

SPECIAL ISSUE PAPER

Victim detection platform in IoT paradigm

Minsung Hong  | Rajendra Akerkar

Big Data Research Group, Western Norway
Research Institute, Sogndal, Norway

Correspondence

Rajendra Akerkar, Big Data Research Group,
Western Norway Research Institute, 6856
Sogndal, Norway.
Email: rak@vestforsk.no

Present Address

Rajendra Akerkar, Big Data Research Group,
Western Norway Research Institute, 6856
Sogndal, Norway.

Funding information

Research Council of Norway (RCN);
Norwegian Centre for International
Cooperation in Education (SiU), Grant/Award
Number: INTPART program

Summary

The advent of Internet of Things (IoT) paradigm is having a great ripple effect in the field of disaster management as well as many other areas. Victim detection has been studied as rescuer- or victim-oriented approach, which utilises the IoT advanced technologies, but they have weaknesses according to disaster types. In this paper, we propose a Victim Detection Platform (VDP) architecture combining both approaches using various advanced technologies such as IoT, drone and edge/cloud computing to offer higher quality services, which ultimately result in swifter, better responses and more lives saved. First, we have reviewed related literature regarding three crucial issues (ie, multi-modal evaluation for reliable data, edge-based real-time response, and privacy-preserved Big Data analysis) to satisfy the service. In order to achieve these important aspects, the VDP architecture is described along with roles/relations of technologies and concepts leveraged to and data sources considered in the platform. To explore the realisation possibility of the proposed approach in real disasters, a validation scenario considering the critical issues and details in a victim detection task is illustrated, and then appropriate techniques, which will be utilised in the proposed VDP, and its justifications are discussed. Finally, we debate how the techniques are harmonised in the VDP and what the challenges are.

KEYWORDS

data privacy, disaster management, edge computing, Internet of Things, multi-modal evaluation, victim detection

1 | INTRODUCTION

Over the past few years, IoT has attracted much attention from both industrial and research communities, and it represents a network consisting of physical objects such as sensors, mobiles, buildings and vehicles in which software and electronics are embedded to connect with Internet and to enable collecting and exchanging data between them.^{1,2} Although IoT techniques cannot directly stop disasters from happening, but as the complementary technology to a poor infrastructure, it is very useful for disaster management, such as disaster predictions, early warning systems and rescue operations.^{3,4}

On the other hand, cloud computing has extensively been leveraged for various services such as analysing Big Data generated from and implementing applications worked in the IoT environment.^{5,6} However, due to the essential characteristics of disaster management tasks requiring precise and effective decision making timely (almost near real-time), cloud computing technology might lose its powerful capabilities. For instance, the delay and latency in interaction between IoT devices and cloud computing layer could be directly linked with the loss of lives of millions of people and tremendous, grave and irrevocable societal damage, in disaster situations. One of the possible ways to overcome this weakness of cloud service is edge computing.³

The quick detection of victims potentially trapped in buildings as a result of all sorts of disasters of natural, accidental, man-made or terror origin is a major issue for first responders. However, as shown in Figure 1, in most of disasters such as building collapse and flood, victims are frequently buried by the debris of building or the earth and sand, eg, Savar building collapse (2013) at the left bottom of the figure. Furthermore, according to types of disaster, the distribution of victims can be concentrated in a small area or extended over a very wide area. In case of disaster impacting a large area such as Takahashi Riber flood 2018 on the figure, the capacity of first responders may be too distributed and limited.

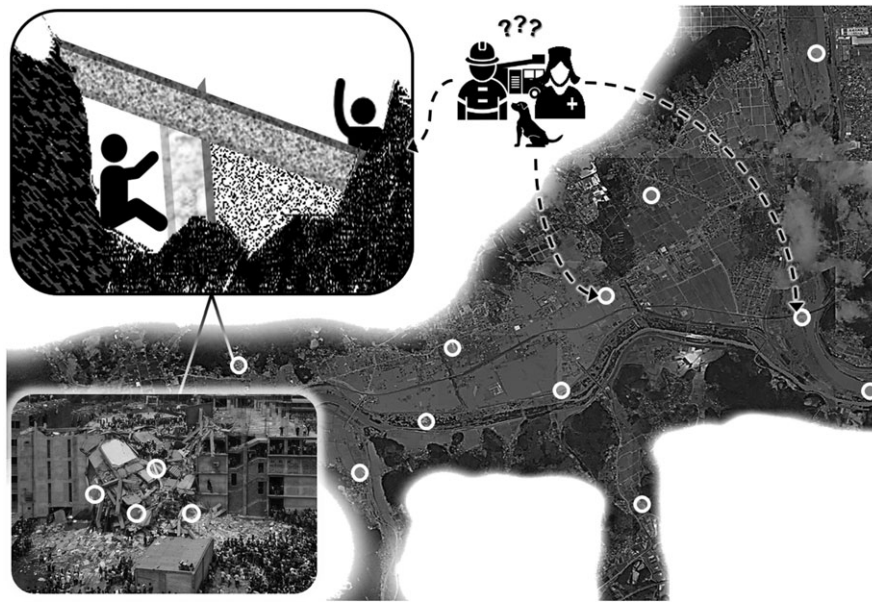


FIGURE 1 General scenes in disasters

Such environment presents unique challenges with all being opaque to human vision. While using advanced technology, caution must be exercised since failure to detect a response can result in victims not being found. On the one hand, false alarms cause a waste of valuable resources. As a result, current rescue teams commonly employing audible detection of victims' cries for help, trained sniffer dogs and cell phones have been pressed by timeliness and effectiveness. Thus, advanced technologies making quick and correct situational awareness of disaster possible should enable the first response teams to save the time taken to detect victims who are clearly invisible, enabling efficient and faster rescue operations leading to higher chances of saving lives and reducing injuries.

In this paper, we propose an architecture of Victim Detection Platform (VDP) in the era of IoT. It aims to integrate various technologies considering sensing, communication, and computing issues to offer higher quality services, which may ultimately result in swifter, better responses and more lives saved. The proposed VDP considers following three critical issues of existing victim detection platforms.

- Although there are many ways to detect victims including acoustic and gas sensors, etc, limitations exist for every single detection technology, and a combination of these different approaches is not seriously considered in previous research studies.⁷ Furthermore, in case of involving various data such as sensor data and social media data, it causes many critical issues (eg, noise in data, contradiction between data, irrelevant data, and malicious rumour) related to reliability of data and information.⁸ These substantially affect not only trust and performance of a system but also damage of assets and loss of lives in real world.
- While some recent computing technologies have been used for detecting victims, there are few studies for an autonomous communication configuration and edge computing of real-time victim detection, compared with other tasks in disaster management. In addition, most of research studies related to victim detection have focused on either local-area or wide-area situational awareness with the advanced technologies and been attempted in one specific disaster.
- As aforementioned, to achieve an effective and efficient wide-area situational awareness, victim's IoT devices, in which personal data is usually saved, should be involved in the disaster management system. Therefore, although disasters could be thought as a severe situation that can ignore a part of individual privacy, this issue must be carefully considered and handled in trade-off between disclosure risk and information loss.⁹

More specifically with respect to these issues, the concrete features of the proposed platform include the following.

- **Multi-modal evaluation for reliable data and information:** This has roles of preprocessing and detecting multi-modal data, as fusion processes eliminating vain or unreliable data, for reliability of data and information.
- **Edge-based communication and computing for real-time response:** It is responsible for local and wide-area situational awareness to provide lasting communication network and conduct efficient response in real-time.
- **Privacy-preserved data-driven analysis:** This can be accomplished through considering edge nodes, which protect private data and transfer only limited and preserved data. Furthermore, this method is able to achieve differential privacy.

