Privacy-Aware Business Processes Modeling Notation (PrvBPMN) in the Context of Distributed Mobile Applications

Wadha Labda, Nikolay Mehandjiev, and Pedro Sampaio

Centre for Services Research,
University of Manchester,
Manchester, UK
wadha.labda@postgrad.manchester.ac.uk,
{n.mehandjiev,P.Sampaio}@manchester.ac.uk

Abstract. Distributed mobile applications are increasingly being considered as solutions which provide robustness and performance benefits, especially in contexts such as emergency response systems, where a conventional centralized ICT infrastructure can be rendered inoperative. The information intensive nature of such systems brings to the fore the importance of data distribution through the right workflow channels under conditions of data privacy and short timescales. This paper reports on the early stages of a project aimed at developing a privacy-aware process-level framework for such distributed mobile applications, exemplified through a distributed prototype that can be used to model and manage fire emergency situations in airports. The novelty of the framework arises from modeling, reasoning and generating privacy preserving business processes applicable to distributed mobile information systems.

Keywords: privacy modelling, BPMN, privacy-aware, service-based.

1 Introduction

With the increasing number of natural and man-made disasters, modeling and development of emergency response systems is becoming a key priority for governments and corporations across the globe towards mitigating the impact of natural disasters and/or terrorist attacks. Due to the dynamic, information intensive and life critical nature of emergency response systems, access and management of resources such as data, software applications and human resources need to be securely, effectively coordinated and timely. To address this issue, many researchers have been considering distributed mobile applications as solutions for such emergency situations [11], due to its ability to provide robustness and performance benefits. Emergency situations in airports are considered one of the complex scenarios that need specially designed solutions to handle communications and coordination successfully between different actors participating in the management and rescue response. An excellent interpretation of emergency management was given by [24] which is "getting the

M. Matera and G. Rossi (Eds.): MobiWIS 2013 Workshops, CCIS 183, pp. 120–134, 2013.

right resources to the right place at the right time to provide the right information to the right people to make the right decisions at the right level at the right time". Successful planning and design of emergency management systems could achieve this. One of the key issues system designers must keep in mind while designing mobile distributed solutions for systems is privacy. Failing in correctly defining privacy requirements in a system could cause the failure of whole system. Privacy requirements and constraints must be modeled during design-time and enforced at runtime [16]. There is indeed a body of work on business processes privacy [2][6] yet they did not consider the requirements arising out of mobile context.

In this paper the emergency situation at airports is considered an example of target application domain. It needs specially designed solutions to handle communications and coordination successfully between different actors participating in the management and rescue response. They are expected to use mobile technologies to exchange the evacuation plans and requests for assistance. Key issues to be tackled in the solution design relate to risks related to information leakages and unauthorized use and access to private data in emergency situations [10]. To capture all the requirements of the emergency situation in a conceptual representation that is understood by all stakeholders, business process modeling [21] is used to model such emergency situation processes and define the communications and interaction of different activities. BPMN is used since it supports conceptual descriptions of emergency workflows and it can be used to generate executable code from process specifications. Moreover, it is easy to be understood and analyzed by managers and business stakeholders [6].

A privacy-aware framework and a method for constructing mobile distributed systems are needed to solve this problem. This research is investigating the different approaches that can be developed to address privacy in process-level notations in distributed service systems, and aiming to complement systems analysis and design approaches with tailored techniques for modeling and reasoning about privacy issues that can enable model checking of privacy constraints in distributed service systems.

This paper introduces a work in progress in this direction. A case study on airport fire emergency management system using passenger's mobile devices is presented. This paper is structured as following: Section 2 presents a background about the notions and technologies that is used to develop our approach. Section 3 presents a motivating example on Airport fire emergency situations and the challenges related to it, how to represent the situation using BPMN, then present the privacy requirements related to the target domain. Section 4 presents the initial details of our work in progress approach, and it shows an example of applying our approach to the fire emergency situation. Section 5 discusses related work and identifies the gap that our work is addressing. Section 6 describes the conclusions and future work.

2 Motivating Example

The following is a scenario that motivates our research and from which we will extract privacy requirements for emergency response in distributed mobile information systems.. The selected scenario is a critical fire emergency situation at Airports.

The following section will present the general business process of the airport scenario. Then the challenges and privacy requirements will be discussed. After that, a process-level representation of the scenario will be given. Moreover, some of the related work on process-level emergency management systems will be discussed.

