [8]. Fourth, invalid information may be shared in an emergency and the corresponding sources may be untrustworthy [6]. Fifth, privacy of Data Owners (DOs) whose information is collected and processed, and authorized access to such information, are essential [5]. Sixth, identification and data retrieval should be done with as low a delay as possible [2], [6]–[9].

To address some of the above challenges in the emergency response domain two main approaches can be seen in existing products and in the literature. In the first approach, data collection, processing, and dissemination are taking place during an emergency. Well-known companies like Google [10], Facebook [11], and Microsoft [12] have products that enable identifying missing people in the recent disastrous incidents. Social media has been used in risk and crisis communication [13]. Microblogs such as Twitter have been utilized by the general public and FRs to share and disseminate information during catastrophic events like the hurricane Sandy. Such information includes situation of affected area, the dynamics and progress of the situation, safety announcements, an individual's well being and location, and so forth. In [14] the authors performed an experiment in which Twitter was used to deliver a high volume of messages. The participants interact to address rumours and misinformation. The studies show that social media can improve cooperation between digital volunteers, emergency management officials, etc. [14], [15]. The credibility of information shared in Twitter for fourteen high impact events was analysed in [16]. The authors show that only 17% of the tweets comprising situational awareness information was credible. A graph-based information management system was designed to access and collect data from various social media sources to be used for emergency response [6]. The use of Twitter to broadcast information during a high impact event was studied in [17]. The use of Twitter in Tohoku earthquake was studied in [18]. The work concluded that the unreliable retweets were the main problem the users faced during the disaster. The messages in Twitter were analysed with respect to crisis coordination in [19]. The study focuses on those messages on Twitter that can be used to increase situational awareness of an emergency incident. Similar works have studied social media with respect to emergency response [20]–[22]. Most of the above studies and solutions are based on crowd-sourcing information for which data accuracy, trustworthiness, and privacy are remaining concerns.

The other approach considers foreseeing future emergencies occurrences. In this approach, the general public, autonomous organizations such as governmental organizations (GOs), non-governmental organizations (NGOs), communities, and so forth, are encouraged to outsource their information to a storage system of their choice before anything happens. Then, in an emergency, the basic sources of information would be those storage systems. As an example, the website Smart911 enables people to upload information about themselves such as their addresses, health conditions, family information, etc. [23]. When an individual calls 9-1-1, his/her information becomes available to the emergency dispatcher. This work suggests limited functionality since data access is only authorized if the caller is the one whose information is required. In [9], the registered individuals privately and confidentially outsource their information in the form of keywords to a central cloud server and mobile storage entities in their proximity area. This work increases the data availability even if an emergency vandalizes the communication infrastructure. In addition, it respects privacy and ensures accurate and reliable information is available to FRs at the time of an incident. The authors in [24] propose an information system and construct a community-based virtual database gathering heterogeneous information from various resources for emergency management. This work uses information and network resources of a community to manage emergencies. In [25], the system detects emergencies and enforces temporary access control policies. Such policies are defined in advance to bypass regular data access rules in an emergency to increase availability of information. The main disadvantage of the aforementioned works in this approach is that a DO must completely trust a server to handle his/her information.

Despite all the above efforts in the emergency response domain, three main challenges have not received enough attention: these are privacy, data access authorization, and filtering of large volume of data. In this work, we focus on the combination of the aforementioned issues and propose a location-aware access authorization scheme that enables authorized FRs to retrieve Personal Information (PI) relevant to an ongoing emergency.

In the literature, we can find two main kinds of access authorization, namely Direct Authorization (DA) and Indirect Authorization (IA). DA methods are usually used in private domains which are typically comprised of family, personal physician, friends, and neighbours, while IA is used in public domains that include researchers, healthcare personnel, other doctors, and so forth [26].

In DA, any user who is interested in an individual's information should directly contact him/her. This procedure remains the same even in an emergency. For example, in [27]–[31], upon a request from a user, the DO sends decryption keys only if the user passes the authorization check phase. Similarly, Smart911 authorizes an emergency dispatcher only when a DO calls 9-1-1 [23]. The DA approach is impractical in emergency situations for two main reasons: firstly, it does not scale well; and secondly, DOs may be unconscious or may not even be reachable to grant access to the FRs at the time of an incident.

On the other hand, IA has been used for the public domain in which DOs either delegate access authorization to a cloud server [9], [25], [32]–[36] or force access policies into an encrypted form of data using a variant of functional encryption (e.g., Attribute-based Encryption (ABE) or Predicate Encryption (PE)) upon outsourcing data [37]–[39]. In this approach, a user seeking some information, without contacting DOs, sends a request to a server, and retrieves the information. Thus, this approach scales well which makes it more suitable for emergency situations. However, considering the works [32], [33], DOs might not be comfortable with delegating the entire access rights to a server. This is because DOs will not have control over the authorization process any more. Besides, for self-authorized approaches using ABE, there has been limited work which incorporates dynamic attributes, such as location and time, into an access policy. In this regard, the common method has been to presume a fixed range of values within which such attributes are fluctuating [40].

This approach does not overcome the dynamics of an emergency where location and time of its occurrence are unknown. We further discuss this matter in Section V.

In all of the above authorization methods, the general approach to emergency modelling is the Break-the-Glass concept. The DOs (or an authority) in the system provide(s) master keys to FRs enabling them to access data once an emergency occurs [41]. For example, using ABE a DO may merely use an ''*emergency*'' attribute in the access policy and generate a ciphertext. Such a solution may enable unauthorized users to access information. In addition, it may cause FRs to become overwhelmed by the large volume of accessible data. However, access to PI should only be authorized if its owner is somehow involved in the emergency incident. The Break-the-Glass method is impotent to respect such a requirement. In addition, the Break-the-Glass method is not capable of filtering irrelevant data since lots of data verifications are required.

In this work, we take the first steps toward providing authorized data access for emergency response. We propose a location-aware authorization scheme which protects access authorization and privacy, and filters irrelevant data by taking into consideration the time and location of the ongoing emergency. This requires incorporating dynamic attributes (i.e., location and time) into the authorization scheme. To construct such a scheme, we employ Ciphertext-Policy Attribute-based Encryption (CP-ABE). Using CP-ABE, a DO is able to enforce his/her preferred access policy into ciphertext. However, movements of a DO to different locations in addition to the changes of time may result in high number of ciphertext updating messages which may make the scheme very inefficient. To tackle such an issue, we innovatively incorporate CP-ABE with Broadcast Encryption (BE). We use BE in an unconventional way to incorporate the location attribute into an access policy. In this case, we broadcast a message to a set of locations instead of individuals. On the other hand, because of the characteristics of an emergency, we delegate the time control of access authorization to a cloud server. We assume the cloud server is on-line all the time. In this case, when an emergency happens, the Public Safety Answering Point (PSAP) sends an emergency trigger message comprising the time of emergency occurrence, the time interval in which FRs' queries are considered valid, and the location area of the incident. When a cloud server receives a query, it checks the validity of the query generation time, and if it was within the allocated time interval, the server updates ciphertext accordingly and sends it to the FR. The new ciphertext is only valid for a specified time interval. As a result of the preceding approaches, a DO does not need to delegate the entire authorization process to a trusted third party server. Furthermore, integrating BE with CP-ABE to enforce the location attribute, and delegating the control on the time of access to an on-line server, decreases the frequency of ciphertext updating messages.

The proposed scheme imposes constant communication and decryption computation overhead regardless of the number of attributes in the access policy. The updating process also imposes constant communication overhead and is feasible. The scheme also addresses the key escrow problem in which the total reliance on one secret key generating authority is loosened. In addition, the scheme is CPA-selectively secure based on the Bilinear Diffie-Hellman Exponent ($m-$BDHE) intractability assumption. To the best of our knowledge, this work is the first to address such issues in such a context.

To this end, our main contributions in this work can be summarized as follows:

- We provide an extensive literature review to cover state-of-the-art CP-ABE and BE schemes and illustrate comprehensive performance comparison tables to highlight the features and vulnerabilities of existing work in an emergency.
- We propose a new emergency data access model which enables our access authorization scheme to be used as a data filtering technique. The model eliminates irrelevant data based on location and time of an emergency. Our emergency access model can also be interpreted as a new threat model which prevents unauthorized access with respect to the location and time of an emergency.
- We integrate BE with CP-ABE in a novel way and propose our Location-aware authorization scheme (LA-CP-ABE) to address the newly defined emergency data access model. Our LA-CP-ABE scheme mitigates the key escrow problem as well. In addition, the communication overhead and decryption computation complexity are constant regardless of the number of attributes in the access policy.
- We provide extensive security analysis and performance comparisons with the state-of-the-art solutions in domains other than emergency response to demonstrate the efficiency and effectiveness of the LA-CP-ABE scheme.

The remaining sections are as follows. Related work is presented in Section II. Section III introduces the preliminaries of our work. The system model, threat model, and assumptions are presented in Section IV. Challenges toward designing LA-CP-ABE are discussed in Section V. Section VI presents the LA-CP-ABE scheme. Security analysis and performance evaluation are discussed in Sections VII and VIII respectively. Section IX summarizes the paper.

II. RELATED WORK

In this section, we review ABE and BE schemes. Considering emergency response, the performance efficiency of these schemes needs thorough investigation. Furthermore, their limitations with regards to dynamic scenarios should be studied.

A. ATTRIBUTE-BASED ENCRYPTION

Attribute-based Encryption (ABE) is a relatively new authorization and public-key encryption technique which was first proposed by Sahai and Waters [54]. With ABE, an entity

TABLE 1. ABE protocol comparison.

Scheme	ABE type	Security	Access Policy expressiveness	Constant Ciphertext Size	Constant Decryption Computation	Other features
[42]	CP-ABE	Full(CPA-GG)	Tree, Shamir	×	×	Del, Rev
[43]	CP-ABE	Selective	MSP(LSSS)	×	×	-
[44]	CP-ABE	Selective	Tree, Shamir	×	×	Del
[45]	CP-ABE	Full(CPA)	Shamir	✓	×, Constant pairings	-
[46]	ABE	Full(CCA2)	MSP(LSSS)	×	×	-
[47]	Broadcast ABE	Selective	MSP(LSSS)	×	×	Rev., Del.
[48]	CP-ABE	Selective	LSSS	×	×	Multi-authority
[49]	CP-ABE	Selective	Multi-value AND-gate	✓	✓	Short secret key
[50]	CP-ABE	Full (CPA)	Multi-value AND-gate	✓	✓	Hidden policy
[51]	CP-ABE	Selective	Threshold AND-gate	✓	×, Constant pairings	-
[52]	CP-ABE	Selective	AND-gate with PNW	✓	✓	-
[53]	CP-ABE	Selective	Multi-value AND-gate	×	×	-

encrypts a message to some unknown receivers based on an access structure of his/her preference. However, the receivers are only able to decrypt the message provided that they possess a set of attributes satisfying the access policy. For example, Bob would like to share a document with certain individuals who are ''Engineer and Manager''. Note that the access policy for this example is an AND-gate. Alice has a set of attributes among which are engineer and manager. Therefore, she is able to decrypt the message from Bob. Note that any user who is able to satisfy this access policy is able to decrypt the message. Therefore, ABE is a valuable tool to provide authorization and confidentiality. There are two main types of ABE; CP-ABE [42] and Key-Policy ABE (KP-ABE) [55]. In CP-ABE, secret keys are associated with a set of attributes and ciphertext specifies the access policy. In KP-ABE, the ciphertext is associated with the set of attributes and access policy are enforced into the secret key of a user. In this work, we only focus on CP-ABE as it provides more control over who can have access to data in comparison with KP-ABE.

We categorize CP-ABE schemes based on various access policies. The first sub-category is comprised of schemes which offer flexible and expressive access policies. Here, the schemes rely on monotone access tree structure supporting AND-gate, OR-gate, and threshold [43]. These schemes use a secret sharing scheme such as Shamir's secret sharing [42], [44], [45]. In addition, some schemes utilize Linear Secret Sharing Scheme (LSSS) facilitating the conversion of any boolean formula into an LSSS representation (i.e., Monotone Span Program (MSP)) [43], [46]–[48]. In both cases, the encrypting party chooses a secret and shares it among the attributes in the access policy following the secret sharing paradigm and generates ciphertext. The ciphertext size in these schemes grows linearly with the number of attributes in the access policy. In addition, the computation complexity for the decryption process in such schemes depends on the number of attributes satisfying the access policy. Therefore, it can be seen that there is a trade-off between expressiveness of an access policy and efficiency of the scheme in terms of communication overhead, computation complexity, and delay. The more expressive an access policy is, the less efficient the CP-ABE scheme becomes.

On the other hand, the second sub-category is comprised of protocols with lower flexibility and expressiveness for the access policy. In theses schemes, the access policy does not support OR-gates in particular. Here, the schemes support AND-gates access structure and threshold access structure [49]–[52]. The attributes may have a single positive value, both positive and negative values, or multiple values (e.g., $+1$, -1, $(2, 3, -5, \ldots)$ respectively). In addition, some schemes provide wildcards in the access structure which means that an attribute can have any value in its allowed range. There are schemes in this group where the ciphertext size depends on the number of attributes in an access policy [53]. However, the majority of the schemes have constant ciphertext size regardless of the number of attributes in the access policy. In addition, large number of constructions offer constant decryption computations. In this case, it is particularly important to have a constant number of pairing operations as this is the dominant factor of computation complexity and delay. Constant communication and computation costs are attractive to critical applications in which resources are constrained and low delay is of significance.

Emergency situations are highly dynamic in which the time and location of data access are varied. Therefore, such dynamic features make the use of CP-ABE complicated. To the best of our knowledge, a concrete CP-ABE scheme that incorporates dynamic attributes into the ciphertext has not yet emerged. We will elaborate corresponding challenges and requirements in details in Section V. On the other hand, CP-ABE schemes need a Trusted Authority (TA) to compute the secret keys. In this case, the problem of key escrow rises in which the TA is able to decrypt every encrypted document. Our proposed scheme mitigates such an issue. Table 1 shows different features of CP-ABE schemes. In Table 1, Del means delegation of secret keys, Rev means revocation of users or attributes, and PNW means positive negative wildcard.

B. BROADCAST ENCRYPTION

Broadcast Encryption (BE) enables a broadcaster to encrypt a message for some subset S of users in a system with a total of n' users. In this regard, any user in S uses his private key to decrypt the ciphertext. However, users outside of S cannot learn any information from the ciphertext and cannot collude with each other to decrypt the message. Such a feature makes a BE scheme collusion resistant. Applications of BE are several such as key distribution and secure distribution of copyright media [56]–[59].