To introduce and discuss the proposed VDP, we first review related works to figure out vital elements of victim detection approaches using advance technologies in disasters. Regarding these important points, the proposed VDP is described, and then related concepts and technologies, data sources used, architecture and sub layers' roles belonging to the proposed approach are discussed in turn. To show feasibility of our platform,

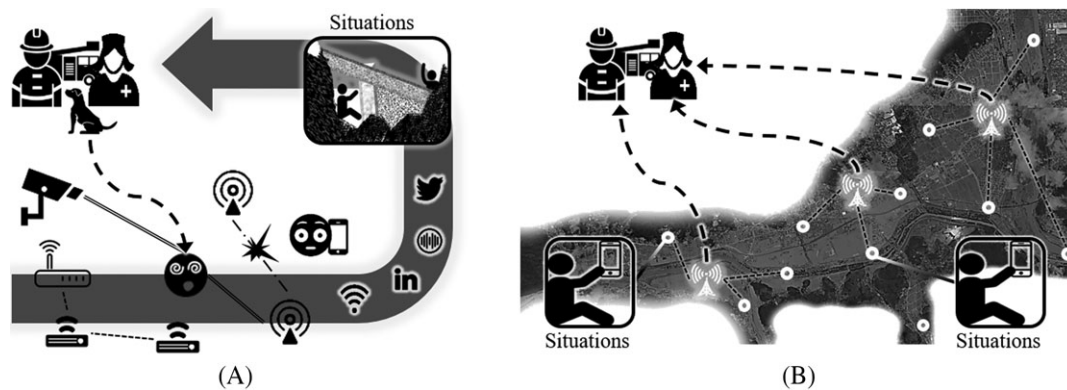


FIGURE 2 Two current approaches for victim detection. A, Rescuer-oriented approach; B, Victim-oriented approach

with a validation scenario considering the crucial requirements, we introduce appropriate techniques, which will be utilised and debate how they are harmonised in our architecture. Then, challenges for realising our platform in real world are described. Finally, conclusion is presented.

2 | RELATED WORK

2.1 | Victim search-and-rescue

Existing victim detection methods can be categorized into two groups, namely, rescuer-oriented and victim-oriented approaches. Emergency managers and first responders can get aware of the situation at the scene by drawing on and using affected civilians' location data, imageries taken by unmanned air vehicles (UAV), texts, videos and images from social media, Wi-Fi signals and Bluetooth beacon-based detection, acoustic sensors, and Doppler radars, as shown in Figure 2.

The rescuer-oriented approaches require active and focused involvement of rescuers. While these methods utilise recent sensing and ICT technologies, they are inefficient for some situations where the affected area is large such as 2018 Japan floods. Recent studies and projects propose to use robots and ICT technologies to support victim search and rescue (SAR) in disasters, particularly when looking for affected people, gathering information and communication.¹⁰ The first real use of robots took place during the response effort of the World Trade Centre attacks on September 11, 2001. Data collected from the incident has been analysed in detail.¹¹ Despite there is a negative assessment about the role of robots in disaster management, the recent advance of technologies provides small size, simplicity, high reliability and low cost of them.¹² Thereby, many papers have recently been published to support detecting victims. For example, NimbRo robot has been developed to rescue victims in disaster scenarios like the Fukushima nuclear accident, with a danger of collapse or toxic contamination.¹³ However, compared to the more general topic of human detection, the disaster scenario having been used can only be considered a small niche and it appears that a large portion of the research is related to the robotic initiatives such as Robocup and DARPA. Moreover, it is difficult for that kind of robots to be effectively operated in wide-area disasters such as flood, tsunami and earthquake, due to the extensivity, whereas regarding the increase of recent papers studying UAVs, a drone has been raised as one of the efficient alternatives for dealing with a broad affected area.^{14,15}

In contrast, the victim-oriented approaches actively involve the participation of the IoT devices owned by the victims. For example, cell-phones can send cellular and Wi-Fi signals to other devices and base stations in vicinity. The problem of these kind approaches based on fixed infrastructures is difficulty to provide the lasting communication from the IoT devices to rescuers, since a natural disaster like earthquake and tsunami would possibly result in the failure of cellular base stations. Thereby, there have recently been conducted studies on leverage aircraft especially drones as intermediators to connect with IoT devices owned by victims.¹⁶ Radio observations such as global system for mobile communications (GSM) and Wi-Fi are usually available for this purpose.¹⁷ However, in these approaches, the IoT devices only have passive roles such as broadcasting locations of victims through beacon.¹⁸ In addition, there are some limitations such as battery life of a device, radio signal power and victim's activity status.¹⁹ Valuable opportunity of obtaining useful and enrich victim-side data such as various sensor data and social media data should be kept.^{20,21} While the rescuer-oriented approaches have been discussed thoroughly in recent years especially the image recognition-based victim detection, victim-oriented approaches are still under-explored.

2.2 | Multi-modal evaluation

Data fusion regarding post-disaster victim detection will help in gaining the current available knowledge and experience,^{22,23} which, in turn, will be useful in decreasing the overall cost of these activities. In addition, multi-modal data fusion in post-disaster management helps in analysing, discovering and organising all the pertinent information.²⁴ Typical devices used for victim detections include snake-like cameras, fiberscopes, sensitive listening devices and measuring devices such as laser rangefinders, strain gauges, and levels. Recent studies focus on a use of more

diversified ICT technologies including ultra-wideband radar, Infrared Camera, Lidar sensor, and social media.^{25,26} Every single technology has some limitations due to the capability of the sensing and communication technology used.²⁷ For example, UWB radar faces the challenge of low signal-to-noise ratio conditions, which affects the detection accuracy drastically. Social media approach depends on a connected environment, which could be unavailable in a post-disaster scenario, especially for earthquake. Of course an approach focusing on single data resource may not work when corresponding sensors are destroyed by disaster. Some studies showed that the use of multi-model approach is promising for people detection.^{7,28} However, a use of multi-model approach for victim detection considering different sensing and detection technologies is still under-explored. Moreover, one of important issues is to keep data reliability against noise data, contradictory data, irrelevant data, malicious rumour and so on.²⁹ Although there is a large amount of papers attempting to conserve data reliability in the field of IoT,³⁰⁻³² research and discussions about trustworthiness of data and information from multi-sources in the field of disaster management are still few, despite the important issue related to human life. In the proposed VDP, multi-modal data is modelled and learnt by deep neural network based on the powerful resources of cloud. The model is used for edge nodes to improve effectiveness and efficiency of edge level by reducing transmission of useless data.³³

2.3 | Edge-based communication and computing

Many studies discussed about edge computing technologies to improve the situational awareness of a system by using efficient content caching and computing on edge nodes.^{34,35} For example, Cloudlet and fog computing move a part of responsibilities from cloud to edge for reducing the communication delay and providing local computing and storage support.³⁶ That is to say, in case of disaster management, the edge computing could offer rescue for victim in (near) real-time by reducing the data transmission delay between edge nodes and decision making. While these works have focused on the advantage of edge computing, the edge selection problem in a decentralized network is not discussed seriously.³⁷ To continuously communicate between edge nodes even in disaster situations having destroyed infrastructures, mobile ad hoc network (MANET) techniques have been studied for independent, dynamic and self-adaptive networks consisting of wireless mobile nodes for SAR in disaster situations with less infrastructure or without.^{38,39} Due to drawbacks of position-based MANET demanding additional data about the physical location of each node, existing research studies have focused on hybrid methods (proactive- and reactive-based) as a topology-based approach for the SAR task.⁴⁰ However, our platform has more choices, since we leverage drones as edge nodes capable of providing their physical locations. Furthermore, there are few studies^{36,41} to apply edge computing to disaster management as well as victim detection, and the cooperation between non-edge nodes is still not addressed.⁴² In a post-disaster scenario, the communication capability of each node is limited; thus, a cooperation between non-edge nodes should be efficiently utilized to improve the performance of a system.

2.4 | Privacy-preserved data analysis

In the field of disaster management, privacy issues have mostly been considered in studies^{43,44} related to healthcare because of the personal data being handled, such as genome and health records rather than data of natural or man-made disasters. On the one hand, a lot of attention from IoT research studies has been drawn for ensuring the confidentiality of data collected from heterogeneous IoT devices, the secure transmission, the integration and aggregation in middleware/edge devices, as well as the privacy-preserving data analytics.^{45,46} In this regard, in disaster situations, combination of disaster management and IoT means that the personal data is possibly easier to be gathered through various devices. That is to say, data privacy is one of the most critical issues for disaster management even if not directly related to healthcare. Data protection could be divided into three approaches (ie, data-, computation- and results-driven methods) according to the intended usages.⁹ This paper utilises data/information fusion for data privacy regarding to techniques' advantages such as reducing useless data transmission and leveraging diversity for complementarity. We should choose appropriate protection methods by considering the importance of data correctness being required in SAR tasks related to human lives at the scene of disasters. Thus, the proposed VDP uses multivariate microaggregation as one of data-driven methods to get at least approximate results with original data.⁴⁷ Moreover, non-perturbative approaches such as (sub-) sampling methods are introduced to avoid distortion of the original data. Of course, cryptographic protection methods will be applied to keep original data in case of vital data directly connecting with human lives.