2.1 Airport Fire Emergency Scenario: General Business Process

A fire occurs on the airport ground. The fire affects the emergency control unit, so no communication can be transferred from there. Luckily the airport has a backup plan of using smart phones as a media for communication. These handsets belong to the people in charge of emergency control, and could include the handsets of airport passengers, which will increase privacy concerns. A prompt and efficient solution must be reached which will save peoples' lives, airport resources and preserve privacy of all parties. In case of a fire emergency on Airport location, there are a standard procedure steps to manage such emergencies. These steps are emergency detection, emergency response and emergency response evaluation. Each step has its own sub-processes shown in Figure 1. To enable the use of passengers' mobile devices in an emergency situation, one scenario could be downloading specially designed application to the passengers' mobile devices' systems that will automatically sense the fire alarm and act based on it. This could be downloaded when user purchase and download their tickets. The system will ask them to if they would like to participate in evacuation plan if a fire emergency occurs at the airport.

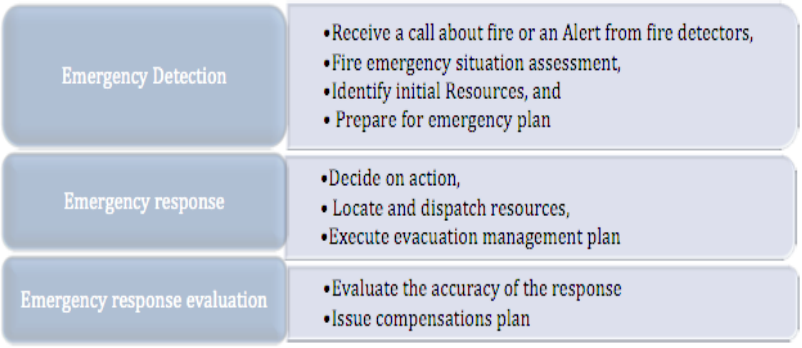

Fig. 1. Emergency Response Sub-Processes

2.2 Process-Level Representation of Airport Emergency Scenario

Key to the Success of an emergency response system is the quick and reliable response. For this purpose the use of BPMN modeling provides an effective approach that ensures emergency response processes are clearly defined and easy to be followed. BPMN defines the syntax of the process and specifies messages and information flows between participants in the process. Refer to [3] for more information on BPMN. A key limitation of BPMN for modeling emergency is its lack of ability to

provide the semantics of the modeled system. However, it provides an intuitive notation that can be mapped to formal constructs to support model checking and reasoning. Figure 6 below is a partial representation of airport emergency response management situation pointing out possible privacy issues. Association of privacy constraints in modeling emergency situations ensures that the system will be aware of privacy constraints and enforce them when a realistic emergency situation occurs.

3 Background

This section will present a background on the technologies that will be used in our approach. First, the business processes and BPMN is discussed. Then, a definition of privacy and its dimensions is presented.

3.1 Business Processes

We implement and get engaged in business processes in our daily life either being us as the requester of services or the provider. A business process is a set of activities that may need more that one entity to work collaboratively to achieve a business objective [4]. Business process Management (BPM) [21] has been utilized as one of software engineering technologies that is used to model system requirements and processes. With the rapid growth of businesses and technologies, it has become a necessity for business managers', decision makers and software designers to closely collaborate and participate in the designing processes of a given system. BPM defines the syntax of the process and specifies messages and information flows between participants in the process. A key limitation of BPM for modeling business processes is its lack of ability to provide the semantics of the modeled system [21]. However, it provides an intuitive notation that can be mapped to formal constructs to support model checking and reasoning. Moreover, BPM are considered central information storage [15]. For this reason, all relevant information should be included or at least linked to the models. There are many existing modeling languages that differ in expressiveness and semantics such as Business Process Modeling Notation (BPMN) [3], Event Driven Process Chain (EPC)[22], Petri Nets [13], and UML Activity Diagrams (AD) [16]. In this research we will use BPMN as the formal modeling language for our research. The rationale behind this is that BPMN can be extended easily to support system semantics.

3.2 Business Process Modeling Notation (BPMN)

To achieve a successful integration and a system with competitive advantage, system designers and developers should find a modeling method that supports agility and change management. For this purpose the use of BPMN modeling provides an efficient approach that ensures processes are clearly defined and easy to be followed [21]. BPMN defines the syntax of the process and specifies messages and information flows between participants in the process. BPMN diagrams have four main elements:

Flow objects, connection objects, artifacts, and swimlanes. Flow objects, such as activities, events, and gateways, define the process behavior. Connection objects define the messages flows between the flow objects, and there are three different types of connection objects: sequence flow, association and message flow. Data objects are considered as artifacts, and swimlanes define the different participants in the process [3]. BPMN does not express the semantics of the modeled system. However, it can be extended to support system semantics. That's why we are working on developing an extension to BPMN to enable semantic definitions of the process, and look into mapping these constructs to an execution language such as business process execution language (BPEL).