In BE, it is preferable that the following features are achieved: the system is public key which means that anyone can broadcast ciphertext; receivers are stateless which means that they do not need to update their private keys; and a BE is collusion resistant against all users outside the selected set S [60]. Note that BE schemes constitute two main parts. One part uses a group secret key as an input to a symmetric encryption scheme such as AES, and encrypts the message with that. The other part is the actual BE scheme which is a public key scheme to broadcast the group secret key. Then, receivers decrypt the BE message (i.e., the group secret key) first, then use that as the input to the symmetric encryption scheme to decrypt the actual message.

Fiat *et al.* proposed the first formal BE with $O(t\log^2 t \log n')$ ciphertext-size where n' is the total number of users in the system and t is the threshold that guarantees the collusion resistance of the scheme [61]. Naor *et al.* proposed a fully collusion resistant BE scheme [62]. The scheme broadcasts a message to all users except a small set r' of revoked ones. The ciphertext size of the scheme is proportional to $O(r')$, but the private keys are of size $O(\log^2 n')$. The works in [63] and [64] decreased the private key size of the scheme to $O(\log n')$. Selvi *et al.* also proposed a fully collusion resistant BE scheme [65]. In such works [62]–[65], the ciphertext size grows linearly with the size of the receivers set (i.e, $|S|$), or the number of revoked users $|r'|$. However, Boneh *et al.* proposed two fully collusion resistant BE schemes [66]. The size of the ciphertext in the first construction is constant and for the second one is $O(\sqrt{n'})$. The scheme applies bilinear maps to achieve the ciphertext size for both schemes. However, the scheme is based on the selective security model in which the security proof is done with a prior step called initialization. In such a step, an adversary chooses the target set, $\widehat{S} \subseteq S$, corresponding to his/her challenge ciphertext. Similarly, Gentry and Waters [60] proposed a BE scheme which is secure against an adaptive attacker meaning that the attacker can send any set $\widehat{S}$ of challenge ciphertext and the initialization step is eliminated from the proof. Delerablée *et al.* proposed a dynamic BE scheme in which there is a Join operation that alters public keys to address such dynamicity [67]. The ciphertext-size and private key size of the scheme are constant. Boneh *et al.* proposed another fully collusion resistant BE scheme which has $O(\lambda\sqrt{n'})$ ciphertext-size where λ is the security parameter [68].

TABLE 2. BE Protocol Comparison.

Scheme	Communication overhead	Computation complexity	Security
[62]	$O(r')$	$O(\log n')$	FCR
[63]	$O(r')$	$O(\log n')$	FCR
[64]	$O(r')$	$O(n')$	FCR
[65]	$(S+4)\lvert G_1\rvert$	$2\tau_e + S\tau_g$	FCR, Adaptive
$[66]_{1,2}$	$\{2\lvert G\rvert\}_1, \{O(\sqrt{n'})\}_2$	$2\tau_e + S\tau_g$	FCR, Static
[67]	$\lvert G_1\rvert + \lvert G_2\rvert$	$2\tau_e + r\tau_g$	FCR, Static
[60]	$2G_1$	$2\tau_e + S\tau_g$	FCR, Adaptive
[68]	$O(\sqrt{n'})$	$4\tau_e + \lvert S+1\rvert\tau_g$	FCR, Adaptive

Considering an emergency, the communication overhead and computation complexity of BE schemes should satisfy the requirements of an emergency. Table 2 summarizes the aforementioned BE schemes. In this table, FCR means Full Collusion Resistant, τ_e and τ_g represent the number of pairing computation and group arithmetic operations respectively and are the dominating sources of computation delay. For communication overhead, we merely show the elements that are the points of difference in varied schemes. In other words, we neglected the ciphertext element representing the output of a symmetric encryption scheme.

III. PRELIMINARIES

In this section, we provide the details about the underlying tools and algorithms that are used in our system. In addition, the intractability assumption of our LA-CP-ABE scheme is explained.

A. COMPOSITE-ORDER BILINEAR GROUPS

We construct our LA-CP-ABE scheme using composite-order bilinear groups [46]. A group generator function $\mathcal{G}$ takes as input the security parameter λ and outputs a description of a bilinear group $\mathbb{G}$. We define $\mathcal{G}$'s output as $(N, \mathbb{G}, \mathbb{G}_T, e)$, where $N = pr$ is a product of two distinct primes (p and r), $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic groups of order N, and $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is a map that is

1) Bilinear: $\forall g, h \in \mathbb{G},\ a, b \in \mathbb{Z}_N, e(g^a, h^b) = e(g, h)^{ab}$
2) Non-degenerate: $\exists g \in \mathbb{G}$ such that $e(g, g)$ has order N in $\mathbb{G}_T$.

We assume that the group operations in both $\mathbb{G}$ and $\mathbb{G}_T$ and the bilinear pairing map e are computable in polynomial time with respect to λ. Suppose that G_p and G_r are the subgroups of order p and r, respectively. In a composite-order bilinear group, there exists an orthogonality property as follows: if $h \in G_p$ and $h' \in G_r$, $e(h, h') = 1_T$ where 1_T is the identity element in $\mathbb{G}_T$. To show this, suppose g is a generator of group $\mathbb{G}$. Then, g^p generates G_r and g^r generates G_p. Therefore, suppose for some x, y, $h = (g^x)^r$ and $h' = (g^y)^p$. Then,

$$e(h, h') = e(g^{xr}, g^{yp}) = e(g^x, g^y)^{pr} = 1. \tag{1}$$

B. ANONYMOUS KEY AGREEMENT

An anonymous one-way key agreement is proposed in [69] using bilinear maps. The algorithm guarantees sender-side

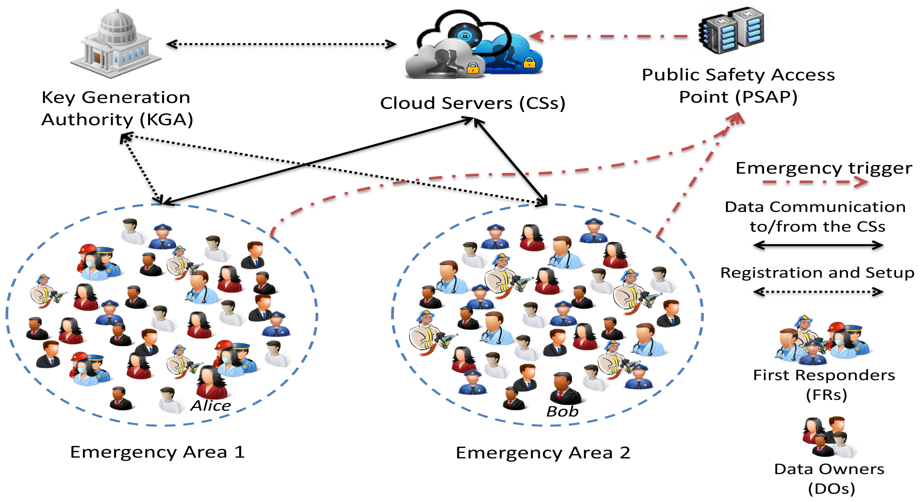

FIGURE 1. System model.

anonymity as a result of non-interactive key agreement. Considering our application, this is an important feature because preserving privacy of an FR actions (i.e., data requests) from the cloud server requires that the linkage between the identity of the FR and his/her actions is broken [5]. This linkage can be broken by hiding the identity of the FR. Sender-side anonymity also can protect DOs privacy. This is because the identity/role of an FR (e.g., Bob/Policeman) may reveal some information about a DO.

In most of one-way anonymous communications, authenticating a non-anonymous server is needed. Here, using this algorithm, the shared key is implicitly authenticated. In other words, the sender is assured that only the server can compute the key. Suppose there is a cryptographic hash function $H : \{0, 1\}^* \rightarrow \mathbb{G}$. An authority generates a master secret key s, uses a public identity of a recipient $ID_{\mathbb{B}}$ along with the sender's private key $SK_{\mathbb{A}} = Q_{\mathbb{A}}^s = H(ID_{\mathbb{A}})^s \in \mathbb{G}$, and generates a session key as follows:

1) Sender $\mathbb{A}$ computes $Q_{\mathbb{B}} = H(ID_{\mathbb{B}}) \in \mathbb{G}$. $\mathbb{A}$ chooses a random number $\alpha \in \mathbb{Z}_P$ where P is the order of $\mathbb{G}$, and generates the pseudonym $P_{\mathbb{A}} = Q_{\mathbb{A}}^{\alpha}$ and sends it to the receiver $\mathbb{B}$. Then, $\mathbb{A}$ generates the session key $k = e(Q_{\mathbb{B}}, SK_{\mathbb{A}})^{\alpha} = e(Q_{\mathbb{B}}, Q_{\mathbb{A}})^{s\alpha}$.
2) Recipient $\mathbb{B}$ computes the session key using $SK_{\mathbb{B}} = H(ID_{\mathbb{B}})^s$ as follows,
$k = e(P_{\mathbb{A}}, SK_{\mathbb{B}}) = e(Q_{\mathbb{A}}, Q_{\mathbb{B}})^{s\alpha}$.

C. COMPLEXITY ASSUMPTION

The complexity assumptions for our system are based on decisional Bilinear Diffie-Hellman Exponent assumption (BDHE). Recall that $\mathbb{G}$ is a bilinear group of composite-order N. The $m-$BDHE problem in $\mathbb{G}$ takes $(h, g, g^a, g^{(a^2)}, \ldots, g^{(a^m)}, g^{(a^{m+2})}, \ldots, g^{(a^{2m})}) \in \mathbb{G}^{2m+1}$, as input and outputs $e(g, h)^{(a^{m+1})} \in \mathbb{G}_T$. Suppose, $g_i = g^{(a^i)} \in \mathbb{G}$. We say an algorithm A has advantage ϵ in solving $m-$BDHE in $\mathbb{G}$ if $\Pr[\mathcal{A}(h, g, g_1, \ldots, g_m, g_{m+2}, \ldots, g_{2m}) = e(g_{m+1}, h)] \geq \epsilon$, where the probability is over the random choice of generator g in $\mathbb{G}$, the random choice of h in $\mathbb{G}$, the random choice of a in $\mathbb{Z}_N$, and the random bits used by $\mathcal{A}$.

IV. SYSTEM MODEL AND THREAT MODEL

It is assumed that a city is divided into n distinct zones with equal areas, each having a unique pseudo-identity L_{id}. We choose a cloud server storage model to maintain data and perform data updating procedure. The system is comprised of several entities as follows.

Key Generation Authority (KGA): This entity generates the secret keys of the system and performs the setup algorithm. It is assumed that there are two separate KGAs; one is for location and time attributes, and the other is for the rest of the attributes, introduced in Section VI.

Public Safety Answering Point (PSAP): This entity receives an emergency signal including 9-1-1 calls and sensor signals (e.g., smoke detectors, heat detectors and so forth), and triggers the cloud servers and FRs accordingly.

Cloud Server (CS): We assume that there is a central cloud server which stores all encrypted PI.

DO: This entity is a member of the general public who registers to the system by communicating with KGAs and uploads his/her encrypted PI to the CS.

FRs: These are the governmental authorities including policemen, fire fighters, and paramedics. They also will register to the system by communicating to the KGAs and receive the system parameters and their secret keys.

As depicted in Fig 1, there is an area (e.g., Emergency Area 2) in which an emergency incident has occurred. Note that before an incident happens and during normal conditions, those DOs who have registered to the system outsource their encrypted PI to the CS. The goal of this work is to provide authorized access to location-aware data for FRs. It is assumed that an agent is equipped with a smartphone which has a tamper proof GPS. Such a tool has secure components to perform simple calculations and secure storage [70], [71]. The user cannot access the secure component of GPS and it is assumed that GPS performs honestly. The communication between the users in the system and KGAs/CS can be facilitated using WiFi, 2G, 3G, etc.

We assume that KGAs are fully trusted, but the CS is honest but curious. This means that the CS follows the procedure of the scheme in an honest way, but tries to learn as much information as possible. We assume that KGAs authenticate DOs and FRs and only then it transfers secret keys to those entities. The authentication procedure is out of the scope of this work, but it can also be provided using well-known methods [72]–[74]. We also assume that there exists eavesdropper adversaries who live among the general public and would like to learn as much information as possible.

In this work, a data access model is also proposed. Since any emergency is related to a location and occurs at a certain time, our model enables authorized access to victims' information at the time of an emergency from a predefined distance to the emergency scene. This model ensures the data access is authorized, a DO is involved in an emergency, and at the same time filters irrelevant information that is available to FRs. Consider Fig 1: the information of Bob who is located in Emergency Area 2 may not be useful for an FR who is located inside Emergency Area 1. This way the level of data accuracy and relevance to an emergency increases.

Finally, considering our access model as a threat model, if a user is in location area L_i at time τ_t, she/he is not able to access a DO's data if the DO is located in $L_{i'}$ for $i \neq i'$. In addition, the generated key for the L_i and τ_t is invalid for the same location at time $\tau_{t+t'}$ at which the DO is not located any more. This provides higher level of privacy protection than the Break-the-Glass approach. We will further elaborate our model for incorporating location areas into our scheme in Section VI where we will demonstrate that the proposed access model is flexible and does not prevent authorized users from accessing information when required.

V. CHALLENGES TOWARD DESIGNING LOCATION-AWARE CP-ABE SCHEMES

Effective emergency response requires that communication overhead, and computation complexity/delay of the authorization scheme, be sufficiently small that authorized data access is facilitated. Therefore, constant ciphertext-size CP-ABE schemes with constant computation complexity are suitable choices for authorization. Here, we sacrifice the flexibility and expressiveness of an access policy for the sake of better performance. However, incorporating dynamic attributes (i.e., location and time) into an access policy of this particular kind of CP-ABE is challenging. In this section, we will elaborate the corresponding challenges with regards to both DOs (as ciphertext generators) and FRs (as data consumers).

From a DO's perspective, there are three natural ways to include dynamic attributes into ciphertext. First, a DO could trivially predict the time/location and include them into ciphertext in the first place. This may sound easy as there are limited locations that a DO may visit per day. However, the DO may become anxious since she/he has to follow the predicted schedule. Furthermore, only one out of many choices of location and time attributes would be legitimate at any instance. In this case, the proper access policy category that would fit the preceding approach is $(t, n)-$threshold. However, it is a complex task to combine both dynamic and static attributes into an access policy. This is because out of t attributes, 2 have to be specified for location and time and $t-2$ for the rest of the attributes. Therefore, an FR possessing t matching attributes excluding location and time may still be able to decrypt the message.