3 | VICTIM DETECTION PLATFORM

Although there are more advanced technologies to enhance current approaches, a combination of both approaches through drone technology can be imagined. Regarding this, Figure 3 shows the concept of VDP. For disasters which affect wide area, the victim-oriented approach efficiently provides information about the situation of extensive area (ie, wide-area situational awareness). Even though cellular base stations break down by disasters, they could be replaced with UAVs as a communication intermediary. First responders obtain information about the overall situation of the wide area and then decide which plan is best for saving people's life. During rescuers' arrival to a disaster scene, they may figure out victims' situations using a variety of data from various resources such as sensors and social media for quickly and safely starting relief operations (ie,

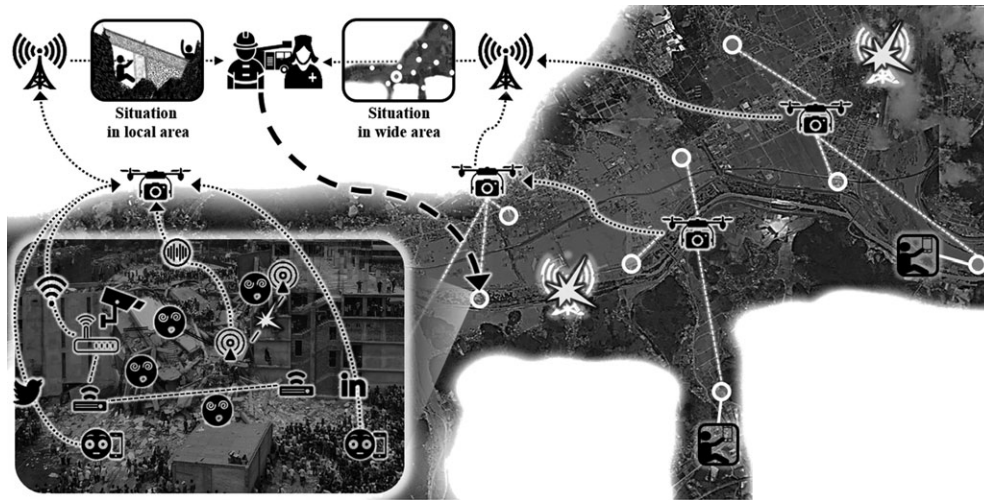


FIGURE 3 Hybrid approach with drone technique

local-area situational awareness). In this case, the UAVs could have various roles as, not only mediators and observers but also quick analysers. A combination of these two types of situational awareness is very important for rapid, efficient and effective rescues, because of its more rigorous requirements (eg, timeliness and resource limitation) in disasters.

With respect to reviews in Section 2, the proposed VDP focuses on intelligence coming down to three aspects.

1. **Multi-modal evaluation:** Its role is processing and detecting multi-modal data for data fusion. In addition, to maintain reliability of data and information, trust modelling and model learning are conducted for the multi-modal data (ie, sensor and social media data) by deep neural networks, based on powerful resources of cloud system. The learned model is then propagated into edge level for effective and efficient edge analysis. In particular, note that it is important to preprocess or filter duplicated and vain data in edge nodes with respect to preventing useless usage of limited resource and to improve effectiveness and efficiency of cloud computing.
2. **Edge-based communication and computing:** It is responsible for local- and wide-area situational awareness to efficiently and continuously response in real-time. To do this, in the edge layer level, autonomous network configuration is performed with UAVs as intermediate devices (ie, edge nodes) among others such as sensors and drones, whereas in the cloud layer, various artificial intelligence (AI) techniques such as online optimisation are introduced for deployment and reallocation of resources including drones.
3. **Privacy-preserved data-driven analysis:** As aforesaid, a system working with personal devices may have many possible problems related to privacy. Likewise, with purposes of edge analytics, data aggregation is conducted in each edge node for both data protection and elimination of vain or unreliable data. In the cloud layer level, information fusion is conducted based on privacy-preserved data sampled and randomised in edge nodes before transmission of the information to analysis parts such as online optimisation, trust modeling and model learning.

3.1 | Advanced techniques in VDP

Figure 4 illustrates the VDP overview including components and their functions to achieve upper intelligence. Details will be explained along with its modules in Section 3.3. Roles of and relations among major techniques and concepts being considered in the proposed VDP are described as follows.

- **Internet of Things and Big Data:** IoT is the proposed VDP's basis concept based on the fact that involved devices should be continuously connected with Internet to timely operate first rescue, even in a situation in which fixed infrastructure, such as cellular base stations, is destroyed. Simultaneously, together with Big Data, IoT also means an environment in which appropriate data from a variety of resources are rapidly being collected in VDP and correct operations of first response are assured. In this regard, these two concepts are used for multi-modal data evaluation and privacy-preserved data-driven analysis.
- **Edge and Cloud Computing:** They work as physical and cyber infrastructures of VDP in IoT and Big Data environment. These computing techniques complement each other to exclude their weaknesses such as response delay of cloud computing and resource shortage of edge computing. For instance, since edge nodes including software for analysis are close to victim, they can figure out an approximate (but sufficiently effective) situation in disasters and effectively support rescue team to save victim's life faster than using cloud resources. On the other hand, in order to provide more precise results, cloud computing based on its powerful resources has a role for handling heavy and large problems that are hard to be processed by resources of edge computing. In addition, in VDP, they are related to autonomous network configuration for communication and deploying and reallocating rescue resources such as drones.

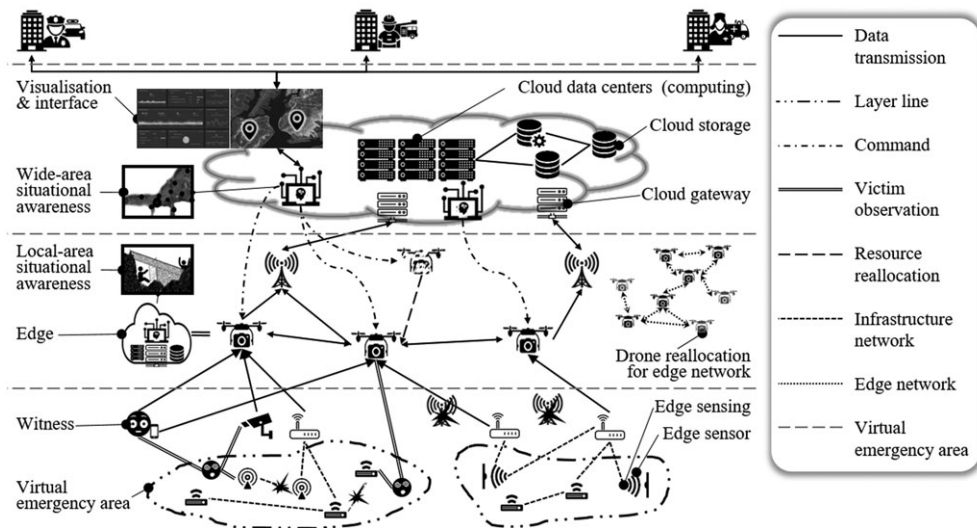


FIGURE 4 Overview of victim detection platform

- Artificial Intelligence:** Although data mining and machine learning methods also play important roles, we can say that AI is a more crucial technique in the proposed platform, because AI techniques, pervading from edge nodes to cloud, perform major functions of VDP. These methods mainly conduct local- and wide-area situational awareness and also support other functions such as trust modelling and learning model through deep neural network in cloud layer. In particular, VDP considers online optimisation and multi-criteria/multi-objective problems for autonomous network configuration and deployment/reallocation of resources, since disaster situations are mostly complicate and incomplete. In addition, we need to consider techniques (eg, sampling and iteration skipping) of approximate computing to reduce relatively long response latency of such AI techniques, as it will be discussed in Section 4.

3.2 | Data sources

This section describes data in VDP, as shown in Figure 5. These data are able to be classified as follows.