3.3 Privacy in Business Processes

In this section we will define what is privacy, present the different dimensions of privacy, and discuss the attributes of the two dimensions that we will cover in our privacy-aware approach.

3.3.1 What Is Privacy?

Privacy as a noun in the dictionary means "The state or condition of being free from being observed or disturbed by other people". Which means the right to be left alone. But this is used to work in the past when less information was tackled online. Now with the enormous amount of information collected every day, the need to provide information online increases and the risk of personal information being exposed or breached also increases [4].

Privacy usually concerns personal or sensitive data, which can be used to identify a person and the misuse of it could cause harm to that person [14]. It is a fundamental human right (Pearson, 2009). Nowadays, there are significant efforts to protect privacy using law and regulations such as Organization for Economic Co-operation and Development (OECD), which defines eight principles, and Federal Trade Commission of United States (FTC), as well as technical solutions [7]. The following sections will discuss privacy in more details specifying the different dimensions and attributes of each dimension.

3.3.2 Privacy Dimensions

When addressing privacy we are considering mainly four dimensions of personal privacy [5], which are Privacy of the person, *i.e.* physical privacy, which mainly concerns a person's physical body and its constituents. The second dimensions are Privacy of personal behavior that is mainly concerned with the privacy of a person behavior, referred to it as media privacy. The third dimension is Privacy of personal communications, which is concerned with freedom of Individuals to communicate using various media without being continuously monitored. The fourth dimension is the privacy of personal data, which protect personal data from being exposed to other individuals and organizations, and an individual must be able to have control over their data even if possessed by other parties. Figure 2 shows these four dimensions. Among the four dimensions, this research is interested in the last two dimensions,

Privacy of personal communication and privacy of personal data because they are more concerned with information system privacy. To be able to develop a framework addressing these two dimensions, a set of attributes that will be defining the privacy-preserving rule is defined below. These attributes also will help to develop the visual privacy-preserving constructs as extensions to BPMN.

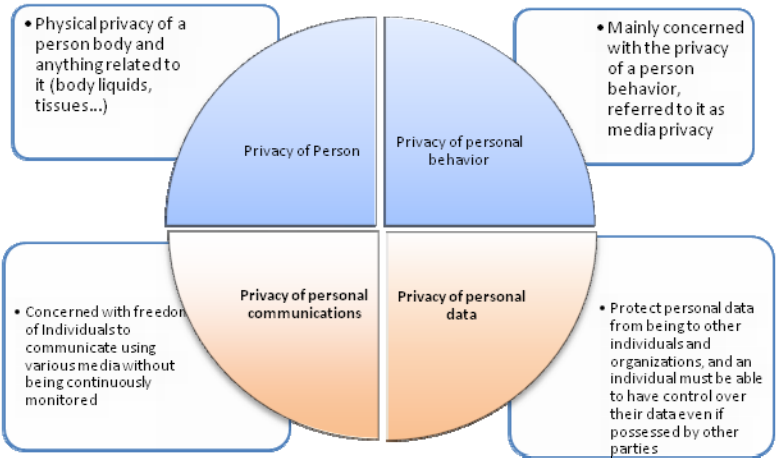

Fig. 2. Privacy Dimensions (Roger Clark, 1999)

Attributes of the first dimension (Privacy of personal data):.

- **Data:** Describe Data categories used in communications or transition of systems or within a single system. They are usually defined in upper-level categories of data that is from privacy point of view will be treated differently. Such categories are:
  - Personal Identifier information: names, address, email addresses, device mac addresses
  - Sensitive information: Social security number, credit card number, medical data
  - Medium sensitivity information: personal information that is not considered as personal identifier such as gender, social relations.
  - Usage data: Browsing and transactions history
  - Public Data: Any data that is made public by users such as hobbies,
- **Actor:** Describe the set of individuals or organizations who can access the data and they are distinct from a privacy point of view.
- **Action:** Describes the activities performed on data (Collect, Read, Update, Disclose, Delete)
- **Purpose:** Describe the purpose of collecting, using or disclosing data.
- **Permissions:** Represent set of permissions granted to actors to access Data, Deontic-permissions (Permitted, Obligation, Forbidden, Permitted if condition true).
- **Conditions:** Requirements that must be met for the actions to be allowed.