The second way of including dynamic attributes into an access policy is that a DO updates the ciphertext every time that she/he moves to another location or after the expiration of a time interval. The cost of such an approach grows linearly with the number of visited locations per day and number of time intervals set by the system. Besides, a DO may visit some similar locations several times a day in different time intervals which makes the updating process very inefficient. Note that a DO can delegate such a process to a smartphone in order to automate the process. Another drawback is the fact that in an emergency, a DO may be unconscious or the smartphone may be broken or lost which may render the updating process incomplete. Therefore, utter reliance on a DO has its own risks.

The third way is to delegate the entire updating process to the CS. This can be done in two ways: one, the CS decrypts the data and re-encrypts it using updated attributes; two, the CS privately updates the data using privacy-preserving proxy re-encryption techniques [75]–[77] in which decryption is not necessary. The first way poses breach of privacy since the CS can access plain data. For the second way, although the CS may not be able to access plain data, DOs may not still want to trust the CS entirely with such a process. In general, total delegation of authorization process requires ultimate trust to a server.

The aforementioned trivial ways are either infeasible, costly, inefficient, or require ultimate trust on a third party. Despite those ways, here, we propose a feasible and efficient way to incorporate dynamic attributes into an access policy. We delegate time of access authorization to the CS and the authorization for location and static attributes is enforced by DOs. To incorporate time of access, the CS checks the validity of a data request and then updates the ciphertext accordingly or rejects the request. Location authorization will be done by DOs. A DO will choose a set of preferred locations (that can be the most frequent locations in, e.g., a week such as *Home, School, Work place, Grocery store, etc.*) for which he generates ciphertext. Note that a DO does not need to predict the time at which he/she visits location areas in the preferred set. Using this technique relieves the DO from unnecessary updating process every time he visits some common location which results in the decrease in the computation and communication overheads. It is worth mentioning that a DO still can update the ciphertext very efficiently if he moves out of all the locations in the preferred set. To implement this, we integrate BE with CP-ABE. In our scheme, BE is used unconventionally for locations instead of individuals. Each location has a unique ID. A sender broadcasts his/her data to n locations and an FR in one of those locations can decrypt data using his/her private key. Therefore, BE results in a $(1, n)-$threshold access structure.

From an FR's perspective, the challenge is to provide the FRs with proper secret keys corresponding to the dynamic attributes. Recall that BE schemes are preferred to be stateless meaning that the private keys should remain unchanged. However, updating ciphertext with new locations and time requires freshly generated private keys corresponding to those attributes. This introduces a contradiction between static BE private keys and the dynamic feature of location-awareness. There are two main options to overcome such a challenge. First, an FR sends a key updating request to a KGA specified for those dynamic attributes every time that she/he wants to decrypt data. Here, the KGA may become a single point of failure. Second, an FR can securely generate proper secret keys. This requires a tamper proof device [78], [79].

VI. LOCATION-AWARE CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTION

Let us dive into the implementation of the LA-CP-ABE scheme. Here, we elaborate the location area model first, and then the construction of the scheme is presented. In the proposed scheme, DOs choose a set of location areas called *preferred location set*, S'', from the set of all possible location areas $\mathbb{L}$. S'' consists of a collection of location areas that a DO frequently visits such as *Home, School, Work place, Grocery store, etc.*

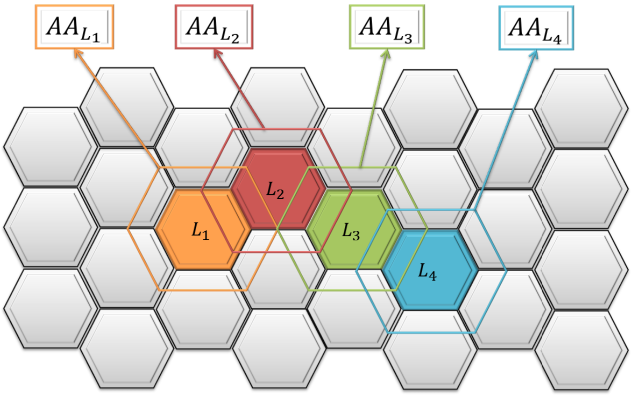

FIGURE 2. **Location Area Model.**

Since it is desirable for FRs to be able to access data before they arrive at the location scene (area) of an emergency, for each location area L_a, we define an *Associated Area* AA_{L_a} as depicted in Fig 2. Note that the hexagons used in Fig 2 are just for illustration purposes and do not mean that we assume a cellular network communication infrastructure. The task of updating the ciphertext with new location areas is delegated to the DO's smartphone to automate the process. For instance, when a DO is in L_1, the AA_{L_1} has been incorporated to the ciphertext. In other words, a DO updates his/her ciphertext based on the boundaries of L_1, but an FR can have access to his/her data based on the wider boundaries of AA_{L_1}.

The diameter of an associated area could be chosen in a way that the distance to the target location area gives the FRs sufficient time to retrieve the information before arriving at the scene. Here, there is a trade-off between privacy preservation, access authorization and data availability which depends on the drive time from the boundaries of a associated area to the emergency scene, geographical terrain of the area (e.g., urban area or rural area), data communication availability/reliability in that area, and so forth. Optimizing this diameter value is an interesting problem; however, it is out of the scope of this work.

Fig 2 also illustrates the trajectory of a DO from L_1 to L_2, then to L_3, and finally to L_4. For each change of a location, a DO needs only to remove/add one location area from/to the ciphertext. The proposed scheme does not need to regenerate the entire ciphertext when a DO changes his/her location. The scheme merely updates the original ciphertext by multiplying it with one group element by either adding or removing an attribute (refer to subsection VI-B for more details). This is done with minimum communication overhead and low computation complexity. However, if the change of a location is among the ones in the S'', there is no need for ciphertext updating.

A. CONSTRUCTION

We used [60] to construct the proposed LA-CP-ABE scheme. Let $\mathcal{G}$ be an algorithm that, on input security parameter λ, generates two groups of composite-order $N = pr$ with bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$. Let $H_K : \{0, 1\}^* \rightarrow \mathbb{Z}_N$ be a keyed hash function and $H_1 : \{0, 1\}^* \rightarrow \mathbb{G}$ a cryptographic hash function. Also, let $\mathbb{L} = \{L_1, L_2, \ldots, L_n\}$ be a set of all location areas; $U = \{A_0, A_1, A_2, \ldots, A_l\}$ be a universe of attributes where $|U| = l + 1$; $V_i = \{v_{i,1}, v_{i,2}, \ldots, v_{i,a_i}\}$ be a set of all possible values for attribute $i \in [1, l]$ and $a_i = |V_i|$; $W_{FR_u} = \{A_0, W_1, W_2, \ldots, W_\varrho\}$ is the attribute list of the FR_u where $W_i \in V_i$ and $\varrho + 1 = |W_{FR_u}| \leq |U|$. We assume A_0 is a default attribute shared among all users of the system. We assume that KGA_1 generates the parameters for the static attributes, and KGA_2 generates the parameters for the location attribute. In this case, $\mathcal{G}(\lambda)$ is run jointly by the two authorities. This means that KGA_1 and KGA_2 get the same description of $(\mathbb{G}, \mathbb{G}_T, e)$.

Setup $(\lambda, \mathbb{L}, (U, V))$*:* This algorithm is done by KGA_1 and KGA_2. In the following, $\overset{R}{\leftarrow}$ and $\in_R$ mean elements are assigned/chosen randomly from a group. For KGA_1, it takes as input λ and (U, V). It chooses a generator $g_1 \in G_p$, $q, R, \Lambda \overset{R}{\leftarrow} G_p$, and $\alpha, t_{i,j} \in_R \mathbb{Z}_N$ with $i \in [1, l]$,

$j \in [1, a_i]$. Note that Λ corresponds to A_0. KGA_1 computes $Y_0 = e(g_1, q)^{\alpha}$, $Y_2 = e(R, R)$, and $T_{i,j} = g_1^{t_{i,j}}$ for $\forall i, j$.

For KGA_2, it takes as input the security parameter λ, and the location set $\mathbb{L}$. It sets $\alpha', \beta, x \in_R \mathbb{Z}_N$, chooses a generator $g_2 \in G_r$, and $h_0, h_1, h_2, \ldots, h_n \overset{R}{\leftarrow} G_r^{n+1}$, where h_0 is a default parameter shared among all entities in the system, and h_i for $i \in [1, n]$ represents the AA_{L_i}. KGA_2 computes $Y_1 = e(g_2, g_2)^{\alpha'}$.

Finally, the public parameters PK includes a description of $(\mathbb{G}, \mathbb{G}_T, e)$ as well as

$$PK \leftarrow \left\{ \begin{array}{l} g_1, q, R, \Lambda, Y_0, Y_2, \{T_{i,j}\}_{i \in [1,l], j \in [1,a_i]}, \\ g_2, Y_1, h_0, h_1, \ldots, h_n \end{array} \right\}$$

and $MSK = \{q^{\alpha}, g_2^{\alpha'}, \beta, x, \{t_{i,j}\}_{i \in [1,l], j \in [1,a_i]}\}$ is the set of private parameters where x is the master secret key allocated to the CS. Setup outputs (PK, MSK).

Key Generation (PK, MSK, S, W_{FR_u})*:* This algorithm is done by the KGAs. It takes PK, MSK as input for both authorities. However, for KGA_2, it takes another input parameter which is a set of authorized location areas with their corresponding associated areas, S where $|S| \leq \mathbb{L}$ for an FR_u or a group of FRs, and for KGA_1 it takes the set of attributes of the user W_{FR_u}. KGA_1 picks $r'_u \in_R \mathbb{Z}_N$, and KGA_2 picks $r_u \in_R \mathbb{Z}_N$. Finally, they output the user's secret key

$$SK_u = \begin{cases} SK_0 = H_1(FR_u)^{\beta}, \\ SK_1 = q^{\alpha} \Lambda^{r'_u}, \\ SK_2 = g_1^{-r'_u}, \\ SK_3 = g_2^{-r_u}, \\ SK_4 = R^x h_0^{r_u} g_2^{\alpha'}, \\ SK_{i,j} = T_{i,j}^{r'_u} & \forall v_{i,j} \in W_{FR_u}, \\ SK'_{j1} = h_{j1}^{r_u} & \forall j1 \in \{n\} \setminus \{S\}, \\ SK''_{j2} = h_{j2}^{r_u} & \forall j2 \in \{S\}, \end{cases}$$

and gives SK_u to the FR_u. Note that SK_0, SK_4, and SK''_{j2} will be securely transferred to the GPS component of the user's smartphone. The GPS also receives S.

Encrypt (PK, M, D, S')*:* A DO chooses $s, t \in_R \mathbb{Z}_N$, $D = \{D_1, D_2, \ldots, D_{l'}\}$ as an access structure where $D_i \in V_i$ and $|l'| \leq |l|$, $S' = L_c \bigcup S''$ where L_c is the current location (if $L_c \in S''$ then $S' = S''$), The message M (which is comprised of the DO's health record, emergency information, etc.), and computes

$$K = Y_0^s \times Y_1^t \tag{2}$$

$$C = \begin{cases} D, S', \\ C_0 = \xi'_K(M), \\ C_1 = g_1^s, \\ C_2 = g_2^t, \\ C_3 = (\Lambda \prod_{v_{i,j} \in D} T_{i,j})^s \times (h_0 \prod_{j \in S'} h_j)^t, \end{cases}$$

where ξ' is a symmetric encryption scheme (e.g. AES). The DO outsources C to the CS. Note that for all distinct access structures $\forall D, D'$, $\sum_{v_{i,j} \in D} t_{i,j} \neq \sum_{v_{i,j} \in D'} t_{i,j}$ is assumed.

Key-Agreement (L_E, CS_{id}, r)*:* This algorithm is done by the GPS component of an FR's device. It takes as input the location of an emergency L_E, the identity of the CS and $r \in_R \mathbb{Z}_N$. GPS checks if the location of the FR is in AA_{L_E}. If the check is passed, it generates a pseudonym $\theta = Q_{FR_u}^r$, and a one-way session key as in (3).

$$k = e(Q_{FR_u}, Q_{CS})^{r\beta} \tag{3}$$

GPS sends back $\{\theta || \xi'_k(L_{id} || E'_t || \eta)\}$ to the FR where $\eta \in_R \mathbb{Z}_N$ is a random nonce and E'_t is the current time. The GPS stores k, L_{id}, η, E'_t.

CS-Encrypt $(C_1, L_{id}, \tau_t, PK, x)$*:* The CS receives an emergency trigger message from PSAP as $E_{Trigger} = \{L_E || E_t || \tau_t\}$ where E_t is the emergency occurrence time, and τ_t is the time interval within which FRs' data requests are valid. The CS also receives a request from an FR consisting of $\{\theta || \xi'_k(L_{id} || E'_t || \eta)\}$ from which the server uses θ to generate the shared key k and decrypts $\xi'_k(L_{id} || E'_t || \eta)$. The CS checks if $E'_t \in \tau_t$ and retrieves data. Note that time intervals could be defined by the authorities considering the maximum response time of FRs. Afterwards, the CS checks whether $L_{id} \bigcap S' \neq \emptyset$. If the check is passed, the CS modifies C_1 in order to incorporate the time attribute to the ciphertext as

$$C'_2 = g_2^t \times R^{1/(x + H_k(L_{id} || \tau_t || \eta))}. \tag{4}$$

The CS sends back to the FR the new ciphertext $C_{new} = (S', D, C_0, C_1, C'_2, C_3)$.

GPS-KGen (SK_4, PK, S', τ_t)*:* This algorithm is done by the GPS component. The user sends S' and τ_t to the GPS. The GPS will check whether $S \bigcap S' \neq \emptyset$ and $E'_t \in \tau_t$. If the checks are passed, the GPS picks the corresponding $h_j^{r_i}, \forall j \in S \bigcap S'$, and generates a one-time key.

$$SK'_4 = R^{H_k(L_{id} || \tau_t || \eta)} \times R^x h_0^{r_u} g_2^{\alpha'} \prod_{j \in \{S \bigcap S'\}} h_j^{r_u}, \tag{5}$$

and sends it to the user. Note that in the time interval τ_t, the shared key k is valid. Here, for every new S', the GPS generates a new $\eta_{new} = H_k(\eta_{old})$. This changes the value of SK'_4 for the new S'.