- Sensor data from a variety of sources:** These kinds of data are gathered through edge sensing from edge nodes. According to sensor types, collected data forms varies, ie, continuous or discrete numerical data, ordinal or categorical data. Thus, we should use appropriate algorithms and methods for these data types. Sensors of proximity, pressure, smoke, motion detection, humidity, optical and acoustic sensors or a sensor smart phone sensors could be used to detect buried victims and aware situations in vicinity.
- Social media data related to disaster:** Leveraging these data containing a text, an image and a video to disaster management has been studied for various tasks and been proved its effectiveness for not only detecting a disaster but also assessing its damage.⁴⁸ Particularly, texts like tweets have been mainly utilized; also, images belonging to involved imageries and videos have been analysed through advanced techniques such as neural networks for disaster management. However, as aforementioned, the relevance of these data must be evaluated, because of their characteristics related to ordinary life or malicious rumour.
- Edge communication network data:** This category is divided into two kinds of data, ie, edge nodes' and communication status-related data. For example, to optimise the distribution of drones and improve effectiveness and efficiency of communication in drone network, corresponding modules needs data related to network component's dynamic status such as location, battery and throughput. These data should be filtered and transferred according to their usefulness due to problems of traffic increase and restricted resources.
- Command and feedback data for rescuers:** Even if VDP would detect victims well, it cannot directly save people's lives without rescuers. Furthermore, feedback from rescuer teams might be the most important data being obtained from the closest places to the disaster scene by reliable data providers (ie, rescuers). Thus, command and feedback data between managers and first responders should be applied to VDP's related functions (eg, deployment of relief resources such as drones) in advance to support rescue operations.
- Statistical and environmental data for disaster:** These data include disaster-related information such as formal datasets and sensing data in the past or present. Since disasters are extremely different according to their types, and rescue operations are very affected by dynamic environments such as weather and climate, from distributed sensors and public facilities, cloud computing layer should rapidly collect and analyse these data to provide appropriate decisions in real-time.

The proposed VDP uses significantly various data. Although it gives us many challenges, it also provides valuable opportunities. For instance, one type of data indicates only part of situational awareness, while usage of various data provides diversified aspects to gain more precise overview over situations. In particular, it allows us to perform cross-evaluation for obtaining reliable data and information.

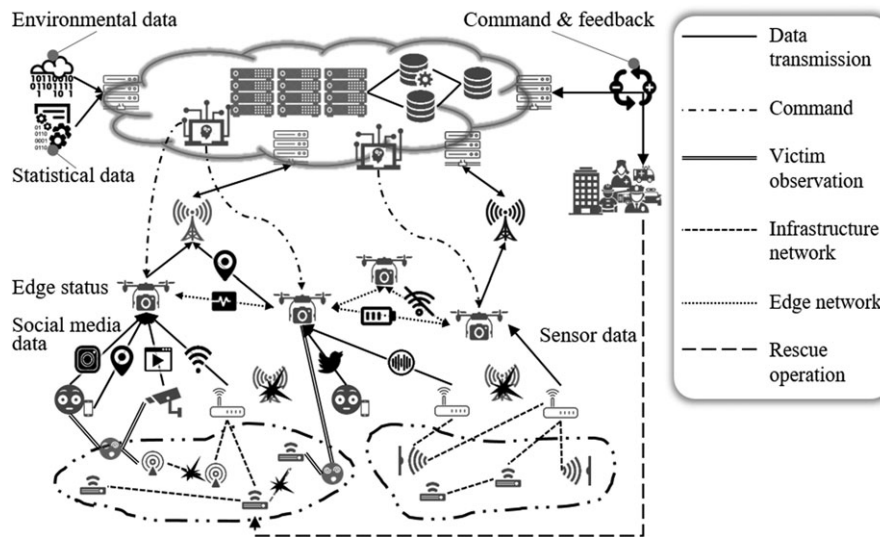


FIGURE 5 Data flow of victim detection platform

3.3 | VDP architecture

In large-scale disasters, data-driven disaster response is usually rather challenging as the underlying communication networks are also been disrupted. Hence, building a resilient network for data collection and dissemination is essential for effective disaster response. Besides, the emergency communication networks (ECNs) need to be immediately established to response to disaster operations. For example, the ECN centre can collect messages from disaster areas and notify the victims who require disaster-relief actions. Based on the constructed resilient communication networks and mobile-based ECNs, heterogeneous data sources will be gathered that include automated and human sensor data, mobility and communication data, online social network data and public government data as mentioned in Section 3.2.

Based on such data, in order to address urgent needs, protect first responders against multiple and unexpected dangers and enhance their capacities, VDP efficiently integrating different technologies considering sensing, communication, and computing issues is proposed. It aims to achieve a significant reduction of response time related to victim SAR phase by providing situational awareness solution of both wide-area and local-area for improving detection and localisation of trapped victims. In particular, the overall concept of VDP is to create multi-modal victim detection based on multi-access edge computing technology. The platform is used to inform first responders on how to improve disaster rescue planning, as well as to save the time taken for detecting victims who are not visible, enabling more efficient and rapid rescue operations.

In this regard, as shown in Figure 6, VDP consists of four different layers, namely, local coordination, edge-assisted intermediary, organizational coordination and interaction layers. The first layer coordinates communication between sensors to enable a local storage of sensed data without relying on a communication infrastructure. The second, edge computing layer, integrates data from the first layer and then filters and analyses the data at any edges (eg, sensors, actuator, gateways and smart mobiles), which have capabilities of storage and computing power, before sending it to cloud. The third layer conducts online optimisations related to rescue resources based on Big Data analytics. Finally, the last layer defines concrete steps towards a more efficient rescue operations according to the information collected and analysed from other three layers.

3.3.1 | Local coordination layer

This layer is in charge of conducting efficient communication between sensing devices, which are involved during a response process, such as personal devices and drones in sensing of social infrastructure. These device nodes have embedded intelligence, perform professional tasks, and collaborate with each other through service interactions. In this layer, there are three aspects, ie, communication standards according to the range of the infrastructure, various sensors and devices belong to the infra for sensing data from people, machines and environments, and relevant multi-modal data from such devices.

3.3.2 | Edge-assisted intermediary layer

It supports or replaces an infrastructure that is not intelligent enough to handle disaster situations through equipping with rich sensors and connectivity. This layer includes following sub-parts: (1) a multi-modal-based detection extracts the victim information by using a variety of data from different sources with considered reliability; (2) data fusion performs sampling, randomising and aggregation to preserve data privacy; (3) to achieve lasting a network communication and reduce traffic and response delay between edge nodes (ie, drones), an autonomous network configuration is performed based on edge status data; (4) as a key of swift wide-area situational awareness, the communication constructed between edge and cloud computing layers is optimised with considering results about its coverage and throughput analysed by the cloud layer;

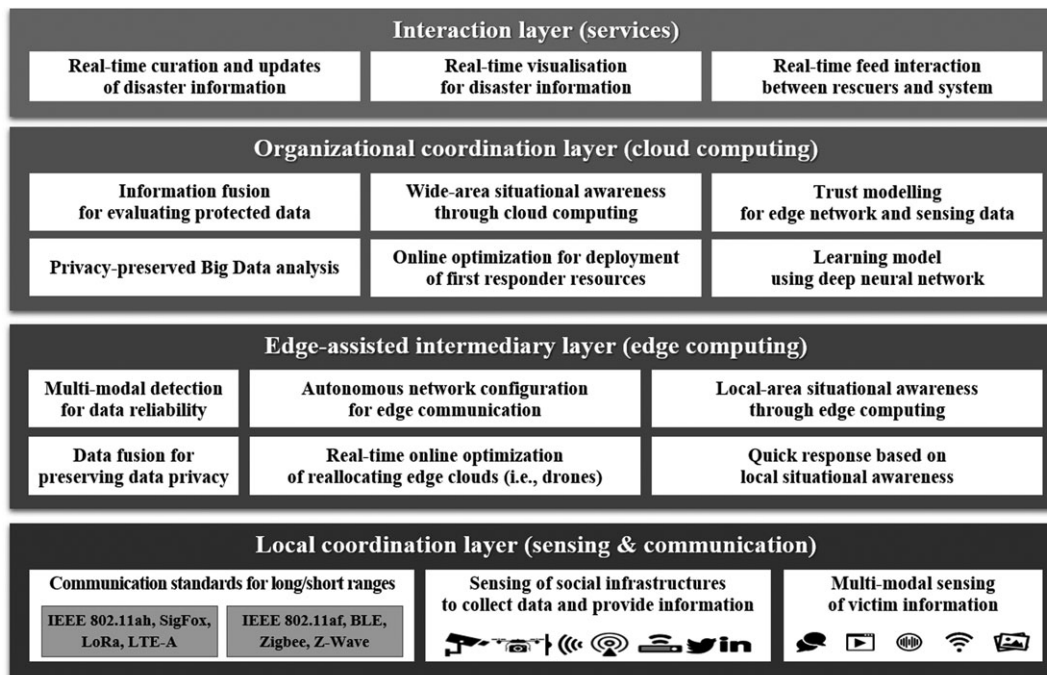


FIGURE 6 Architecture of victim detection platform

(5) each edge node is connected with physical local area and aware of its situations based on computation and caching of themselves; and (6) quick responses based on the local situational awareness are simultaneously progressed at this layer to reduce delay from the upper cloud layer.