- **Data Retention:** Defines the period of time the data is kept at the requested end. Such rules could be: delete once done with transaction, keep for personal analysis, indefinite.
- **Enforcement mechanism:** Mechanisms that will be used to enforce privacy such as Policy (Laws and regulations), data encryption, Rules, …

These attributes will be covered in both dimensions, however an additional attributes for the communication privacy dimension is added below.

Attributes of the second dimension (Privacy of personal communication):.

- **Anonymity:** ensure that personal information is kept anonymous to others, i.e. remove all identifiable information from the data.
- **Unlinkability:** ensure that others are not able to link different data to each other to identify the person.
- **Pseudonymity:** use pseudonym identifiers, to act as users' real identities
- **Sensitive Propagation:** ensure that privacy preferences are kept through out the whole process including the interactions with other providers.
- **Sensitive communication Level:** level of sensitivity should be specified so that the communication privacy will be considered based on the level (Low, Medium, High)

Figure 3, presents two ontological representations of the privacy preserving attributes for both dimensions.

3.4 Privacy Requirements of the Domain

The dynamic nature of emergencies makes the system vulnerable for intended and unintended privacy attacks from malicious users. Thus, identifying the privacy issues and constraints at the design phase, helps in reducing this vulnerability problem. In addition to this, we have to keep in mind, while addressing privacy issues, the functional requirements such as efficient and effective response especially in emergency response. Examples of these issues are: Personal information leakage from passengers' mobile devices, unauthorized access to airport systems confidential files and information, and Intruder or terrorist trying to access and link different personal data to identify users and miss use the data. Association of privacy constraints in modeling business processes ensures that the system will be aware of privacy constraints and enforce them. The following are some privacy requirements of an emergency response management system:

- **Access Control:** Access to resources as well as actions need to be restricted to certain roles or subjects. (PARBAC)
- **Separation of Duty:** More than one subject is required to successfully complete the process.
- **Binding of Duty:** The same subject needs to execute several tasks of a process.

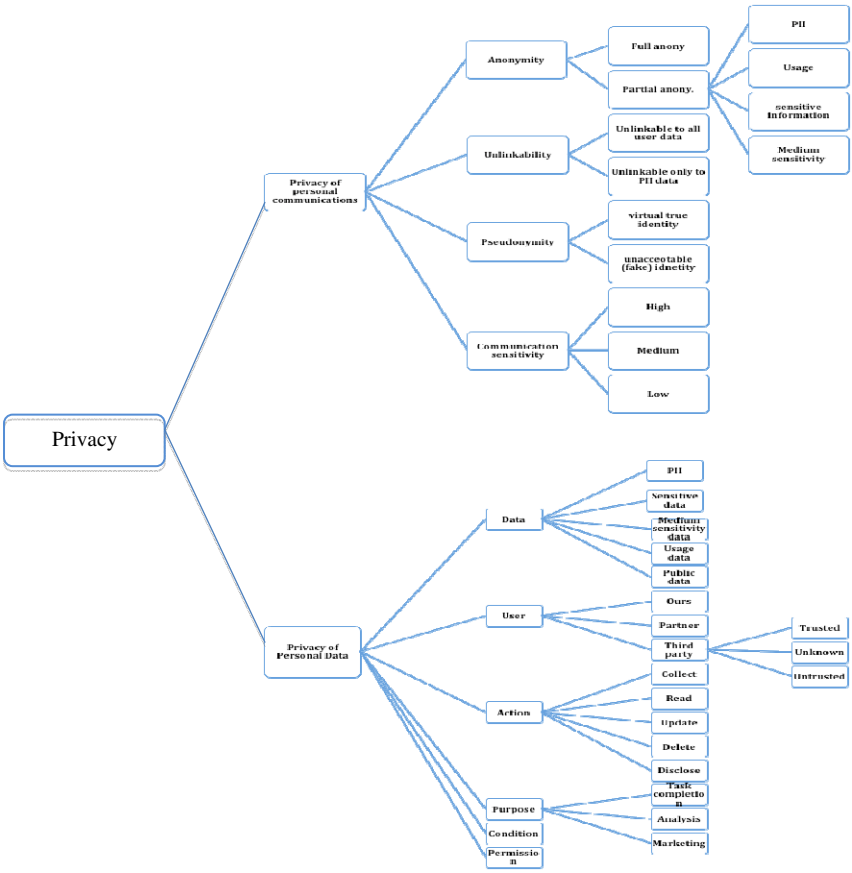

Fig. 3. Ontological Representations of Privacy Requirements

- **Necessity to Know:** A subject should only be able to access the information that is strictly necessary for completing a certain task.
- **Privacy preserving actions** such as anonymization or pseudonymization and Unlinkablity.
- **Purpose binding:** Data collected for one purpose should not used for another purpose without user consent)