Decrypt (PK, C, SK_u, S', S, D)*:* The user extracts K as follows,

$$K = \frac{K' \times K''}{e(R, R)}, \tag{6}$$

$$K' = e\Big(C_1, SK_1 \times \prod_{v_{i,j} \in D} SK_{i,j}\Big) \times e\Big(C_3, SK_2\Big), \tag{7}$$

$$K'' = e\Big(SK'_4 \times \prod_{j_1 \in S'} SK'_{j_1}, C'_2\Big) \times e\Big(SK_3, C_3\Big). \tag{8}$$

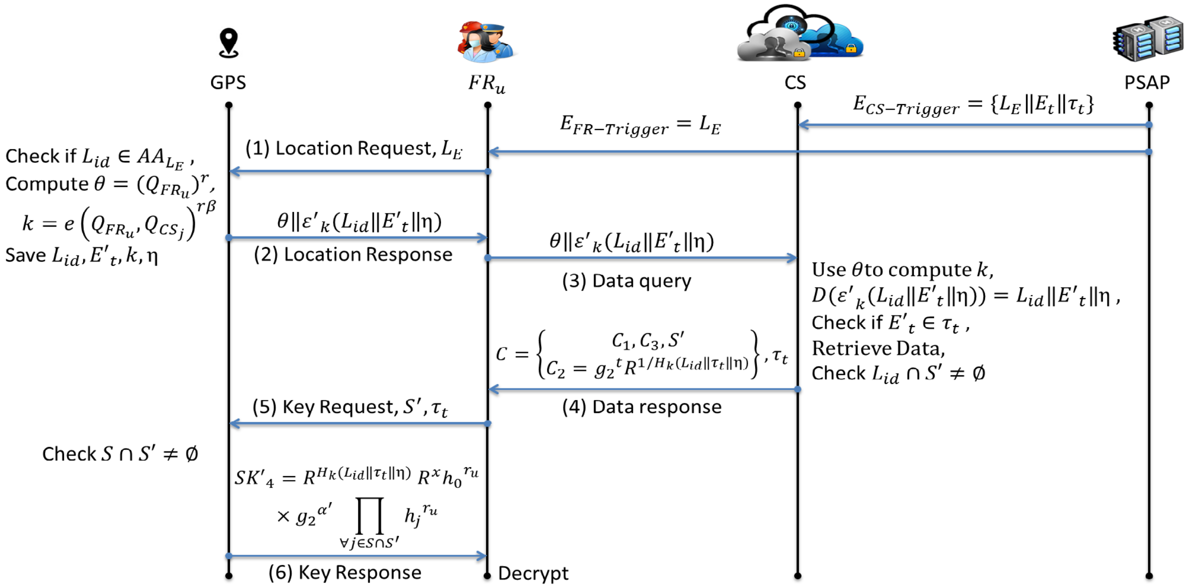
GPS
FR_u
CS
PSAP
$E_{CS-Trigger} = \{L_E \| E_t \| \tau_t\}$
$E_{FR-Trigger} = L_E$
(1) Location Request, L_E
Check if $L_{id} \in AA_{L_E}$,
Compute $\theta = (Q_{FR_u})^r$,
$k = e\left(Q_{FR_u}, Q_{CS_j}\right)^{r\beta}$
Save L_{id}, E'_t, k, η
$\theta \| \varepsilon'_k(L_{id} \| E'_t \| \eta)$
(2) Location Response
$\theta \| \varepsilon'_k(L_{id} \| E'_t \| \eta)$
(3) Data query
Use $\theta$to compute k,
$D(\varepsilon'_k(L_{id} \| E'_t \| \eta)) = L_{id} \| E'_t \| \eta$,
Check if $E'_t \in \tau_t$,
Retrieve Data,
Check $L_{id} \cap S' \neq \emptyset$
$C = \left\{ \begin{matrix} C_1, C_3, S' \\ C_2 = {g_2}^t R^{1/H_k(L_{id} \| \tau_t \| \eta)} \end{matrix} \right\}, \tau_t$
(4) Data response
(5) Key Request, S', τ_t
Check $S \cap S' \neq \emptyset$
$SK'_4 = R^{H_k(L_{id} \| \tau_t \| \eta)}\, R^x {h_0}^{r_u}$
$\times {g_2}^{\alpha'} \prod_{\forall j \in S \cap S'} {h_j}^{r_u}$
(6) Key Response
Decrypt

FIGURE 3. Message exchange paradigm.

Correctness: We check that decryption recovers the correct value of K,

$$\begin{aligned} K' &= e\Big(g_1^s, q^\alpha \Lambda^{r'_u} \times \prod_{v_{i,j} \in D} T_{i,j}^{r'_u}\Big) \\ &\quad \times e\Big((\Lambda \prod_{v_{i,j} \in D} T_{i,j})^s \times (h_0 \prod_{j \in S'} h_j)^t, g_1^{-r'_u}\Big) \\ &= e\Big(g_1^s, q^\alpha\Big) \times e\Big(g_1, \Lambda \times \prod_{v_{i,j} \in D} T_{i,j}\Big)^{sr'_u} \\ &\quad \times \Big(\Lambda \prod_{v_{i,j} \in D} T_{i,j}, g_1\Big)^{-sr'_u} \\ &= e(g_1, q)^{s\alpha}. \end{aligned} \tag{9}$$

And,

$$\begin{aligned} SK'_4 \times \prod_{j_1 \in S'} SK'_{j_1} &= R^{H_k(L_{id}||\tau_t||\eta)} \\ &\quad \times R^x h_0^{r_u} g_2^{\alpha'} \prod_{j \in \{S \bigcap S'\}} h_j^{r_u} \\ &\quad \times \prod_{j_1 \in S' \setminus \{S \bigcap S'\}} h_{j_1}^{r_u} \\ &= R^{(H_k(L_{id}||\tau_t||\eta)+x)} g_2^{\alpha'} (h_0 \prod_{j \in S'} h_j)^{r_u}. \end{aligned} \tag{10}$$

Plugging (10) into (8) gives us

$$\begin{aligned} K'' &= e\Big(R^{(H_k(L_{id}||\tau_t||\eta)+x)}, R^{1/(x+H_k(L_{id}||\tau_t||\eta))}\Big) \\ &\quad \times e(g_2^{\alpha'}, g_2^t) \times e\Big((h_0 \prod_{j \in S'} h_j)^{r_u}, g_2^t\Big) \\ &\quad \times e\Big(g_2^{-r_u}, (\Lambda \prod_{v_{i,j} \in D} T_{i,j})^s \times (h_0 \prod_{j \in S'} h_j)^t\Big) \\ &= e(R, R) \times e(g_2, g_2)^{t\alpha'} \times e((h_0 \prod_{j \in S'} h_j), g_2)^{tr_u - tr_u} \\ &= e(R, R) \times e(g_2, g_2)^{t\alpha'}, \end{aligned} \tag{11}$$

Plugging (9) and (11) into (6) results in (12) as required.

$$K = Y_0^s \times Y_1^t \tag{12}$$

Fig 3 illustrates the message (shown by arrows) exchange paradigm among FR_u, GPS, CS, and PSAP. Note that messages exchanged from 2 to 4 are assumed to be in the same time interval τ_t. As Fig 3 illustrates, an FR and the CS receive their corresponding emergency trigger message. The FR gets its location from the GPS component (messages 1-2), and forms a query to retrieve data (message 3). After receiving the data response (message 4), the FR extracts S', τ_t and sends them to the GPS component (message 5). It generates the one-time key SK'_4 and sends it back to the FR (message 6). Finally, the FR decrypts the ciphertext.

B. UPDATING CIPHERTEXT

In our construction, the purpose of updating ciphertext is to change the access policy. An access policy is comprised of a subset of locations and a subset of static attributes. Alteration in either one of the subsets, changes access privileges. Note that DOs have control over their information and in defining and updating the authorization set. However, this task can be delegated to their smartphones to automate the process. In this regard, if a DO moves out of his preferred location set, it will update the ciphertext.

For example, if a DO defines an access policy as $D = \{v_{2,3}, v_{4,2}, \ldots, v_{6,3}\}$, and he wants to remove $v_{4,2}$ and add $v_{8,1}$, the updating massage will be $C_{updating} = \{D_{new}, T_{4,2}^{-s} \times T_{8,1}^s\}$ which will be sent to the CS. Then, the CS modifies the corresponding record as follows: $C_{3,new} = C_3 \times T_{4,2}^{-s} \times T_{8,1}^s$. Note that changing the location set is done following the same procedure.

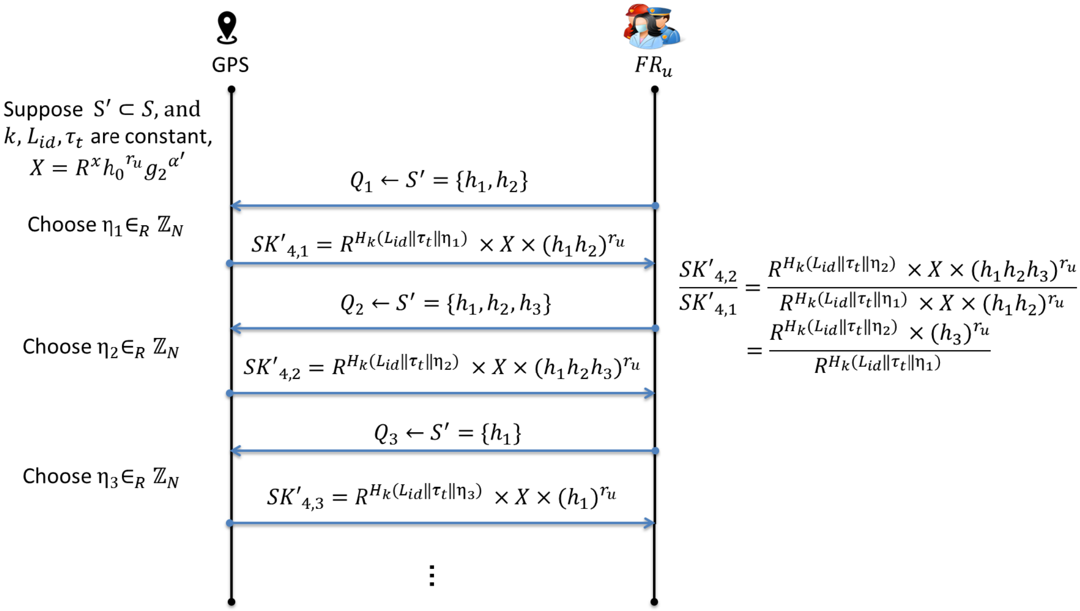
GPS
FR_u
Suppose $S' \subset S$, and
k, L_{id}, τ_t are constant,
$X = R^x {h_0}^{r_u} {g_2}^{\alpha'}$
$Q_1 \leftarrow S' = \{h_1, h_2\}$
Choose $\eta_1 \in_R \mathbb{Z}_N$
$SK'_{4,1} = R^{H_k(L_{id}\|\tau_t\|\eta_1)} \times X \times (h_1h_2)^{r_u}$
$Q_2 \leftarrow S' = \{h_1, h_2, h_3\}$
Choose $\eta_2 \in_R \mathbb{Z}_N$
$SK'_{4,2} = R^{H_k(L_{id}\|\tau_t\|\eta_2)} \times X \times (h_1h_2h_3)^{r_u}$
$Q_3 \leftarrow S' = \{h_1\}$
Choose $\eta_3 \in_R \mathbb{Z}_N$
$SK'_{4,3} = R^{H_k(L_{id}\|\tau_t\|\eta_3)} \times X \times (h_1)^{r_u}$
⋮
$\frac{SK'_{4,2}}{SK'_{4,1}} = \frac{R^{H_k(L_{id}\|\tau_t\|\eta_2)} \times X \times (h_1h_2h_3)^{r_u}}{R^{H_k(L_{id}\|\tau_t\|\eta_1)} \times X \times (h_1h_2)^{r_u}} = \frac{R^{H_k(L_{id}\|\tau_t\|\eta_2)} \times (h_3)^{r_u}}{R^{H_k(L_{id}\|\tau_t\|\eta_1)}}$

FIGURE 4. Key query/response between an FR and GPS.

C. OUTSOURCING DECRYPTION

Outsourcing decryption has been used in many works to transfer the heavy burden of pairing computation to one or several powerful servers. However, it is important that the server does not learn any information about the private key or the message during the partial decryption process. Notice that the decryption algorithm requires D and S' in order to proceed. Here, those sets can be acquired using a round of communication between an FR_u and the CS. Consider the following suppositions:

$$SK_1 \times \prod_{v_{i,j} \in D} SK_{i,j} = A, \tag{13}$$

$$SK_2 = B, \tag{14}$$

$$SK_3 = C, \tag{15}$$

$$SK'_4 \times \prod_{j_1 \in S'} SK'_{j_1} = D. \tag{16}$$

Then, the FR chooses a random number $\delta \in_R \mathbb{Z}_N$ and instead of message (3) in Fig 3 sends $\{A^\delta || B^\delta || C^\delta || D^\delta || L_{FR_u} || \theta || \xi(\tau_t || \eta) || ID_{DO}\}$ to the CS. The server computes the following

$$K'_{new} = e(C_1, A^\delta) \times e(C_3, B^\delta) = K'^\delta, \tag{17}$$

and,

$$K''_{new} = e(D^\delta, C'_2) \times e(C^\delta, C_3) = K''^\delta, \tag{18}$$

and sends $K'_{new} \times k''_{new}$ back to the FR. The user computes (19) and decrypts the message

$$K = \frac{(K'_{new} \times k''_{new})^{1/\delta}}{e(R, R)}. \tag{19}$$

VII. SECURITY ANALYSIS OF LA-CP-ABE

In this section, we will analyse the security of the LA-CP-ABE scheme. We will first discuss some security points of the proposed scheme. Then, we show that the proposed authorization scheme is proven selectively secure under the $m-$BDHE assumption.

The FR and an observer of the message (3) in Fig 3 cannot undetectably manipulate $\xi'_k(L_{id}||\tau_t||\eta)$ since it is protected using the AES symmetric encryption scheme. The symmetric shared key is computed using SK_0 and a random number. Recall that SK_0 was securely transferred to the GPS. Moreover, the random number is changed for every location query which causes the shared key to change accordingly. Therefore, an FR cannot bypass a GPS to generate legitimate data queries himself/herself. In addition, the CS ensures that the message has been generated by GPS and proceeds with the algorithm.

In addition, the secure GPS of a smartphone computes the session private key SK'_4 by which the message can be decrypted. Note that only if the location and time interval attributes of the ciphertext match the ones in the SK'_4, will the $e(R, R)$ component be eliminated. Otherwise, it would have some unknown exponent which causes the decryption to fail. In this case, such data is filtered and considered irrelevant to the ongoing situation.