3.3.3 | Organisational coordination layer

More complicated computation and more correct decision making is carried out at this layer with a huge computational power and a large of storage, as follows. (1) Multi-modal data is modelled and integrated through an information fusion processing. It could be conducted with considering privacy preservation and data reliability. (2) Big Data analysis based on only essential data could be efficient for an online optimisation to quickly provide results to the first responders. It also considers other data (command and feedback for rescuer teams and statistical and environmental data related to disasters). (3) Results of the optimisation of data locally gathered are combined for wide-area situational awareness, and then they are used to make decisions about actions such as supporting first responder's, drone's, or volunteer's resources and evacuation warning. (4) Based on the situations of wide-area and edge network, distribution plans of resources such as UAVs are established through an appropriate online optimisation technique. (5) The heterogeneous and huge data easily contains unreliable data such as ordinary posts in social media or error data from sensors. In this regard, trust of these various sources should be managed by trust modelling. (6) The model could be learnt with deep neural network for near- or far- future works, based on enriched computation resources. Parameters being a result of a model learning will be propagated into edge computing layer to filter useless data and reduce the amount of transmissions.

3.3.4 | Interaction layer

This layer is important in first response, with respect to following aspects. (1) Real-time information fusion and update are needed to interact with stakeholders to make more effective and efficient decisions. (2) Interactive visualisation techniques offer recent information of wide- and local- area situations with intuitive and easy ways to first responders such as police, fire station and hospital. (3) Prompt responses of VDP could be achieved through the real-time and cumulative operation results of the proposed framework and the continuous interaction experience with stakeholders in disasters.

4 | DISCUSSION

In order to show feasibility of the proposed architecture and discover relevant challenges, this section presents simple but sufficient validation scenarios based on important issues of victim detection in disaster management discussed in Section 2.

4.1 | Validation scenario

Victim detection processes require rapid and correct situational awareness about critical requirements with respect to huge loss of properties and people's lives. In the case of disaster affecting wide area such as flood or earthquake, it will be crucial for SAR operations based on wide/local-area situational awareness because of difficulty in positioning the victims. Therefore, appropriate techniques should be introduced in situational awareness to achieve timeliness and correctness. However, these two purposes sometimes have trade-off relation, since correct decisions might be more easily and harmoniously reached through large amount and variety of data rather than by small and single data. In other words, it means that data analysis based on small and single data can help to make sufficient decisions in short time. Therefore, techniques required for situational awareness in disasters should satisfy both requirements (ie, having computation capacities for large/varied data in real-time).

In addition, it is able to be assumed that people could share social media feeds about an affected area and upload sensing data from a variety of sensors embedding into their personal devices, through communication network including edge nodes. There are two issues about data reliability. One is that social media data should be distinguished from general data related to normal issues (eg, water pollution or beverage advertisement), or ordinary life. Another is that we should judge the reliability of data from sensors, according to whether the data is generated in a normal situation or unusual situations caused by disaster or sensor flaw.

In another possible scenario, those personal devices are able to send its cellular signals including GPS to base stations. Even when the devices' battery runs out, last GPS signal can be used to select potential locations of victims. That is to say, personal data gathered from mobiles or tablets are useful for SAR. On the other hand, transmission and storage of these data from the personal devices should be cautious, even in a very special situation like disaster, when urgency might seem to be looked more important than the personal information protection. Thus, since collected data may much more easily contain sensitive data by the era of Big Data being more accelerated with IoT, it is essential that advanced technologies used for victim detection should have capability to deal with privacy issue.

4.2 | Harmonisation of techniques for VDP

This section discusses techniques that are proper for the victim detection and how they are harmonised in the proposed architecture. There are four following purposes of using various techniques in VDP.

- (i) **Continuous providing communication network:** has some requirements such as edge nodes replacing base stations, node deployment through optimisation and suitable communication standards.
- (ii) **Reliable data through multi-modal data fusion:** could be obtained in IoT environment,⁴⁹ like the example in previous scenario. First, social media data should be judged in its relevance with disasters before used for victim detection. The reliability of data from a variety of sensors must be verified against sensor flaw, transmission delay and so on. These processed data are important to make appropriate decisions in SAR tasks and to reduce useless waste of resources in urgent situations.
- (iii) **Situational awareness for wide/local- area in real-time:** should be conducted with a large amount (and variety) of data in real-time and serve correctness at the same time. Therefore, edge computing assigning computation power and data storage in the environment in which it is needed, as close as possible, is necessary.
- (iv) **Privacy-preserved Big Data analysis:** is endangered by indiscriminate collection. However, it can be achieved through proper restrictions for usage and transmission coverages of personal data. For example, such original data is only stored in personal devices and then transferred to other layers after appropriate preprocessing.

As mentioned in the scenario, UAVs have a role of intermediary to replace base stations which are destroyed by disasters. In order to provide continuous communication between disaster scene and VDP, drones compose mobile ad hoc networks (MANET). Although there are various kind of routing protocols, position-based MANET routing protocol is appropriate in the proposed VDP, since each drone can transfer its GPS signal to cloud layer.⁴⁰ On the one hand, hierarchy routing could also be a proper candidate, because it allows to decline drones' weight and burden, to save battery and to increase activity time by dividing roles into connectors (ie, managers) and observers. Therefore, to achieve the aim (i), we consider a hybrid routing protocol based on position and topology-based MANET routing protocols. In order to deploy edge nodes into proper locations with considering deficient resources and dynamic situations, evolution strategies as one of genetic optimisation algorithms are suitable.⁵⁰ However, multi-objective optimisation problems (MOOPs) should also be managed, since MANET based on UAVs have various constraints such as saving low battery and improving throughput of data transmission, providing continuous communication and increasing scalability of network coverage. In addition, detecting personal devices through UAVs generally uses Wi-Fi or Bluetooth signals from the devices. In this case, there are two possible methods. One is detection based on an application which provides Mac address of installed mobile. Another is finding Wi-Fi emission without the application. Of course, the former is better for improving detection accuracy and saving batteries of drones and mobiles.¹⁸ There are many standards like IEEE 802.11a/b/g/n/ah/af and Bluetooth 2.0/4.0, the IEEE 802.11ah appropriate with its wide coverage (over 1000 m) and high data throughput (78 Mbps).

The heterogeneity and sheer volume of data being harvested in disasters require high reliability and ultra-low latency for rapid and correct first response. To improve reliability and latency requirements as the objective (ii), optimal processing methods must be conducted by cross-evaluation through multi-modal data at edge/cloud layers to reduce the unnecessary and redundant information before transmission to other edges or the

cloud. In the edge layer, simple machine learning algorithms should be introduced for detecting anomaly sensor data due to restricted storage and computational power, whereas in the cloud layer, collected various data could be integrated through more sophisticated or complicated techniques such as deep learning. In VDP, for cross-evaluation of reliable data and information, restricted Boltzmann machine (RBM) as one of deep neural networks will be utilised, because the RBM is a suitable tool for combining different perspectives captured in signals of multi-modal data from multiple sensors.⁵¹ On the other hand, we could not assume that various kinds of data are always able to be used in disasters, because of sensor flaw, transmission delay and so on. Therefore, reliability assessment of signal data from multi-sources (ie, one type of sensors) should also be considered. Here, multi-source deep belief network (MSDBN) could be appropriate to keep data reliability by identifying common components hidden in multi-source signal data.⁵² As mentioned, the relevance between social media data and disasters should be verified. It can be simple because of using drones as intermediates providing their locations. For example, social media data reaching to the VDP through served communication network has the highest priority for analysis and utilisation. Due to the fact that, when disasters occur, first response is the most urgent task to save people, we only consider these social media data, to avoid wasting restricted resources, rather than analysing overall social media data.