4 Our Privacy-Aware Approach

Modeling privacy requirements on the process level requires the extension of the process modeling language (BPMN) with privacy concepts. Our approach is extending BPMN Meta model with formal constructs for the privacy requirements we specified before. We have developed ontology to represent each construct and used Semantic Web Rule Language (SWRL) [18] to represent the different rules and constraints on the BPMN notations. SWRL will help us to automate the transformation to

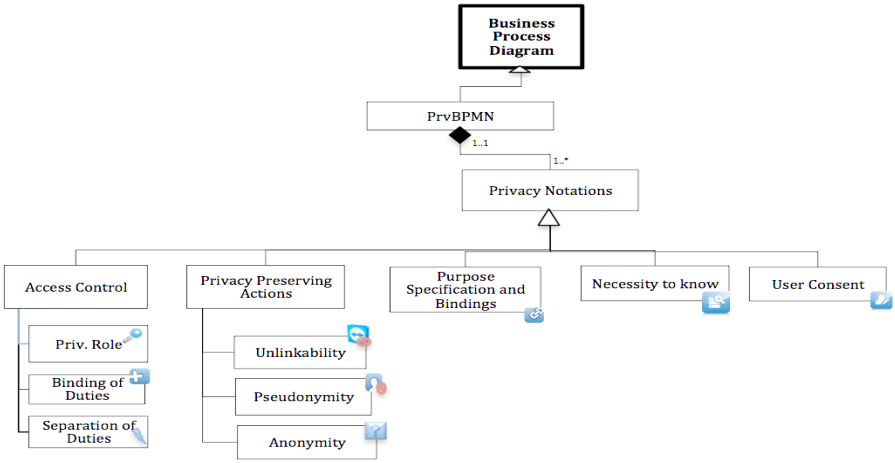

Fig. 4. PrvBPMN meta model with representing notations

execution language such as BPEL. Figure 4 presents the Meta model of our identified privacy requirements that extends the meta model of business processes diagram [15]. Also, their visual notations that will be used to annotate the BPMN model are added in the privacy requirements Meta model to represent the meanings of each notation. Moreover, in Figure 5, we have mapped privacy notations to BPMN elements based on what privacy requirements can be used to annotate each element in the BPMN diagram. Also, we will be using PARBAC [8] model to represent the access control requirements to protect data. PARBAC adopted the expression of a general privacy policy rule:

```
allow [DataUser]
to perf orm [Operation] on [DataT ype]
for [Purpose] provided [Condition]
carry out [Obligation]
```

Our access control rules are following the same format. Following is an example:

```
allow [user]
to perform [access] on [resources]
for [assistInER] provided [nessecaryAndnoIdentifiable]
carry out [notUseItForOtherPurposes]
```

The above rule is saying that “When in an airport emergency, a general user can access only necessary not identifiable resources to assist in emergency response (ER). Users should not be able to link available resources to other to be used for other purposes”. Presenting the rule using PARBAC will make it easier for us to transform it to a formal reasoning language like SWRL, for compliance checking and privacy enforcement. The following is a SWRL representation of the above rule, where u is the user, x is the requested to access resource.