Furthermore, an FR should not be able to extract the private key element SK_4 of its GPS to be able to bypass it. To mitigate that, a new unique $\eta_{new} = H_k(\eta_{old})$ is computed for each new set of locations S' (message (5) in Fig. 3). In this case, the queries from the FR to the GPS result in random looking varied values. Fig.4 illustrates key query/response when $S' \subset S$ is assumed and the queries are in the same time interval and at the same location (i.e., k is fixed). Even under such assumptions, the FR is not able to extract $X = R^x h_0^{r_u} g_2^{\alpha'}$ or $h_j \in Q_i \setminus Q_{i'}$. In Fig. 4, $h_3^{r_u}$ or $h_2^{r_u}$ cannot be extracted from $\frac{SK'_{4,2}}{SK'_{4,1}}$ or $\frac{SK'_{4,1}}{SK'_{4,3}}$ respectively since η is changing for each new Q_i, therefore, $R^{H_k(L_{id}||\tau_t||\eta)}$ is changing for respective queries. Notice that the GPS cannot extract $g_2^{\alpha'}$ since it has been blinded using R^x. And, since they are orthogonal to each other (1), this obfuscating element will be cancelled in the pairing computation in the decryption process.

The proposed scheme calculates a session key from the term θ to prevent replay attack. In this regard, the decryption key is valid for a certain location area and within single time interval. This also is an important factor to consider for addressing our new threat model. For example, if an FR receives a private key for some data associated with a certain location area and time interval τ_t, then the user should not be able to decrypt the data for the same location within another time interval $\tau_{t+t'}$. In this case, our access model is superior to the Break-the-Glass model. Recall that in that concept, the master key always decrypts the corresponding ciphertext. Our scheme restricts data access based on the time and location of an emergency by which irrelevant data is filtered and a higher level of privacy is provided. Besides, considering the proposed scheme, both the CS and DOs are involved in the authorization process. This decreases the risk of privacy breach if the server turns malicious.

We integrated BE with CP-ABE to incorporate the location attribute in an access policy. In this case, using BE implies a $(1, n)-$threshold access structure meaning that possessing private keys corresponding merely to one location attribute leads to successful decryption of the message. Observe that if a DO has included his/her home and work location areas (e.g. L_1, L_2 respectively) in the ciphertext, an FR who is visiting either one of the Associated areas (e.g. AA_{L_1}) can generate the proper private key to decrypt his/her data even if the DO is currently located at the other location (L_2 in this example). This can be avoided by updating the ciphertext by the DO upon leaving the home location area. Here, there is a trade-off between the ciphertext updating computation/communication costs and data filtering accuracy: the bigger the size of S'', the smaller the data filtering accuracy. We will further demonstrate such costs in Section VIII.

In addition, to decrease the probability of privacy breach, we can incorporate an Audit-trail technique to log all of the activities which can be used to spot unauthorized data access [80]. Here, this process should be operated and managed by a trusted party to avoid collusion or illegitimate modifications to the log.

Moreover, the CS cannot learn anything from the outsourcing computations since the components are blinded by the exponent δ. Finally, we also avoid the key escrow problem, since we use two separate KGAs to generate secret keys of the system. Note that setup algorithms in both KGAs receive the same description of $(\mathbb{G}, \mathbb{G}_T, e)$. One of the KGAs generates the private keys corresponding to location attribute, and the other one for the static attributes. Therefore, there is no single key generating authority that can decrypt all messages. Here, we assume that KGAs do not collude with each other.

We prove our LA-CP-ABE scheme is selectively secure based on the decisional $m - BDHE$ assumption. Note that if BDHE is assumed to be hard in the subgroups G_p and G_r, then it can be assumed to be hard in the composite order group $\mathbb{G}$ as well. We follow the selective CPA security game in which we assume that an attacker $\mathcal{A}$ wins the game with advantage ϵ. It is worth mentioning that we can also achieve CCA security as well using well-known methods used in [81] and [82]. We construct an algorithm $\mathcal{B}$ that uses $\mathcal{A}$ to break the $m - BDHE$ assumption with the advantage of at least ϵ. The $m - BDHE$ challenger generates two problem instances as below.

For the subgroup G_p, the instance is comprised of g_1^c and the set $(g_1, g_1^a, g_1^{(a^2)}, \ldots, g_1^{(a^m)}, g_1^{(a^{m+2})}, \ldots, g_1^{(a^{2m})}, Z_1) \in \mathbb{G}^{2m} \times \mathbb{G}_{T,p}$, where $m = l \times |V_i| + |FRs|$ is the number of attributes times the size of their value set plus the number of FRs in the system. Suppose $|V_i| = v$ is the same for all of the attributes. For the subgroup G_r, the instance is comprised of $g_2^{c'}$ and the set $(g_2, g_2^b, g_2^{(b^2)}, \ldots, g_2^{(b^{m'})}, g_2^{(b^{m'+2})}, \ldots, g_2^{(b^{2m'})}, Z_2) \in \mathbb{G}^{2m'} \times \mathbb{G}_{T,r}$, where $m' = n + |FRs|$ is the size the location set in the system plus the number of FRs in the system.

Suppose that the challenger selects $\rho \in_R \{0, 1\}$ and $\rho' \in_R \{0, 1\}$ (the two selections are independent from one another). If $\rho = 0 = \rho'$, then $Z_1 = e(g_1, g_1)^{ca^{m+1}}$, and $Z_2 = e(g_2, g_2)^{c'b^{m'+1}}$. Otherwise, if $\rho = 1 = \rho'$, then Z_1 and Z_2 are random elements of $\mathbb{G}_{T,p}, \mathbb{G}_{T,r}$ respectively. The challenger gives the two $m - BDHE$ instances to $\mathcal{B}$. Consider the game between $\mathcal{B}$ and the adversary $\mathcal{A}$ as follows:

Initialization: $\mathcal{A}$ commits to sets $D \subseteq [1, m - |FRs|]$ and $S' \subseteq [1, m' - |FRs|]$.

Setup: $\mathcal{B}$ generates $\varphi = \{u_1, u_2, u_3, y_0, \ldots, y_m\}, \varphi' = \{u'_1, y'_0, \ldots, y'_{m'}\} \overset{R}{\leftarrow} \mathbb{Z}_N$. Note that we allocate $\{y_1, \ldots, y_v\}$ to A_1, $\{y_{v+1}, \ldots, y_{2v}\}$ to A_2, etc. In other words, suppose there is map function $\rho(i, j) = (i - 1)v + j \in [1, m - |FRs|]$ for $1 \leq i \leq l$ and $1 \leq j \leq v$. This function is used to assign a number in $[1, m - |FRs|]$ to $T_{i,j}$. Then, $\mathcal{B}$ sets

$$q \leftarrow g_1^{u_1} \tag{20}$$

$$R \leftarrow g_1^{u_2} \tag{21}$$

$$\Lambda \leftarrow g_1^{y_0 u_3} \tag{22}$$

$$T_{i,j} \leftarrow g_1^{y_{\rho(i,j)}} \quad \textit{for } \rho(i,j) \in D \tag{23}$$

$$T_{i,j} \leftarrow g_1^{y_{\rho(i,j)} + a^{\rho(i,j)}} \quad \textit{for } \rho(i,j) \in [1, m - |FRs|] \setminus D \tag{24}$$

$$h_0 \leftarrow g_2^{y'_0} \tag{25}$$

$$h_i \leftarrow g_2^{y'_i} \quad \textit{for } i \in S' \tag{26}$$

$$h_i \leftarrow g_2^{y'_i + b^i} \quad \textit{for } i \in [1, m'] \setminus S' \tag{27}$$

Note that $A_0 = \Lambda \in D$ is always true. Formally, $\mathcal{B}$ sets $\alpha \leftarrow y_0 u_3 \times a^{m+1}$ and $\alpha' \leftarrow y'_0 u'_1 \times b^{m'+1}$. Thus, public parameters are

$$PK = \begin{cases} g_1, q, R, \Lambda, e(g_1, q)^{\alpha}, e(R, R), \{T_{i,j}\}_{i \in [1,l], j \in [1,v]}, \\ g_2, e(g_2, g_2)^{\alpha'}, h_0, h_1, \dots, h_n, \end{cases}$$

where $e(g_1, q)^{\alpha}$ and $e(g_2, g_2)^{\alpha'}$ can be computed as

$$e(g_1, q)^{\alpha} = e(g_1^{a^m}, (g_1^{a})^{u_1})^{y_0 u_3} = e(g_1, g_1^{u_1})^{y_0 u_3 \times a^{m+1}}, \qquad (28)$$

and,

$$e(g_2, g_2)^{\alpha'} = e(g_2^{b^{m'}}, g_2^{b})^{u'_1} = e(g_2, g_2)^{u'_1 \times b^{m'+1}}. \qquad (29)$$

$\mathcal{B}$ sends PK to $\mathcal{A}$.

Private Key Queries: $\mathcal{A}$ is allowed to query the private key only for the attributes that were not included in either D or S' except Λ and h_0. We first generate the keys associated with $\mathbb{G}^{2m} \times \mathbb{G}_{T,p}$, and then for the other instance. $\mathcal{B}$ generates $z'_u \overset{R}{\leftarrow} \mathbb{Z}_N$ and formally sets $r'_u = z'_u - u_1 a^{m+1-u}$. For each FR, we personalize the default attributes as follows: $\Lambda_u = g_1^{y_0 u_3 a^u} = (g_1^{a^u})^{y_0 u_3}$, $h_{u,0} = g_2^{y'_0 b^u} = (g_2^{b^u})^{y'_0}$. It outputs,

$$SK_u = \begin{cases} SK_0 = H_1(FR_u)^{\beta}, \\ SK_{u,1} = q^{\alpha} \Lambda_u^{r'_u} \\ = g_1^{u_1 u_3 y_0 a^{m+1}} \times g_1^{z'_u u_3 y_0 a^u - u_1 u_3 y_0 a^{m+1} a^{u-u}} \\ \qquad\qquad = g_1^{z'_u u_3 y_0 a^u}, \\ SK_{u,\rho(i,j)} = T_{i,j}^{r'_u} = g_1^{(y_{\rho(i,j)} + a^{\rho(i,j)}) r'_u} \\ = g_1^{(y_{\rho(i,j)} + a^{\rho(i,j)})(z'_u - u_1 u_3 y_0 a^{m+1-u})}, \\ \qquad \mathit{for} \quad \rho(i,j) \in [1, m - |FRs|] \setminus D \\ SK_{u,2} = g_1^{-r'_u}, \end{cases}$$

For the instance associated with $\mathbb{G}^{2m'} \times \mathbb{G}_{T,r}$, $\mathcal{B}$ generates $z_u, x \overset{R}{\leftarrow} \mathbb{Z}_N$ and formally sets $r_u = z_u - u'_1 b^{m'+1-u}$. It outputs the corresponding elements of the secret key as follows

$$SK_u = \begin{cases} SK_{u,3} = g_2^{-r_u}, \\ SK'_{u,j_1} = h_{j_1}^{r_u} = g_2^{r_u(y'_{j_1} + b^{j_1})} \\ \quad \mathit{for} \quad j_1 \in \{n\} \setminus \{S \bigcup S^*\}, \\ SK_{u,4} = R^x h_{u,0}^{r_u} g_2^{\alpha'} \\ \quad = g_1^{u_2 x} \times g_2^{z_u y'_0 b^u - y'_0 u'_1 b^{m'+1} b^{u-u}} \times g_2^{y'_0 u'_1 b^{m'+1}} \\ \qquad\quad = g_1^{u_2 x} g_2^{z_u y'_0 b^u}, \\ SK''_{j_2} = h_{j_2}^{r_u} = g_2^{r_u(y'_{j_2} + b^{j_2})} \\ \quad \mathit{for} \qquad j_2 \in \{S\} \setminus \{S^*\} \end{cases}$$

Remarks: The tricky part is to simulate the $SK_{u,1}$ and $SK_{u,4}$ values since they are comprised terms of the form $g_1^{a^{m+1}}$ and $g_2^{b^{m'+1}}$ respectively. These terms are unknown to $\mathcal{B}$. However, notice that these terms in the exponent are cancelled out which makes them computable for $\mathcal{B}$. In addition, the distribution of the private key is identical to that of the original scheme.

Challenge: $\mathcal{A}$ chooses a subset $D^* \subset D$, $S^* \subset S'$, two messages M_0, M_1 and sends them to $\mathcal{B}$. $\mathcal{B}$ chooses $\mu \in_R \{0, 1\}$, computes the ciphertext as below, and sends the result to $\mathcal{A}$.

$$K = Z_1^{u_1 u_3 y_0} \times Z_2^{y'_0 u'_1}$$

$$C^* = \begin{cases} C_0^* = \xi'_K(M_{\mu}), \\ C_1^* = g_1^{c}, \\ C_2^* = g_2^{c'}, \\ C_3^* = (\Lambda \prod\limits_{v_{i,j \in D^*}} T_{i,j})^{c} \times (h_0 \prod\limits_{j \in S^*} h_j)^{c'} \\ = (g_1^{y_0 u_3} \prod\limits_{v_{i,j \in D^*}} g_1^{y_{\rho(i,j)}})^{c} \times (g_2^{y'_0} \prod\limits_{j \in S^*} g_2^{y'_j})^{c'} \\ = (g_1^{c y_0 u_3} (g_1^{c})^{\sum_{v_{i,j \in D^*}} y_{\rho(i,j)}}) \times (g_2^{c' y'_0} (g_2^{c'})^{\sum_{j \in S^*} y'_j}). \end{cases}$$

Notice that $\mathcal{B}$ is able to calculate the challenge from the instances as shown above.

CS-Encrypt, GPS-KGen: We use the random oracle model instantiated with HMAC to output the required randomness for the two algorithms.

Guess: Finally, $\mathcal{A}$ outputs a bit $\mu' \in \{0, 1\}$. $\mathcal{B}$ outputs 1 if $\mu = \mu'$ and 0 otherwise. Notice that if $Z_1 = e(g_1, g_1)^{c a^{m+1}}$ and $Z_2 = e(g_2, g_2)^{c' b^{m'+1}}$, then C^* is a valid challenge ciphertext associated with D^*, S^*. Therefore, $\mathcal{A}$ has advantage ϵ. Since $m-$BDHE is known to be a hard problem, the advantage ϵ is negligible. Then, we have the following

$$\begin{aligned} &\Pr[\mathcal{B} \rightarrow 1 | Z_1 = e(g_1, g_1)^{c a^{m+1}}, Z_2 = e(g_2, g_2)^{c' b^{m'+1}}] \\ &\quad = \Pr[\mu = \mu' | Z_1 = e(g_1, g_1)^{c a^{m+1}}, Z_2 = e(g_2, g_2)^{c' b^{m'+1}}] \\ &\quad = \frac{1}{2} + \epsilon. \end{aligned}$$

Otherwise, three other cases may occur; first, both $Z_1 \in \mathbb{G}_{T,p}$ and $Z_2 \in \mathbb{G}_{T,r}$ are random elements; second and third, either one of them is a random element. In all of those cases, $\mathcal{A}$ has no advantage to distinguish the ciphertext generated for M_0 from the ciphertext generated for M_1. This is because all parts of the ciphertext have the same distribution in either $\mu = 0$ or $\mu = 1$. Therefore, $\Pr[\mathcal{B} \rightarrow 0 | Z_1 \text{ and } Z_2 \text{ are } \mathit{random}] = \Pr[\mathcal{B} \rightarrow 0 | Z_1 \text{ or } Z_2 \text{ are } \mathit{random}] = \frac{1}{2}$. □

Note that since x and $u_2 \in \mathbb{Z}_N$ are chosen uniformly at random, and $g_1 \in G_p$, then, $g_1^{u_2 x} = R^x$ reveals nothing about the value of $u_2 x$ modulo r. In other words, $u_2 x$ modulo r is uniformly random. Therefore, in the view of an attacker, the corresponding key is well-distributed.