As aforementioned, an ultra-low latency requirement is essential to support first response by victim detection systems in real-time but is difficult due to massive amount of data being continuously generated by IoT devices. Like traditional approaches, VDP is also based on cloud containing more computing resources and parallelised programming logic. However, our architecture considers edge computing to avoid cloud's scalability problem causing ineffective utilisation and reduced throughput. Moreover, in some cases, processing entire data might require more than the available resources to guarantee the desired latency/throughput. Thus, ApproxIoT⁵³ is able to provide proper functions to handle requirement (iii) that the proposed VDP architecture should meet in disasters. This technique leverages a sampling algorithm to obtain approximate results along with sufficient accuracy, rather than exact output. Here, the VDP adjusts parameters for sampling ratio to adapt the algorithm to each type of general data. On the other hand, we need another technique which can be performed in the VDP architecture to preserve privacy of personal data from victim's device, as the purpose (iv). PrivApprox⁵⁴ was adopted for the proposed VDP because of the usage of an application working in personal devices having limited resources. The technique consists of sampling and randomising to achieve the strong privacy properties such as differential and zero-knowledge privacy. In addition, XOR-based cryptography employing extremely efficient bit-wise XOR operations compared to expensive public-key cryptography allows us to support resource-constrained drones and personal devices in the proposed platform in terms of shortage battery limitation.

So far, recent techniques required to the proposed architecture for victim detection were described together with their advantages in terms of crucial requirements for first response in disasters. To discuss how these technologies are harmonised in the VDP, we illustrate the technical overview of our approach, as shown in Figure 7.

We start with describing the local coordination layer of Figure 6. There are many kinds of sensors and personal devices at a disaster site. In case of data generated from a mobile device privacy issues should be particularly considered. Regarding this, recent privacy-preserving analytics favour a distributed architecture to avoid privacy responsibility being centralised by storage of private data into cloud systems.⁵⁴ In other word, the private data is kept locally to achieve differential privacy. Therefore, the proposed VDP architecture has an mobile application

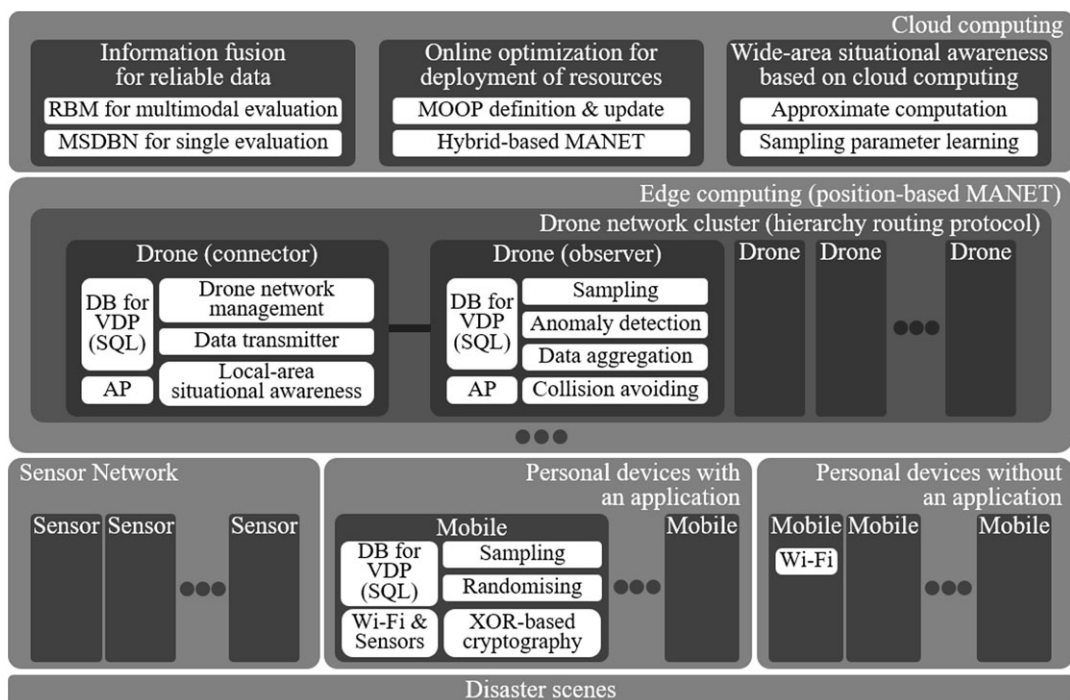


FIGURE 7 Technical overview of victim detection platform

including sampling, randomizing and XOR-based cryptography functions to preserve personal data and to subscribe/response queries from the central cloud layer simultaneously. In addition, the application has another role of broadcasting Wi-Fi signals to announce victim's existence in a specific place of disasters. In this regard, there are two cases according to whether the application is installed into mobile devices or not. As aforementioned, in the case of personal devices, which employed the application, drones having Mac addresses of the devices can detect them more efficiently. Even though a mobile does not have the application installed, UAVs can "sniff" the Wi-Fi emission from the mobile, and upper layers estimate the approximate location of victim through GPS of the drones being connected the victim's devices. Therefore, the proposed VDP is able to preserve and collect sensitive data for privacy issues to conduct more correct victim detection operations along with abundant data.

In the edge-assisted intermediary layer, UAVs compose a hierarchical MANET including connectors and observers. Both of them have own database (DB) temporally storing data, SQL processors conducting aggregation queries and access point (AP) providing Internet for drones, sensors and personal devices, whereas they have different roles (ie, efficient network composition and data processing). The role of the connectors is associated with network management and local-area situational awareness by analysis of edge communication network data and data collected from the local coordination layer. As one example for network management, the deployment plans are decided according to multi-objectives (ie, MOOP) such as wide network (or Internet) coverages, long activity time and stable communication support. For the local-area situational awareness, collected data from drones that belong to same cluster is able to be selectively analysed through relatively simple methods (eg, assemble learning) for first response in real-time. For instance, in initial first response, GPS signals might be transmitted straight along with detection flags to rapidly figure out comprehensive situations in disaster. Otherwise, in the case of narrow areas (eg, building collapse) where many victims have been detected, various tiny machine learning methods should be combined for a partial analysis. Overall, situational awareness will be conducted in the cloud layer with results of the analysis. On the other hand, the most important roles of the observers are detecting victims and gathering data from sensors and personal IoT devices, and then eliminating anomalies from the collected sensor data before sampling and transferring. Private data is sampled and aggregated according to queries from the cloud layer. Note that the collected data already meets differential and zero-knowledge privacy properties through sampling and randomising in personal devices. Even if the observers are maintained by the connectors to avoid collision each other, observer should have autonomous defensive function for crashes being caused by dynamic situations of disasters.

Lastly, the cloud layer conducts high-level analyses based on its high computation power and huge storage. First, the reliability of all collected data from UAVs should be assessed before using them for analysis. In this cloud level, data-reliability problems caused by outside occasions such as sensor flaws does not need to be evaluated, since it is already considered in the edge level. Instead, the data validity should be ensured with assessing inconsistency between data. To do this, RBM and MSDBN could be used for evaluation of multi-modal data and single data, respectively. On the other hand, the deployment optimisation of rescue resources is conducted with respect to situations being analysed based on aggregated data from disaster fields and communication networks. According to response stage, required MOOPs are defined, updated and then spread to edge nodes (ie, connectors) for network management. Wide-area situational awareness is conducted based on approximate data instead of exact data, for requirements about the low-latency and sufficient accuracy for victim detection operations. Statistical and environmental data for a corresponding disaster, real-time command and feedback data between commanders and rescue teams are also utilised. It helps stakeholders to make rapid and correct decision and to learn the appropriate sampling parameters to keep required accuracy for this wide-area situational awareness.

4.3 | Challenges

We described several techniques and their collaborations in the proposed VDP architecture for victim detection. However, since using many data sources and technical methods causes complexity and wide considerations must be covered, there are many challenges that are still remained in the VDP for implementing a system and applying it to real situations. Thus, this section discusses these challenges to figure out future research directions for victim detection.