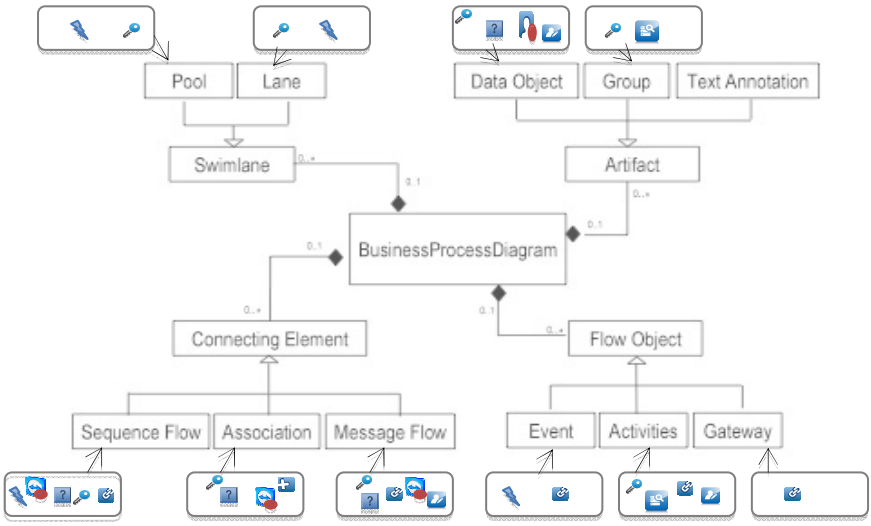

Fig. 5. Mapping of BPMN Elements to Privacy Notations

```
isEmergency(Airport)
^ resourceAccess(?x,?u)
^ locatedIn(?x, Airport)
^ hasStatus(?x, Anonymized)
-> hasOtherLinkedData(?x, ?u, Unlinkable)
```

Moreover, unexpected and exceptional situations tend to happen during emergency situations, which need some special ways of handling them to ensure that they would not cause any issues with privacy. So, to handle exceptional situations easily, it can be represented as events, in this case we will use Event Condition Action (ECA) [12] rules to allow treating them just like not exceptional situations. This part is still under investigation but we have chosen to develop it using ECA rules [12] since we find it a suitable language to address our research objectives. In the following section we will present an application of our approach to the scenario discussed in the previous sec-tion.

4.1 Application of Approach to Specify the Privacy Requirements in the Target Domain

In this section we will present an application of our approach to the Airport emergency situation. We used BPMN to visualize the fire response business process using BPMN. However, we did not present the full process due to space limitations. In Figure 6 we identified four main roles, namely, airport, fire department, medical services, and passengers of the airport. Each role will perform certain activities; some of these activities will have the potential to cause privacy leakages, specially the ones that need personal information such as name, age, location, etc. to complete their tasks. An example illustrated in Figure 6, is when a passenger requests for evacuation plans,

his request would be sent to the evacuation team and they would request some private details such as the location and may be some details about the passenger. Before the passenger provides the needed details he or she needs to ensure that their data is protected and will not be used for other unspecified purposes. The airport will ensure that in their privacy policy. So, during this activity we will need to protect four main privacy requirements, namely access control, to limit the access only to the roles who request the data, purpose bindings, to make sure that the data is used only for the purpose specified in the request, user consent, when needed, and necessity to know, to only provide the information needed to complete the task. So, the airport emergency response team could use our tool to forecast the possible privacy issues that they might face and prepare the needed protection to every situation. On this BPMN diagram we used our identified privacy notations to represent the privacy requirements for each element. That notation will be automatically transformed to execution language to ensure the enforcement of privacy requirements.

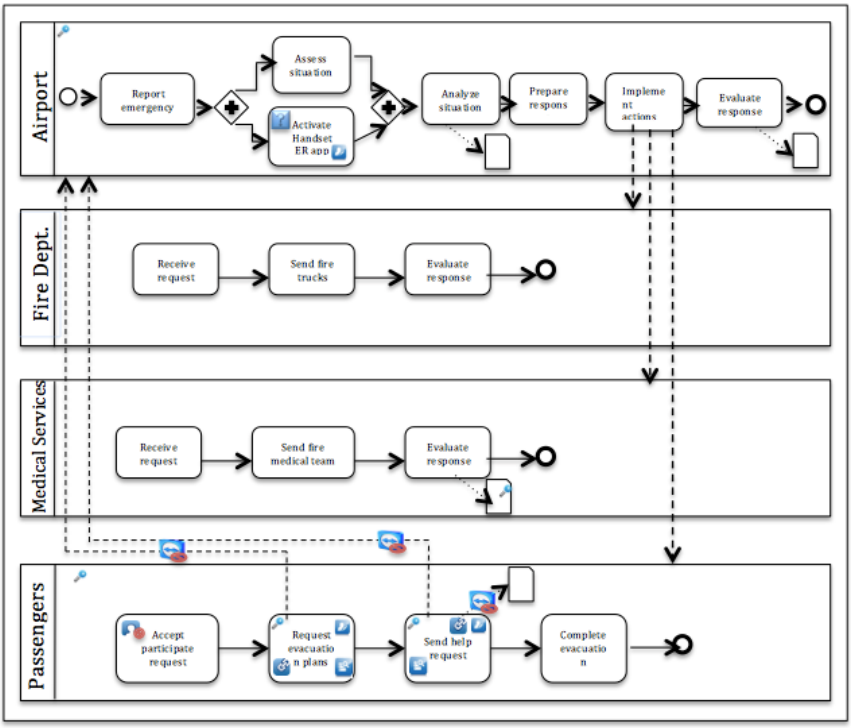

Fig. 6. Privacy Annotated BPMN Representation of Emergency Response Scenario

5 Related Work

The following two sections will discuss some related work on Privacy and BPMN and also existing work on modeling emergency systems.