VIII. PERFORMANCE ANALYSIS OF LA-CP-ABE

In this section, we discuss some significant features of our LA-CP-ABE scheme with regards to the emergency response application. In addition, we analyse computation and communication complexities, storage requirements, and delay. Concerning with CP-ABE schemes, our focus is merely on the constant ciphertext-size and constant number of pairings in the decryption process.

TABLE 3. CP-ABE protocol comparison.

Scheme	Complexity	Ciphertext Size	Decryption Computation overhead	Key Generation computation	Private key size	Access structure	CT-update communication	CT-update computation	Dynamic attribute
[49]	DBDH	$2\vert G_1\vert + \vert G_T\vert + \vert AS\vert$	$3\tau_p + 2G_T$	$(W+4)G_1$	$2\vert G\vert$	$(n,n)-$Threshold	$\vert G\vert$	$(i+j)G$	×
[50]	Composite-Order Bilinear Group, DBDH	$\vert G_T\vert + 2\vert G\vert + \vert AS\vert$	$3\tau_p + 2G_T$	$(W+3)G_p$	$2\vert G\vert$	$(n,n)-$Threshold	$\vert G\vert$	$(i+j)G$	×
[45]	Composite-Order Bilinear Group	$\vert G_T\vert + 2\vert G\vert$	$2\tau_p + (2W)G + 2G_T$	$(l-t+1)(n+2)G$	$(l-t+1)(n+2)\vert G\vert$	$(t,n)-$Threshold	$\vert G\vert$	$(i+j)G$	×
[51]	aMSE-DDH	$\vert G_1\vert + \vert G_2\vert + \vert G_T\vert + \vert AS\vert$	$3\tau_p + tG_1 + (n+t-2)G_T$	$WG_1 + (n-1)G_2$	$(n+\vert W\vert)\vert G\vert$	$(t,n)-$Threshold	$\vert G\vert$	$(i+j)G$	×
[52]	DBDH	$\vert G_T\vert + 2\vert G\vert + \vert AS\vert$	$2\tau_p + 2G_T$	$(2W+4)G$	$2\vert G\vert$	$(n,n)-$Threshold	$\vert G\vert$	$(i+j)G$	×
[83]	l-BDHE	$2\vert G\vert + \vert\xi'\vert$	$(2n+1)\tau_p$	$(2n+1)G$	$(2n+1)G$	AND$_{+-*}$	$\vert G\vert$	$(i+j)G$	×
[40]	B-Co-CDH	$3\vert G\vert$	$3\tau_p + G$	$5G$	$4\vert G\vert$	$(n,n)-$Threshold	×	×	×
[82]	l-BDHE	$\vert G_T\vert + 2\vert G\vert + \vert AS\vert$	$2\tau_p + 2G_T$	$2nG$	$n\vert G\vert + \mathbb{Z}_p$	AND$_{+-}$	$2\vert G\vert$	$2(i+j)G$	×
[84]	$(t,\epsilon,l)-$BDHE	$2\vert G\vert + \vert G_T\vert$	$2\tau_p + 2G_T$	$3nG$	$n\vert G\vert + \mathbb{Z}_p$	AND$_{m*}$	$2\vert G\vert$	$2(i+j)G$	×
$[85]_1$ $[85]_2$	l-BDHE	$\{\vert G_T\vert + 2\vert G\vert\}$ $\{\vert G_T\vert + 3\vert G\vert + \vert\mathbb{Z}_p\vert\}$	$\{2\tau_p + (2n)G\}$ $\{6\tau_p + (2n+2)G\}$	$(W+d)(2n+2)G$	$(n+\vert W\vert)(2n+1)\vert G\vert$	$(t,n)-$Threshold	$\vert G\vert$	$(i+j)G$	×
[86]	Composite-Order Bilinear Group	$\vert G_T\vert + 2\vert G\vert$	$3\tau_p$	$(W+3)G$	$2\vert G\vert$	$(n,n)-$Threshold	$\vert G\vert$	$(i+j)G$	×
[87]	l-BDHE	$\{\vert G_T\vert + 3\vert G\vert + \vert\mathbb{Z}_p\vert\}$	$\{6\tau_p + (2n+2)G\}$	$(W+d)(2n+2)G$	$(n+\vert W\vert)(2n+1)\vert G\vert$	$(t,n)-$Threshold	$\vert G\vert$	$(i+j)G$	×
Ours	l-BDHE	$3\vert G\vert + \vert\xi'\vert$	$(4+\vert S'+D\vert)G + 2G_T$	$(7+\vert S+W_{FR}\vert)G$	$(6+\vert S+W_{FR}\vert)\vert G\vert$	AND$_m$	$\vert G\vert$	$(i+j)G$	✓

Table 3 presents a comprehensive comparison among state-of-the-art CP-ABE protocols. In this table, n is the number of attributes in the universe, l is the number of attributes included in an access policy, t is the threshold value by which an access policy will be satisfied, v is the number of values associated with an attribute, W is the number of attributes that a user possesses, d number of default attributes in the system, AND$_+ - *$ means AND gate with positive, negative, and wildcards, AND$_m *$ means AND gate with multivalued and wildcards, i, j are the numbers of added and removed attributes respectively to the ciphertext.

In Table 3, ciphertext size is constant in all of the schemes regardless of the number of attributes in the access policy. In addition, the table shows that the ciphertext contains an element of the target group $\mathbb{G}_T$ for all schemes except the works [40], [83], and ours. We used such an element as the secret key to a symmetric encryption scheme ξ' (e.g., AES) to increase computation efficiency.

TABLE 4. Time costs comparison.

	Platform	Time
Multiplication-80bit	MSP430 TelosB 8MHz	0.001ms
Pairing-80bit	MSP430 TelosB 8MHz	1.27s
AES-128	ATmega128 16MHz	160Kbit/s
AES-128	AMD64 2.194GHz	198Mbit/s

Besides, based on Table 3, computation complexity for all of the schemes is constant in terms of number of pairing computations. In this case, our scheme is more efficient than others, since we delegated such heavy burden to a powerful server. Notice that our outsourced decryption scheme requires merely 4 pairing operations on the server side. On the other hand, our decryption computation complexity is comprised of $(4 + |S' + D|)$ multiplications in $\mathbb{G}$ and 1 exponentiation plus 1 multiplication in the target group $\mathbb{G}_T$ on the user side. This is explicitly important considering the emergency response application. It can be shown that the delay corresponding pairing computations are much higher than group arithmetic operations. Table 4 indicates the difference in computation delay between bilinear group multiplication/pairing with 80-bit security and AES encryption scheme with 128 bit security. The numbers were extracted from the works in [88]–[90]. The first three rows show the timing costs for resource constraint devices and the last one illustrates a more powerful computer. Observe that even in resource constraint devices as long as the computation complexity is remained constant especially for pairing calculations, respective schemes are still feasible. However, the advantage of our scheme is the use of AES instead of multiplication of the message with a key (e.g., $e(X, X)^x \in \mathbb{G}_T$) which results in higher efficiency even on resource constraint devices.

Comparing the two columns for private key size and access structure in Table 3 shows an interesting conclusion which is the fact that constant private key size results in a very limited access structure $(n, n)-$Threshold. In this case, although a user might have several attributes, there is only one combination that enables him to decrypt a ciphertext. In other words, the attributes and their values used in the ciphertext should perfectly match the ones in a user's private key. On the contrary, AND-gate access structure provides more flexible and expressive access policy for the cost of higher private key size. In this case, the storage requirement for a user demands higher capacity. Our scheme uses multivalued AND-gate.

In addition, Table 3 shows that all the schemes are able to update the ciphertext using the same technique as ours except [40]. Note that those schemes did not present the procedure with which a ciphertext can be updated. The scheme [40] requires to contact a server in order to get the hashed value of the new authorized attribute list and update the aggregated group element in the ciphertext. In fact, to update a ciphertext, that scheme substitutes two out of three elements of the ciphertext whereas others merely modify existing element(s) by multiplication as shown in Section VI-B. The cost of updating ciphertext is similar for all of the schemes except [82], [84] for which two elements of the ciphertext should be modified. Note that the

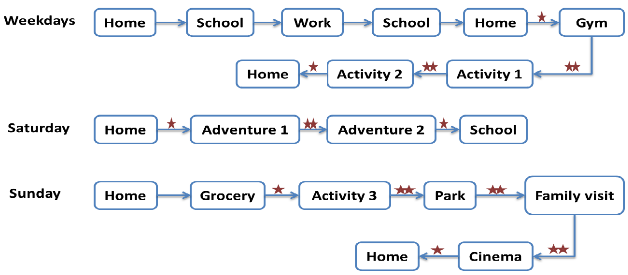

FIGURE 5. Movement trajectory scenario per week.

communication cost of updating a ciphertext does not depend on the number of attributes. This is a key advantage especially in situations where users often change their locations.

Furthermore, the key distinction among the schemes in Table 3 is the ability to incorporate dynamic attributes (i.e., location and time). Our scheme uses BE to incorporate the location attribute to ciphertext at the DO's side, and a server incorporates time attribute to complete the requirement. None of the schemes in Table 3 is able to incorporate dynamic attributes.

Utilizing BE decreases the updating frequency which results in higher degree of computation and communication efficiency. Suppose there are two individuals Alice and Bob who have the same life style meaning that their movements during a week is similar. Fig. 5 illustrates such a scenario in which weekdays and the weekend are shown separately. In this figure, boxes are locations and it is assumed that each box is in a distinct location area. This implies that, for instance from Home to School, a DO needs to update the ciphertext.

Assume that the preferred location set of Alice and Bob are $S''_{Alice} = \{Home, School, Work, Grocerystore\}$ and $S''_{Bob} = \{\emptyset\}$ respectively. Therefore, if Alice moves from one location to another in her set, no updating is necessary. Note that in this case $S' = S''$. In addition, if she moves from a location in the set (e.g., Home) to another one not in the set (e.g., Gym), she only needs to update the ciphertext by adding Gym to it. The stars on top of the arrows in Fig. 5 show when an updating is required for Alice. In addition, the number of stars shows the total number of group multiplications necessary for updating the ciphertext. Despite Alice, Bob needs to update his data for each one of his movement.

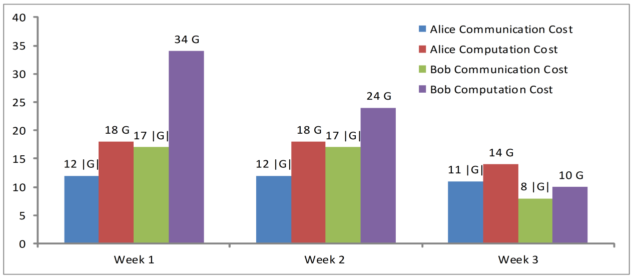

FIGURE 6. The effect of $|S''|$ on communication and computation costs of updating process.

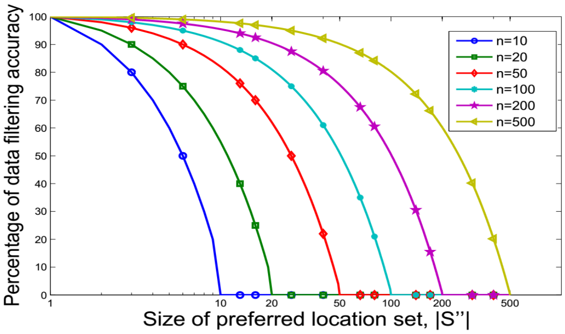

FIGURE 7. Percentage of data filtering accuracy with regards to total number of location areas.

Fig. 6 illustrates the communication and computation costs of the updating process. The horizontal axis shows weeks one through three for which we change S' (recall that $S' = S'' \bigcup L_c$, i.e., the union of the preferred location set and the current location) for both Alice and Bob. The first set of bars represents the scenario showed in Fig. 5. The second set shows the effect of $|S''_{Bob}|$ when Bob includes *Home* and *Work* into his set. Finally, the third set of bars shows the costs when Alice includes *Gym* and *Park* into her set, and Bob includes all boxes except the three *Activities* and the two *Adventures*. Fig. 6 shows that increasing $|S''|$ affects computation complexity more than communication overhead. In this case, the computation complexity and communication overhead of Bob decreased by approximately 60 and 52 percent respectively per week comparing the first week with the second and the third respectively. And, Alice was able to decrease her computation cost by 32 percent and her communication overhead by 8.3 percent per week from week two to three. It can be concluded that if $|S''|$ increases, the ciphertext updating costs (i.e., communication and computation costs) decrease. However, it also decreases the data filtering accuracy. The relationship between data filtering accuracy and $|S'|$, and n is shown in (30) (for $S' = S''$). Here, $1 \leq |S'| \leq n$ which indicates that the accuracy is 100% when $|S'| = 1$ and it drops to 0% when $|S'| = n$.

$$Accuracy = \frac{n - |S'|}{n - 1} \times 100 \tag{30}$$

Fig. 7 illustrates the above relationship. For small n, the percentage of data filtering accuracy drops very fast if $|S'|$ increases. However, when n increases, the accuracy is higher for the same $|S'|$. For example, comparing $n = 10$ and $n = 200$ indicates that for $|S'| = 10$ the accuracy rises from 0 to 95.5% respectively.

The proposed access/threat model is also advantageous in a sense that it decreases the computation and communication burden on the CS in critical situations. Note that the CS first checks that the location of an FR and the time interval within which a data request is occurred (refer to Fig. 3) are legitimate. Without this a prior step, the CS would retrieve, process, and transfer data to the FR.

Table 5 compares our scheme with three other works [40], [47], [83] in more details. In [47], m is the

TABLE 5. Comparison of total computation and communication overhead.