For the proposed VDP as well as general approaches to disaster management, testing their entire or sub modules is very difficult, as we do not know when and where disasters will occur. Therefore, we should execute an empirical simulation in which various possible disaster situations are sufficiently and reasonably considered. In the case of VDP, composing a MANET of drones will be one of simulations most affected by dynamic conditions (eg, UAVs movements, topography changes and surrounding environment variations) of disasters. Fortunately, there is one suitable simulator, ie, FANET, consisting of NS-3 and Gazebo,⁵⁵ which can consider realistic environments for UAVs. It is appropriate to the proposed VDP since it is also a routing protocol based on Hierarchical node clustering and position information of drones. Besides, it can consider various sensor modules (ie, from Wi-Fi to camera sensor) and, thanks to Gazebo, allows to implement functions such as a collision avoidance algorithm.

For privacy-preserving analysis with low-latency in the era of Big Data with IoT environment, we selected two recent techniques. Although PrivApprox and ApproxIoT are quite proper for the proposed VDP architecture because of some reasons (eg, introducing edge computing and utilising application), we should investigate how to apply these techniques to our platform, because they have only been studied under ordinary situations such as taxi ride and energy consumption. We need to implement and test VDP's modules related to these techniques by considering specific disaster situations.

Even if there might be more critical issues, this section described two main challenges directly related to realising our architecture in realistic situations.

5 | CONCLUSION

The quick detection of victims trapped in buildings and debris as a result of natural and man-made disasters is a major issue for first responders. In this regard, rescuer- or victim-oriented approaches, which utilise IoT technologies, have been studied. However, they have weaknesses or are still being studied at an initial stage. Therefore, we propose a Victim Detection Platform (VDP) architecture combining both approaches through advanced technologies such as IoT, drone and edge/cloud computing to provide correct first response in disaster as soon as possible. With comprehensive review, three crucial issues (ie, multi-modal evaluation for reliable data, edge-based real-time response and privacy-preserved Big Data analysis) were debated. Then, the VDP architecture was described along with the role and relation of relevant technologies, concepts (ie, IoT, Big Data, Edge and Cloud computing and AI), and five kinds of data sources utilised in the platform. In order to explore the realisation possibility of our architecture, several scenarios considering the critical issues and details in victim detection were presented, and then four detail requirements were figured out. Finally, appropriate techniques that could be utilised in the proposed VDP were introduced with respect to the requirements, and leveraging justifications were discussed. Moreover, we argued how the techniques are harmonised in the VDP and what the challenges are.

ACKNOWLEDGMENTS

This work was funded by the Research Council of Norway (RCN) and the Norwegian Centre for International Cooperation in Education (SiU) grant through INTPART program.

ORCID

Minsung Hong  <https://orcid.org/0000-0002-9851-176X>

REFERENCES

- Piccialli F, Chianese A. The internet of things supporting context-aware computing: a cultural heritage case study. *Mob Netw Appl*. 2017;22(2):332-343. <https://doi.org/10.1007/s11036-017-0810-4>
- Piccialli F, Jung JJ. Data fusion in the internet of data. *Concurrency Computat Pract Exper*. 2018;30(15). <https://doi.org/10.1002/cpe.4700>
- Rauniyar A, Engelstad P, Feng B, Thanh DV. Crowdsourcing-based disaster management using fog computing in internet of things paradigm. In: Proceedings of the 2nd IEEE International Conference on Collaboration and Internet Computing, CIC; 2016; Pittsburgh, PA. <https://doi.org/10.1109/CIC.2016.074>
- Greco L, Ritrovato P, Tiropanis T, Xhafa F. IoT and semantic web technologies for event detection in natural disasters. *Concurrency Computat Pract Exper*. 2018;30(21). <https://doi.org/10.1002/cpe.4789>
- Manno G, Smari WW, Spalazzi L, Taccari G. A semantic-based federated cloud system for emergency response. *Concurrency Computat Pract Exper*. 2015;27(13):3316-3344. <https://doi.org/10.1002/cpe.3293>
- Botta A, De Donato W, Persico V, Pescapè A. Integration of cloud computing and internet of things: a survey. *Future Gener Comput Syst*. 2016;56:684-700. <https://doi.org/10.1016/j.future.2015.09.021>
- Castillo JC, Fernández-Caballero A, Serrano-Cuerda J, López MT, Martínez-Rodrigo A. Smart environment architecture for robust people detection by infrared and visible video fusion. *J Ambient Intell Humaniz Comput*. 2017;8(2):223-237. <https://doi.org/10.1007/s12652-016-0429-5>
- Lee OJ, Jung JE. Sequence clustering-based automated rule generation for adaptive complex event processing. *Future Gener Comput Syst*. 2017;66:100-109. <https://doi.org/10.1016/j.future.2016.02.011>
- Navarro-Arribas G, Torra V. Information fusion in data privacy: a survey. *Information Fusion*. 2012;13(4):235-244. <https://doi.org/10.1016/j.inffus.2012.01.001>
- Sakour I, Hu H. Robot-assisted crowd evacuation under emergency situations: a survey. *Robotics*. 2017;6(2):8. <https://doi.org/10.3390/robotics6020008>
- Casper J, Murphy RR. Human-robot interactions during the robot-assisted urban search and rescue response at the World Trade Center. *IEEE Trans Syst Man Cybern Part B*. 2003;33(3):367-385. <https://doi.org/10.1109/TSMCB.2003.811794>
- Hasan KM, Newaz SHS, Ahsan MS. Design and development of an aircraft type portable drone for surveillance and disaster management. *Int J Intell Unmanned Syst*. 2018;6(3):147-159. <https://doi.org/10.1108/IJIUS-02-2018-0004>
- Schwarz M, Rodehutsors T, Droeschel D, et al. NimbRo rescue: solving disaster-response tasks with the mobile manipulation robot momaro. *J Field Robotics*. 2017;34(2):400-425. <https://doi.org/10.1002/rob.21677>
- Restas A. Drone applications for supporting disaster management. *World J Eng Technol*. 2015;3:316-321. <https://doi.org/10.4236/wjet.2015.33C047>
- Alex C, Vijaychandra A. Autonomous cloud based drone system for disaster response and mitigation. In: Proceedings of the 2016 International Conference on Robotics and Automation for Humanitarian Applications, RAHA; 2016; Kollam, India. <https://doi.org/10.1109/RAHA.2016.7931889>
- Sherman T, Tellez J, Cady T, et al. Cooperative search and rescue using autonomous unmanned aerial vehicles. In: Proceedings of the 2018 AIAA Information Systems-AIAA Infotech Aerospace, AIAA SciTech Forum, Vol 1490; 2018; Kissimmee, FL. <https://doi.org/10.2514/6.2018-1490>
- Tanzi TJ, Chandra M, Isnard J, Camara D, Sebastien O, Harivelo F. Towards "drone-borne" disaster management: future application scenarios. Paper presented at: XXIII ISPRS Congress, Commission VIII (Volume III-8), ISPRS Annals of photogrammetry, Remote Sensing & Spatial Information Sciences; 2016; Prague, Czech Republic.
- Wang W, Joshi R, Kulkarni A, Leong WK, Leong B. Feasibility study of mobile phone WiFi detection in aerial search and rescue operations. In: Proceedings of the Asia-Pacific Workshop on Systems, APSys'13, Vol 7; 2013; Singapore. <https://doi.org/10.1145/2500727.2500729>