5.1 BPMN and Privacy

Among the well-known efforts in this area is the work of [2], they developed a model-driven framework for web services life cycle management called Servicemosaic. It has three main components: (1) Model representation and manipulation, (2) Analysis and management component, and (3) Development environment. Servicemosaic allows system designers to model privacy aspects using web service protocol. Using extended state machine model, the use and storage of personal information descriptions are integrated with a web service protocol. Privacy aspects such as data collection, disclosure, access, and retention of web service protocols are modeled with this proposed conceptual model. However, there is no support for BPEL code generation; the authors claim that as a future work. Another equally important work is done by [6], which is a platform for process modeling on the web called ORYX. The main aim for this platform is to be extensible and to be used by BPM community. It will help researchers to find a tool ready to be extended to address their research questions. This platform is an influential modeling base for the researchers. However, the authors did not show any work on privacy or any non- functional requirements. Furthermore, [1] presented a work on specifying compliance rules visually and explaining their violations for business processes. They use a pattern-based approach to utilize a visual language (BPMN-Q). [4] have presented a work called SecureBPMN, where they extend visually the BPMN with privacy requirements (Access control, separation of duty, binding of duty and need to know) and enforce it during run time using XACML. SecureBPMN allows for specifying role-based access control (RBAC) as well as other security and compliance properties. RBAC is specified using separate interface while separation and binding of duty is added as components to BPMN visual diagram. In similar fashion with [2] and [4], this research will provide a modeling extension for privacy concerns such as authentication, access control and openness and transparency. Moreover, it will work on a novel technique to reason and transform privacy visual constructs to executable languages.

5.2 Related Work to Emergency Modeling

Managing emergencies requires a considerable amount of heterogeneity across different actors, resources and systems participating in the response and rescue, such as fire departments, medical services departments and so on [22]. Thus, designing a system that is web service-based is considered one of the best possible solutions. The capabilities of the service-oriented models support integration of heterogeneous application interfaces and the exchange of messages between systems on demand. One of the examples of some existing work using web services to implement emergency management systems are in [22], the proposed the EVResponse application which make use of web services to provide to both decision makers and first response unite a real-time reporting capabilities. They define a tier for web services to integrate different applications and enhance the emergency response techniques. In line with that, [15] emphasize the benefits of using web services to coordinate emergency response activities. Moreover, [17] proposed emergency management application, which is a

decision support system that is based on the technology of semantic web services, which will help users to get the needed information more quickly and accurately. The above approaches are just examples of the huge amount of use of web services to facilitate the integration of different systems and help in getting the results more efficiently.

Recently, business process modeling is used to model such emergency situations processes and define the communications and interaction of different activities. The reason for using BPM is that it supports agility, easy to change when needed, and it would be on an application independent level. Moreover, it is easy to be understood and analyzed by managers and business stakeholders [7]. For example, [7] proposed a method to model a web service-based system using Petri net to logically describe the composite web services and they have highlighted the logical modeling usefulness in ensuring the correctness of the system. Most of the existing work used Petri Net to model emergency situations, because of its support to semantics and its underlying algebra, which makes it easier to formally verify the correctness of their models. However, when it comes to modeling non-functional or privacy constraints, it can be complex and confusing to use Petri net because it lacks support to model non-functional requirements [7]. In addition, none of the existing work considered privacy issues in emergency situations, most of the work were focusing on how to model, analyze and verify the modeling methods. The gap in the literature gives an important value to our work, were we will be working on modeling privacy constraints keeping in mind the nature of the emergency situation with unreliable network connections and heterogeneity of mobile devices with its special design requirements. A novel privacy preserving approach to service compositions will be developed, that will allow first to model the problem in BPMN and dynamically generate the underlying formal constructs that will work on reasoning and model checking the correctness and reliability of the model.