Scheme	Communication Overhead				Decryption computation Cost	
	Ciphertext size	Outsourcing communication	Public parameter	Secret key size	User	Outsourced
[47]	$\|G_T\| + (2+l)\|G\|$	-	$(2n+m+3)\|G\| + \|G_T\|$	$(2+W)\|G\|$	$(3+2l)\tau_p + (2l+2)G_T$	-
[83]	$\|\xi'\| + 2\|G\|$	-	$(2n+1)\|G\|$	$(2n+1)\|G\|$	$(2n+1)\tau_p + (2W+1)G + 2nG_T$	-
[40]	$3\|G\|$	$2\|G\|$	$(2n+5)\|G\| + \|G_T\|$	$4\|G\|$	$3\tau_p + G$	$(3W+1)G$
Ours	$3\|G\| + \|\xi'\|$	$4\|G\|$	$(7+lv+n)\|G\| + 3\|G_T\|$	$(6+\|S+W_{FR}\|)G$	$(4+\|S'+D\|)G + 2G_T$	$4\tau_p$

maximum size of allowed attributes associated with ciphertext. The works [47], [83] are broadcast CP-ABE schemes in which explicit receivers are also specified within ciphertext using their identities. The work [40] uses attribute ranges and relations to provide flexible access policy for CP-ABE. As Table 5 indicates, the scheme [47] has better access policy expressiveness in comparison with other works. However, this has an effect on its ciphertext size which is proportional to the number of attributes in the access policy. Other protocols offer constant ciphertext size. In particular, the scheme [83] offers ciphertext size very close to ours. Both of the schemes use symmetric encryption algorithm to encrypt a message using an element in the target group as the secret key.

The work [40] also offers constant ciphertext size, and has the best secret key size among others. The reason lies under the $(n, n)-$threshold access structure which brings about very restrictive access policy. In this case, one can argue that since more storage is easily affordable and cheap to provide, it is better to offer higher access policy expressiveness and still keep the ciphertext size and decryption computation constant which evidently our scheme offers. Comparing outsourcing communication overhead shows that our scheme is less efficient by a factor of two extra group elements than [40]. However, with such extra elements, our decryption computation overhead on the user side is released from pairing computation. This significantly increases the efficiency of our scheme. To show how big a difference is between group multiplication/exponentiation and pairing computations, as one benchmark, using BN256 curve with RELIC library on a modern PC, pairing computation delay is approximately 8.22ms while modular multiplication requires 0.0034ms [91]. This means that the corresponding delay of approximately 2417 group multiplications equals one pairing operation. This was also shown for resource constraint devices in Table 4 in which pairing computation for 80-bit security is proportional to approximately 127 × 10^4 group multiplications. Considering the fact that a smartphone lacks powerful resources in comparison with a server, outsourcing such a heavy burden to a more powerful entity increases computation efficiency and decreases decryption delay drastically. In this regard, our scheme outperforms [40]. In terms of computation complexity, the schemes [47] and [83] are inefficient in comparison to ours as the result of linear relationship between pairing computations and the number of attributes in the access policy/system.

Concerning with the delay requirements, the schemes [47] and [83] in comparison with our scheme and [40] have an advantage which can affect on computation delay significantly. In this case, the former schemes compute pairings over prime-order groups while the latter ones are based on composite-order groups. Freeman [92] showed that the cost of Tate pairing computation in composite-order groups on a 1024-bit supersingular curve is 50 times slower than in Tate pairing on a 170-bit MNT curve in prime-order groups. Freeman also showed that pairing computation on a modern PC is done in approximately 150ms on supersingular curve with $\mathbb{G} \subset E(\mathbb{F}_q) \sim 1024$ bits and $\mathbb{G}_T \subset \mathbb{F}^*_{q^2} \sim 2048$ bits. Using this benchmark, since our outsourced computations require merely 4 pairings, this results in approximately 0.6 seconds of computation delay. Comparing to ours, the decryption process in [47] and [83] imposes $(3 + 2l)$ and $(2n + 1)$ pairings where l and n are the number of attributes in the access policy and in the system respectively. A naive comparison shows that those schemes with $l = n = 100$ impose the same delay as ours.

In order to decrease the computation delay, [92], [93] proposed efficient ways to convert composite-order bilinear groups to prime order groups and yet keeping the orthogonality property. Freeman [92] proposed to use two groups of the same prime-order (e.g. $\log_2 p = 256$) and an asymmetric bilinear map to provide orthogonality feature of composite-order (e.g. $\log_2 N = 3072$) groups in prime-order groups. Then, Lewko [93] provided a generic conversion using Dual Pairing Vector Space (DPVS). However, this method has a drawback in which instead of one paring in composite-order group of n primes, it needs $2n$ pairings in prime-order groups. Using this conversion for our scheme for which we used a composite-order group comprised of 2 primes, we need 4 pairings in prime-order groups for every single pairing originally. Considering our decryption process which requires 4 paring calculations, the prime-order conversion of our scheme requires 16 pairings for such a process. Using Freeman's benchmark in which prime-order pairing computation imposes $3ms$ delay, pairing computation in the decryption process is performed in approximately $50ms$. In comparison with [47] and [83], assuming $l = n = 8$ attributes for those schemes, the computation delay is similar to ours. However, such system parameters are very limited which highlights the effectiveness of our scheme.

TABLE 6. Comparison of computation delay for prime-order and composite-order groups.

Curve/Pairing	$\log_2 n$	Pairing	Exponentiation in $\mathbb{G}_1$	Exponentiation in $\mathbb{G}_2$	Exponentiation in $\mathbb{G}_T$
BN256/Ate	256	5.05	0.55	1.91	5.16
Supersingular/Tate	3072	1276.3	556.9	-	174.88

Table 6 shows the computation delay comparison between prime-order on a BN256 curve using Ate paring and composite-order with two primes on a supersingular curve using Tate pairing on a 2.6 GHz Intel Celeron 64 bits PC with 1 GB RAM that extracted from [94]. The table shows the efficiency of such a conversion in terms of computation delay for 128-bit security. The delays are in milliseconds.

IX. CONCLUSION

In an emergency, FRs require accurate, timely, and location-aware information. Acquiring such information encounters substantial challenges among which filtering large volume of data, privacy, and authorized access have received little attention. To jointly address the aforementioned challenges, this work proposed a location-aware access authorization scheme for emergency response. We integrated BE with CP-ABE to incorporate dynamic attributes (i.e., location and time) into an access policy. The LA-CP-ABE scheme ensures that an authorized FR is able to retrieve relevant, timely, and location-aware information. The performance analysis of LA-CP-ABE indicates the efficiency and effectiveness of the scheme in comparison with state-of-the-art fine grained authorization schemes. Our scheme imposes constant decryption computation complexity and communication overhead. The use of BE for incorporating location attribute decreases the communication cost of updating process. However, there is trade-off between the updating communication cost and accuracy of data. In this case, the large size of $S'' > 1$ implies lower updating cost requirement which may lead to lower location-accurate data. In terms of security, the proposed scheme is CCA-selective secure based on $m-$BDHE assumption and addresses the key escrow problem.

REFERENCES

[1] *Disaster Relief 2.0: The Future of Information Sharing in Humanitarian Emergencies, UN Foundation and Vodafone Foundation Technology Partnership*, Harvard Humanitarian Initiative, Cambridge, MA, USA, 2011.

[2] National Institute of Standards and Technology (NIST). *Research Roadmap for Smart Firefighting*, accessed on May 2015. [Online]. Available: http://www.nfpa.org/SmartFireFighting

[3] J. P. Blair and K. W. Schweit, "A study of active shooter incidents, 2000–2013," Texas State Univ. Federal Bureau Invest., U.S. Dept. Justice, Washington, DC, USA, Tech. Rep., 2014.

[4] J. Larsen, Ed., *Responding to Catastrophic Events*. Basingstoke, U.K.: Palgrave Macmillan, 2013.

[5] H. Ghafghazi, A. El Mougy, H. T. Mouftah, and C. Adams, "Classification of technological privacy techniques for LTE-based public safety networks," in *Proc. 10th ACM Symp. QoS Secur. Wireless Mobile Netw. (Q2SWinet)*, New York, NY, USA, 2014, pp. 41–50.

[6] C. Anderson *et al.*, "A network science approach to open source data fusion and analytics for disaster response," in *Proc. 18th Int. Conf. Inf. Fusion (Fusion)*, Jul. 2015, pp. 207–214.

[7] J. L. Barr, E. R. Burtner, W. Pike, A. M. B. Peddicord, and B. S. Minsk, "Gap assessment in the emergency response community," U.S. Dept. Homeland Secur., Washington, DC, USA, Tech. Rep. PNNL-19782, Sep. 2010.

[8] J. L. Barr, A. M. B. Peddicord, E. R. Burtner, and H. A. Mahy, "Current domain challenges in the emergency response community," in *Proc. 8th Int. ISCRAM Conf.*, vol. 1. Lisbon, Portugal, 2011, pp. 1–4.

[9] H. Ghafghazi, A. ElMougy, H. T. Mouftah, and C. Adams. (Feb. 2016). "Secure data storage structure and privacy-preserving mobile search scheme for public safety networks." [Online]. Available: https://arxiv.org/abs/1602.04493

[10] *Google Person Finder*, accessed on Feb. 2016. [Online]. Available: https://google.org/personfinder/global/home.html

[11] *Disaster Response on Facebook*, accessed on Feb. 2016. [Online]. Available: https://www.facebook.com/disaster/

[12] *Microsoft Solutions for Good*, accessed on Feb. 2016. [Online]. Available: http://www.microsoft.com/about/corporatecitizenship/en-us/nonprofits/solutions-for-good/

[13] S. R. Veil, T. Buehner, and M. J. Palenchar, "A work-in-process literature review: Incorporating social media in risk and crisis communication," *J. Contingencies Crisis Manage.*, vol. 19, no. 2, pp. 110–122, Jun. 2011. [Online]. Available: http://dx.doi.org/10.1111/j.1468-5973.2011.00639.x

[14] K. Kaminska *et al.*, "Digital volunteer supported recovery operations experiment," Defence Res. Develop. Canada, Ottawa, ON, USA, Sci. Rep. DRDC-RDDC-2015-R035, 2015.

[15] K. Starbird and L. Palen, "'Voluntweeters': Self-organizing by digital volunteers in times of crisis," in *Proc. SIGCHI Conf. Human Factors Comput. Syst. (CHI)*, New York, NY, USA, 2011, pp. 1071–1080. [Online]. Available: http://doi.acm.org/10.1145/1978942.1979102

[16] A. Gupta and P. Kumaraguru, "Credibility ranking of tweets during high impact events," in *Proc. 1st Workshop Privacy Secur. Online Social Media (PSOSM)*, New York, NY, USA, 2012, pp. 2:2–2:8. [Online]. Available: http://doi.acm.org/10.1145/2185354.2185356

[17] A. L. Hughes and L. Palen, "Twitter adoption and use in mass convergence and emergency events," *Int. J. Emergency Manage.*, vol. 6, nos. 3–4, pp. 248–260, 2009.

[18] A. Acar and Y. Muraki, "Twitter for crisis communication: Lessons learned from Japan's tsunami disaster," *Int. J. Web Based Commun.*, vol. 7, no. 3, pp. 392–402, Jul. 2011.

[19] M. A. Cameron, R. Power, B. Robinson, and J. Yin, "Emergency situation awareness from twitter for crisis management," in *Proc. 21st Int. Conf. World Wide Web (WWW)*, New York, NY, USA, 2012, pp. 695–698. [Online]. Available: http://doi.acm.org/10.1145/2187980.2188183

[20] S. Utz, F. Schultz, and S. Glocka, "Crisis communication online: How medium, crisis type and emotions affected public reactions in the Fukushima Daiichi nuclear disaster," *Public Relations Rev.*, vol. 39, no. 1, pp. 40–46, Mar. 2013.

[21] T. Heverin and L. Zach, "Microblogging for crisis communication: Examination of Twitter use in response to a 2009 violent crisis in the Seattle-Tacoma, Washington, Area," in *Proc. ISCRAM*, 2010, pp. 1–5.

[22] A. Bruns, J. E. Burgess, K. Crawford, and F. Shaw. #qldfloods and @qpsmedia: Crisis communication on twitter in the 2011 south east queensland floods. ARC Centre of Excellence for Creative Industries and Innovation, Brisbane, Australia, accessed on Feb. 2016. [Online] http://cci.edu.au/floodsreport.pdf

[23] *Smart911*, accessed on Feb. 2016. [Online]. Available: https://www.smart911.com

[24] J. Li, Q. Li, C. Liu, S. U. Khan, and N. Ghani, "Community-based collaborative information system for emergency management," *Comput. Oper. Res.*, vol. 42, pp. 116–124, Feb. 2014.

[25] B. Carminati, E. Ferrari, and M. Guglielmi, "A system for timely and controlled information sharing in emergency situations," *IEEE Trans. Dependable Secure Comput.*, vol. 10, no. 3, pp. 129–142, May 2013.

[26] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted data in cloud computing," in *Proc. 31st Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2011, pp. 383–392.

[27] B. K. Samanthula, Y. Elmehdwi, G. Howser, and S. Madria, "A secure data sharing and query processing framework via federation of cloud computing," *Inf. Syst.*, vol. 48, pp. 196–212, Mar. 2015.

[28] J. Sun, X. Zhu, C. Zhang, and Y. Fang, "HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare," in *Proc. 31st Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2011, pp. 373–382.

[29] R. Lu, X. Lin, and X. Shen, "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 3, pp. 614–624, Mar. 2013.

[30] X. Liang, R. Lu, L. Chen, X. Lin, and X. Shen, "PEC: A privacy-preserving emergency call scheme for mobile healthcare social networks," *J. Commun. Netw.*, vol. 13, no. 2, pp. 102–112, Apr. 2011.

[31] K. Zhang, X. Liang, M. Baura, R. Lu, and X. Shen, "PHDA: A priority based health data aggregation with privacy preservation for cloud assisted WBANs," *Inf. Sci.*, vol. 284, pp. 130–141, Nov. 2014.

[32] Y. Tong, J. Sun, S. M. Chow, and P. Li, "Cloud-assisted mobile-access of health data with privacy and auditability," *IEEE J. Biomed. Health Informat.*, vol. 18, no. 2, pp. 419–429, Mar. 2014.

[33] M. Barua, X. Liang, R. Lu, and X. Shen, "PEACE: An efficient and secure patient-centric access control scheme for eHealth care system," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2011, pp. 970–975.

[34] A. D. Brucker and D. Hutter, "Information flow in disaster management systems," in *Proc. Int. Conf. Availability, Rel., Secur. (ARES)*, Feb. 2010, pp. 156–163.

[35] B. Carminati, E. Ferrari, and M. Guglielmi, "Secure information sharing on support of emergency management," in *Proc. IEEE 3rd Int. Conf. Privacy, Secur., Risk Trust (PASSAT) IEEE 3rd Int. Conf. Social Comput. (SocialCom)*, Oct. 2011, pp. 988–995.

[36] S. Aguinaga and C. Poellabauer, "Method for privacy-protecting display and exchange of emergency information on mobile devices," in *Proc. Int. Conf. Collaboration Technol. Syst. (CTS)*, May 2012, pp. 596–599.