19. Sundqvist J, Ekskog J, Dil BJ, Gustafsson F, Tordenlid J, Petterstedt M. Feasibility study on smartphone localization using mobile anchors in search and rescue operations. In: Proceedings of the 19th International Conference on Information Fusion, FUSION; 2016; Heidelberg, Germany.
20. Foresti GL, Farinosi M, Vernier M. Situational awareness in smart environments: socio-mobile and sensor data fusion for emergency response to disasters. *J Ambient Intell Humaniz Comput*. 2015;6(2):239-257. <https://doi.org/10.1007/s12652-014-0227-x>
21. Amato F, Moscato V, Picciello A, Piccialli F. SOS: a multimedia recommender system for online social networks. *Future Gener Comput Syst*. 2017;93:914-923. <https://doi.org/10.1016/j.future.2017.04.028>
22. Oliveira ACM, Botega LC, Saran JF, et al. Crowdsourcing, data and information fusion and situation awareness for emergency management of forest fires: the project DF100Fogo (FDWithoutFire). *Comput Environ Urban Syst*. 2017. In Press. <https://doi.org/10.1016/j.compenvurbysys.2017.08.006>
23. Piccialli F, Jung JE. Understanding customer experience diffusion on social networking services by big data analytics. *Mob Netw Appl*. 2017;22(4):605-612. <https://doi.org/10.1007/s11036-016-0803-8>
24. Anderson C, Breimyer P, Foster S, et al. A network science approach to open source data fusion and analytics for disaster response. In: Proceedings of the 18th International Conference on Information Fusion, FUSION; 2015; Washington, DC.
25. Li J, Liu L, Zeng Z, Liu F. Advanced signal processing for vital sign extraction with applications in UWB radar detection of trapped victims in complex environments. *IEEE J Sel Top Appl Earth Obs Remote Sens*. 2014;7(3):783-791. <https://doi.org/10.1109/JSTARS.2013.2259801>
26. Yang Z, Schafer J, Ganz A. Disaster response: victims' localization using Bluetooth low energy sensors. In: Proceedings of the 2017 IEEE International Symposium on Technologies for Homeland Security HST; 2017; Waltham, MA. <https://doi.org/10.1109/THS.2017.7943504>
27. Erdelj M, Król M, Natalizio E. Wireless sensor networks and multi-UAV systems for natural disaster management. *Computer Networks*. 2017;124:72-86. <https://doi.org/10.1016/j.comnet.2017.05.021>
28. Breckon TP, Gaszczak A, Han J, Eichner ML, Barnes SE. Multi-modal target detection for autonomous wide area search and surveillance. In: Proceedings of the Emerging Technologies in Security and Defence; and Quantum Security II; and Unmanned Sensor Systems X, Vol 8899; 2013; Dresden, Germany. <https://doi.org/10.1117/12.2028340>
29. Arbia DB, Alam MM, Kadri A, Hamida EB, Attia R. Enhanced IoT-based end-to-end emergency and disaster relief system. *J Sens Actuator Netw*. 2017;6(3):19. <https://doi.org/10.3390/jsan6030019>
30. Lee OJ, Hoang LN, Jung JE, Um T, Lee H. Towards ontological approach on trust-aware ambient services. *IEEE Access*. 2017;5:1589-1599. <https://doi.org/10.1109/ACCESS.2017.2663407>
31. Cuomo S, Michele PD, Piccialli F, Galletti A, Jung JE. IoT-based collaborative reputation system for associating visitors and artworks in a cultural scenario. *Expert Syst Appl*. 2017;79:101-111. <https://doi.org/10.1016/j.eswa.2017.02.034>
32. Tonyali S, Akkaya K, Saputro N, Uluagac AS, Nojournian M. Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled smart metering systems. *Future Gener Comput Syst*. 2018;78:547-557. <https://doi.org/10.1016/j.future.2017.04.031>
33. Yuan J, Li X. A reliable and lightweight trust computing mechanism for IoT edge devices based on multi-source feedback information fusion. *IEEE Access*. 2018;6:23626-23638. <https://doi.org/10.1109/ACCESS.2018.2831898>
34. Jutila M. An adaptive edge router enabling internet of things. *IEEE Internet Things J*. 2016;3(6):1061-1069. <https://doi.org/10.1109/JIOT.2016.2550561>
35. Goudarzi F, Asgari H, Al-Rawashidy HS. Traffic-aware VANET routing for city environments—a protocol based on ant colony optimization. *IEEE Syst J*. 2018. <https://doi.org/10.1109/JSYST.2018.2806996>
36. Chen L, Englund C. Every second counts: integrating edge computing and service oriented architecture for automatic emergency management. *J Adv Transp*. 2018;2018:7592926. <https://doi.org/10.1155/2018/7592926>
37. Yeow K, Gani A, Ahmad RW, Rodrigues JJPC, Ko K. Decentralized consensus for edge-centric internet of things: a review, taxonomy, and research issues. *IEEE Access*. 2018;6:1513-1524. <https://doi.org/10.1109/ACCESS.2017.2779263>
38. Quispe LE, Galan LM. Behavior of ad hoc routing protocols, analyzed for emergency and rescue scenarios, on a real urban area. *Expert Syst Appl*. 2014;41(5):2565-2573. <https://doi.org/10.1016/j.eswa.2013.10.004>
39. Ochoa SF, Santos RM. Human-centric wireless sensor networks to improve information availability during urban search and rescue activities. *Information Fusion*. 2015;22:71-84. <https://doi.org/10.1016/j.inffus.2013.05.009>
40. Anjum SS, Noor RM, Anisi MH. Review on MANET based communication for search and rescue operations. *Wirel Pers Commun*. 2017;94(1):31-52. <https://doi.org/10.1007/s11277-015-3155-y>
41. Chen WP, Tsai AH, Tsai CH. Smart traffic offloading with mobile edge computing for disaster-resilient communication networks. *J Netw Syst Manag*. 2018;27(2):463-488. <https://doi.org/10.1007/s10922-018-9474-z>
42. Cao X, Wang F, Xu J, Zhang R, Cui S. Joint computation and communication cooperation for mobile edge computing. In: Proceedings of the 16th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, WiOpt; 2018; Shanghai, China.
43. Smari WW, Clemente P, Lalande JF. An extended attribute based access control model with trust and privacy: application to a collaborative crisis management system. *Future Gener Comput Syst*. 2014;31:147-168. <https://doi.org/10.1016/j.future.2013.05.010>
44. Yu W, Liu Z, Chen C, Yang B, Guan X. Privacy-preserving design for emergency response scheduling system in medical social networks. *Peer-to-Peer Netw Appl*. 2017;10(2):340-356. <https://doi.org/10.1007/s12083-016-0429-4>
45. Wang H, Jiang X, Kambourakis G. Special issue on security, privacy and trust in network-based big data. *Information Sciences*. 2015;318:48-50. <https://doi.org/10.1016/j.ins.2015.05.040>
46. Wang H, Zhang Z, Taleb T. Editorial: special issue on security and privacy of IoT. *World Wide Web*. 2018;21(1):1-6. <https://doi.org/10.1007/s11280-017-0490-9>
47. Tonni SM, Rahman MZ, Parvin S, Gawanmeh A. Securing big data efficiently through microaggregation technique. In: Proceedings of the 37th IEEE International Conference on Distributed Computing Systems Workshops, ICDCS Workshops; 2017; Atlanta, GA. <https://doi.org/10.1109/ICDCSW.2017.65>
48. Castillo C. *Big Crisis Data: Social Media in Disasters and Time-Critical Situations*. Cambridge, UK: Cambridge University Press; 2016.
49. Piccialli F, Jung JJ. Towards the internet of data: applications, opportunities and future challenges. *J Parallel Distributed Comput*. 2018;116:1-2. <https://doi.org/10.1016/j.jpdc.2018.03.003>

50. Zheng YJ, Chen S, Ling H. Evolutionary optimization for disaster relief operations: a survey. *Appl Soft Comput.* 2015;27:553-566. <https://doi.org/10.1016/j.asoc.2014.09.041>
51. Srivastava N, Salakhutdinov R. Multimodal learning with deep Boltzmann machines. *J Mach Learn Res.* 2014;15(1):2949-2980.
52. Ge L, Gao J, Li X, Zhang A. Multi-source deep learning for information trustworthiness estimation. In: Proceedings of the 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD; 2013; Chicago, IL. <https://doi.org/10.1145/2487575.2487612>
53. Wen Z, Quoc DL, Bhatotia P, Chen R, Lee M. ApproxIoT: approximate analytics for edge computing. In: Proceedings of the 38th IEEE International Conference on Distributed Computing Systems, ICDCS; 2018; Vienna, Austria. <https://doi.org/10.1109/ICDCS.2018.00048>
54. Quoc DL, Beck M, Bhatotia P, Chen R, Fetzter C, Strufe T. PrivApprox: privacy-preserving stream analytics. In: Proceedings of the 2017 USENIX Annual Technical Conference; 2017; Santa Clara, CA.
55. Ahn T, Seok J, Lee I, Han J. Reliable flying IoT networks for UAV disaster rescue operations. *Mob Inf Syst.* 2018;2018:2572460. <https://doi.org/10.1155/2018/2572460>

How to cite this article: Hong M, Akerkar R. Victim detection platform in IoT paradigm. *Concurrency Computat Pract Exper.* 2019;e5254.

<https://doi.org/10.1002/cpe.5254>