[37] J. Zhou, X. Lin, X. Dong, and Z. Cao, "PSMPA: Patient self-controllable and multi-level privacy-preserving cooperative authentication in distributed m-healthcare cloud computing system," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 6, pp. 1693–1703, Jun. 2015.

[38] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131–143, Jan. 2013.

[39] X. Liang, M. Barua, R. Lu, X. Lin, and X. S. Shen, "HealthShare: Achieving secure and privacy-preserving health information sharing through health social networks," *Comput. Commun.*, vol. 35, no. 15, pp. 1910–1920, Sep. 2012.

[40] Z. Wang, D. Huang, Y. Zhu, B. Li, and C.-J. Chung, "Efficient attribute-based comparable data access control," *IEEE Trans. Comput.*, vol. 64, no. 12, pp. 3430–3443, Dec. 2015.

[41] A. D. Brucker, H. Petritsch, and S. G. Weber, "Attribute-based encryption with break-glass," in *Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices*. Heidelberg, Germany: Springer, 2010, pp. 237–244.

[42] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2007, pp. 321–334.

[43] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Public Key Cryptography—PKC*. Heidelberg, Germany: Springer, 2011, pp. 53–70.

[44] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in *Automata, Languages and Programming*. Heidelberg, Germany: Springer, 2008, pp. 579–591.

[45] C. Chen *et al.*, "Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures," in *Topics in Cryptology—CT-RSA*. Heidelberg, Germany: Springer, 2013, pp. 50–67.

[46] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Advances in Cryptology—EUROCRYPT*. Heidelberg, Germany: Springer, 2010, pp. 62–91.

[47] N. Attrapadung and H. Imai, "Conjunctive broadcast and attribute-based encryption," in *Pairing-Based Cryptography—Pairing*. Heidelberg, Germany: Springer, 2009, pp. 248–265.

[48] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Advances in Cryptology—EUROCRYPT*. Heidelberg, Germany: Springer, 2011, pp. 568–588.

[49] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," in *Information Security Practice and Experience*. Heidelberg, Germany: Springer, 2009, pp. 13–23.

[50] X. Li, D. Gu, Y. Ren, N. Ding, and K. Yuan, "Efficient ciphertext-policy attribute based encryption with hidden policy," in *Internet and Distributed Computing Systems*. Heidelberg, Germany: Springer, 2012, pp. 146–159.

[51] J. Herranz, F. Laguillaumie, and C. Ràfols, "Constant size ciphertexts in threshold attribute-based encryption," in *Public Key Cryptography—PKC*. Heidelberg, Germany: Springer, 2010, pp. 19–34.

[52] N. Doshi and D. Jinwala, "Hidden access structure ciphertext policy attribute based encryption with constant length ciphertext," in *Advanced Computing, Networking and Security*. Heidelberg, Germany: Springer, 2012, pp. 515–523.

[53] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in *Applied Cryptography and Network Security*. Heidelberg, Germany: Springer, 2008, pp. 111–129.

[54] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology—EUROCRYPT*. Heidelberg, Germany: Springer, 2005, pp. 457–473.

[55] N. Attrapadung, B. Libert, and E. de Panafieu, "Expressive key-policy attribute-based encryption with constant-size ciphertexts," in *Public Key Cryptography—PKC*. Heidelberg, Germany: Springer, 2011, pp. 90–108.

[56] J. Horwitz, "A survey of broadcast encryption," *J. ACM*, 2003.

[57] D. R. Stinson, "On some methods for unconditionally secure key distribution and broadcast encryption," in *Selected Areas in Cryptography*. USA: Springer, 1997, pp. 3–31.

[58] D. R. Stinson and T. van Trung, "Some new results on key distribution patterns and broadcast encryption," *Designs, Codes Cryptogr.*, vol. 14, no. 3, pp. 261–279, Sep. 1998.

[59] M. Luby and J. Staddon, "Combinatorial bounds for broadcast encryption," in *Advances in Cryptology—EUROCRYPT*. Heidelberg, Germany: Springer, 1998, pp. 512–526.

[60] C. Gentry and B. Waters, "Adaptive security in broadcast encryption systems (with short ciphertexts)," in *Advances in Cryptology—EUROCRYPT*. Heidelberg, Germany: Springer, 2009, pp. 171–188.

[61] A. Fiat and M. Naor, "Broadcast encryption," in *Advances in Cryptology—CRYPTO*. Heidelberg, Germany: Springer, 1994, pp. 480–491.

[62] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in *Advances in Cryptology—CRYPTO*. Heidelberg, Germany: Springer, 2001, pp. 41–62.

[63] D. Halevy and A. Shamir, "The LSD broadcast encryption scheme," in *Advances in Cryptology—CRYPTO*. Heidelberg, Germany: Springer, 2002, pp. 47–60.

[64] M. T. Goodrich, J. Z. Sun, and R. Tamassia, "Efficient tree-based revocation in groups of low-state devices," in *Advances in Cryptology—CRYPTO*. Heidelberg, Germany: Springer, 2004, pp. 511–527.

[65] S. S. D. Selvi, S. S. Vivek, R. Gopalakrishnan, N. N. Karuturi, and C. P. Rangan, "Provably secure ID-based broadcast signcryption (IBBSC) scheme," in *Proc. IACR Cryptol. ePrint Arch.*, 2008, p. 225.

[66] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," in *Advances in Cryptology—CRYPTO*. Heidelberg, Germany: Springer, 2005, pp. 258–275.

[67] C. Delerablée, P. Paillier, and D. Pointcheval, "Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys," in *Pairing-Based Cryptography—Pairing*. Heidelberg, Germany: Springer, 2007, pp. 39–59.

[68] D. Boneh and B. Waters, "A fully collusion resistant broadcast, trace, and revoke system," in *Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2006, pp. 211–220.

[69] A. Kate, G. Zaverucha, and I. Goldberg, "Pairing-based onion routing," in *Privacy Enhancing Technologies*. Heidelberg, Germany: Springer, 2007, pp. 95–112.

[70] S. Capkun and J.-P. Hubaux, "Secure positioning of wireless devices with application to sensor networks," in *Proc. IEEE 24th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM)*, vol. 3. Mar. 2005, pp. 1917–1928.

[71] S. Čapkun, K. B. Rasmussen, M. Čagalj, and M. Srivastava, "Secure location verification with hidden and mobile base stations," *IEEE Trans. Mobile Comput.*, vol. 7, no. 4, pp. 470–483, Apr. 2008.

[72] R. M. Needham and M. D. Schroeder, "Using encryption for authentication in large networks of computers," *Commun. ACM*, vol. 21, no. 12, pp. 993–999, Dec. 1978.

[73] M. Bellare, R. Canetti, and H. Krawczyk, "Keying hash functions for message authentication," in *Advances in Cryptology—CRYPTO*. Heidelberg, Germany: Springer, 1996, pp. 1–15.

[74] I. Butun, M. Erol-Kantarci, B. Kantarci, and H. Song, "Cloud-centric multi-level authentication as a service for secure public safety device networks," *IEEE Commun. Mag.*, vol. 54, no. 4, pp. 47–53, Apr. 2016.

[75] X. Liang, Z. Cao, H. Lin, and J. Shao, "Attribute based proxy re-encryption with delegating capabilities," in *Proc. 4th Int. Symp. Inf., Comput., Commun. Secur. (ASIACCS)*, New York, NY, USA, 2009, pp. 276–286.

[76] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *Proc. 5th ACM Symp. Inf., Comput. Commun. Secur. (ASIACCS)*, New York, NY, USA, 2010, pp. 261–270.

[77] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.

[78] "GPS blue force tracking systems application note," U.S. Department of Homeland Security (DHS), System Assessment and Validation for Emergency Responders (SAVER), 2014.

[79] "Automatic vehicle locating systems-summary," U.S. Department of Homeland Security (DHS), System Assessment and Validation for Emergency Responders (SAVER), 2010.

[80] S. Kumar and E. H. Spafford, "A pattern matching model for misuse intrusion detection," Dept. Comput. Sci., Purdue Univ., West Lafayette, IN, USA, Tech. Rep. CSD-TR-94-013, Jun. 1994.

[81] R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext security from identity-based encryption," in *Advances in Cryptology—EUROCRYPT*. Heidelberg, Germany: Springer, 2004, pp. 207–222.

[82] C. Chen, Z. Zhang, and D. Feng, "Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost," in *Provable Security*. Heidelberg, Germany: Springer, 2011, pp. 84–101.

[83] 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.

[84] Y. Zhang, D. Zheng, X. Chen, J. Li, and H. Li, "Computationally efficient ciphertext-policy attribute-based encryption with constant-size ciphertexts," in *Provable Security*. Springer International Publishing, 2014, pp. 259–273.

[85] A. Ge, R. Zhang, C. Chen, C. Ma, and Z. Zhang, "Threshold ciphertext policy attribute-based encryption with constant size ciphertexts," in *Information Security and Privacy*. Heidelberg, Germany: Springer, 2012, pp. 336–349.

[86] Y. S. Rao and R. Dutta, "Recipient anonymous ciphertext-policy attribute based encryption," in *Information Systems Security*. Heidelberg, Germany: Springer, 2013, pp. 329–344.

[87] W. Teng, G. Yang, Y. Xiang, T. Zhang, and D. Wang, "Attribute-based access control with constant-size ciphertext in cloud computing," *IEEE Trans. Cloud Comput.*, vol. PP, no. 99, p. 1, doi: 10.1109/TCC.2015.2440247.

[88] R. Roman, C. Alcaraz, and J. Lopez, "A survey of cryptographic primitives and implementations for hardware-constrained sensor network nodes," *Mobile Netw. Appl.*, vol. 12, no. 4, pp. 231–244, Aug. 2007.

[89] L. B. Oliveira *et al.*, "TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks," *Comput. Commun.*, vol. 34, no. 3, pp. 485–493, Mar. 2011.

[90] Crypto++. (2009). *Crypto++5.6.0 Benchmark*. [Online]. Available: http://www.cryptopp.com/benchmarks-amd64.html

[91] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in *Public-Key Cryptography—PKC*. Heidelberg, Germany: Springer, 2013, pp. 162–179.

[92] D. M. Freeman, "Converting pairing-based cryptosystems from composite-order groups to prime-order groups," in *Advances in Cryptology—EUROCRYPT*. Heidelberg, Germany: Springer, 2010, pp. 44–61.

[93] A. Lewko, "Tools for simulating features of composite order bilinear groups in the prime order setting," in *Advances in Cryptology—EUROCRYPT*. Heidelberg, Germany: Springer, 2012, pp. 318–335.

[94] A. Guillevic, "Comparing the pairing efficiency over composite-order and prime-order elliptic curves," in *Applied Cryptography and Network Security*. Heidelberg, Germany: Springer, 2013, pp. 357–372.

HAMIDREZA GHAFGHAZI (S'14) is currently pursuing the Ph.D. degree with the School of EECS, University of Ottawa. He is currently involved in privacy preserving techniques for public safety networks. His research interests include applied cryptography, security and privacy, public safety networks, Internet of Things, cloud computing, and wireless sensor networks.

AMR ELMOUGY received the M.Sc. degree from Concordia University in 2006, where he was involved in channel coding techniques for MIMO-OFDM systems, and the Ph.D. degree from Queen's University in 2013, where he was involved in cognitive solutions for wireless sensor networks. He is currently an Assistant Professor with the German University in Cairo (GUC). He is currently leading several research projects in areas encompassing software-defined networks, Internet-of-Things, intelligent transportation systems, smart grids, security and privacy, and public safety networks. Prior joining GUC, he was a Post-Doctoral Fellow with the University of Ottawa, where, he was leading the project entitled An LTE testbed for public safety networks, which targeted the creation of a testbed for a modern communication network to be used by public safety officials. In this project, he was responsible for project management, coordination of efforts between academic researchers, industry partners, and government officials, and research on security and privacy for this network. He has supervised several Ph.D. and M.Sc. students and authored many publications.

HUSSEIN T. MOUFTAH (F'90) received the B.Sc. degree in electrical engineering and the M.Sc. degree in computer science from the University of Alexandria, Egypt, in 1969 and 1972, respectively, and the Ph.D. degree in electrical engineering from Laval University, Canada, in 1975. He joined the School of Electrical Engineering and Computer Science, University of Ottawa, in 2002, as a Tier 1 Canada Research Chair Professor, where he became a Distinguished University Professor in 2006. He was with the ECE Department, Queen's University (1979-2002), where he was prior to his departure a Full Professor and the Department Associate Head. He has six years of industrial experience mainly with Bell Northern Research of Ottawa (Nortel Networks). He served as the Editor-in-Chief of the *IEEE Communications Magazine* (1995-1997) and the IEEE ComSoc Director of Magazines (1998-1999), the Chair of the Awards Committee (2002-2003), the Director of Education (2006-2007), and a member of the Board of Governors (1997-1999 and 2006-2007). He was a Distinguished Speaker of the IEEE Communications Society (2000-2007). He has authored or co-authored ten books, 72 book chapters, and over 1400 technical papers, 14 patents, six invention disclosures, and 144 industrial reports. He is the joint holder of the 20 Best/Outstanding Paper Awards. He has received numerous prestigious awards, such as the 2016 R.A. Fessenden Medal in Telecommunications Engineering of the IEEE Canada, the 2015 IEEE Ottawa Section Outstanding Educator Award, the 2014 Engineering Institute of Canada K. Y. Lo Medal, the 2014 Technical Achievement Award of the IEEE Communications Society Technical Committee on Wireless Ad Hoc and Sensor Networks, the 2007 Royal Society of Canada Thomas W. Eadie Medal, the 2007-2008 University of Ottawa Award for Excellence in Research, the 2008 ORION Leadership Award of Merit, the 2006 IEEE Canada McNaughton Gold Medal, the 2006 EIC Julian Smith Medal, the 2004 IEEE ComSoc Edwin Howard Armstrong Achievement Award, the 2004 George S. Glinski Award for Excellence in Research of the University of Ottawa Faculty of Engineering, the 1989 Engineering Medal for Research and Development of the Association of Professional Engineers of Ontario, and the Ontario Distinguished Researcher Award of the Ontario Innovation Trust. He is a fellow the Canadian Academy of Engineering (2003), the Engineering Institute of Canada (2005), and the Royal Society of Canada RSC Academy of Science (2008).

CARLISLE ADAMS is a Professor with the School of Electrical Engineering and Computer Science, University of Ottawa. His research interests and technical contributions span applied cryptography, security, and privacy, including the CAST family of symmetric encryption algorithms, secure protocols for PKI environments, access control in electronic networks, and privacy enhancing technologies.