6 Conclusion and Future Work

The gap in the literature gives an important value to our work, modeling privacy constraints, keeping in mind the nature of the emergency situation with unreliable network connections and heterogeneity of mobile devices with its special design requirements. Our aim is to develop a privacy-aware service-based framework and system that will be used to model and manage fire emergency situations in airports and can be also extended to other situations. A novel privacy preserving extension to BPMN approach will be developed, that will allow first modeling the problem in BPMN and dynamically generating the underlying formal constructs that will work on reasoning and model checking the correctness and reliability of the model. For this research problem to be addressed it will need a structured approach to build and evaluate the framework to ensure it has rigor and relevance. Hence, the Design Science approach will be employed to address the research problem. The specific model of Design Science research to be used in this research is that presented by Hevner et al. (2004). The future research tasks of this project are shown in the following steps:

First, develop a complete BPMN representation tool of the Airport scenario including all privacy constraints. While addressing privacy issues, functional requirements such as efficient and effective response must be taken into account. This extension to BPMN must be verified and checked. Therefore, a privacy-aware model checker will be developed based on existing formal constructs. A prototype will also be developed to test and validate the framework.

References

1. Awad, A., Weidlich, M., Weske, M.: Visually specifying compliance rules and explaining their violations for business processes. Journal of Visual Languages & Computing 22(1), 30–55 (2011)
2. Benatallah, B., Reza, H., Nezhad, H.R.M., Casati, F., Toumani, F., Ponge, J.: Service Mosaic: A Model- Driven Framework for Web Services Life-Cycle Management. IEEE Internet Computing 10(4), 55–63 (2006)
3. Business Process Modeling notation (BPMN), version 1.2, Object Management Group (OMG) (January 2009)
4. Brucker, A.D., Hang, I.: Secure and Compliant Implementation of Business Process-Driven Systems. In: La Rosa, M., Soffer, P. (eds.) BPM 2012 Workshops. LNBIP, vol. 132, pp. 662–674. Springer, Heidelberg (2013)
5. Clarke, R.: Introduction to dataveillance and information privacy, and definitions of terms (1999), `http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html`
6. Decker, G., Overdick, H., Weske, M.: Oryx- Sharing Conceptual Models on the Web. In: Li, Q., Spaccapietra, S., Yu, E., Olivé, A. (eds.) ER 2008. LNCS, vol. 5231, pp. 536–537. Springer, Heidelberg (2008)
7. Han, R., Liu, K., Ju, Y., Zhao, J.: A Petri net theory-based method for modeling web service-based systems. In: 4th WiCOM, Dalian, China, pp. 1–7 (2008)
8. He, Q.: Privacy Enforcement with an Extended Role-Based Access Control Model, North Carolina State University at Raleigh, Raleigh, NC (2003)
9. Hevner, A., March, S., Park, J., Ram, S.: Design Science in Information Systems Research. MIS Quarterly 28(1), 75–106 (2004)
10. Landau, S.: Security and privacy landscape in emerging technologies. IEEE Security & Privacy 6(4), 74–77 (2008)
11. Landgren, J., Nulden, U.: A study of emergency response work: patterns of mobile phone interaction. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1323–1332 (2007)
12. Poulovassilis, A., Papamarkos, G., Wood, P.T.: Event-condition-action rule languages for the semantic web. In: Grust, T., et al. (eds.) EDBT 2006 Workshops. LNCS, vol. 4254, pp. 855–864. Springer, Heidelberg (2006)
13. Peterson, J.L.: Petri net theory and the modeling of systems. Prentice-Hall (1981)
14. Pearson, S.: Taking Account of Privacy When Designing Cloud Computing Services. In: ICSE Workshop on Software Engineering Challenges of Cloud Computing, CLOUD 2009, pp. 44–52 (2009)
15. Rodríguez, A., Fernández-Medina, E., Piattini, M.: A BPMN Extension for the Modeling of Security Requirements in Business Processes. IEICE - Transactions on Information and Systems E90-D(4), 745–752 (2007)

16. Russell, N., van der Aalst, W.M.P., ter Hofstede, A.H.M., Wohed, P.: On the Suitability of UML 2.0 Activity Diagrams for Business Process Modelling. In: Third Asia-Pacific Conference on Conceptual Modelling (APCCM 2006). CRPIT, vol. 53, pp. 95–104 (2006)
17. Song, Y.J., Lee, D.H., Yim, J.G., Nam, T.Y.: Privacy Aware Adaptable Web Services Using Petri Nets. In: Proceedings of the 2007 International Conference on Convergence Information Technology (ICCIT 2007), pp. 1933–1938. IEEE Computer Society, Washington, DC (2007)
18. Semantic Web Rule Language (SWRL) (May 2004), http://www.w3.org/Submission/SWRL/
19. Tanasescu, V., Gugliotta, A., Domingue, J., Davies, R., Gutiérrez-Villarías, L., Rowlatt, M., Richardson, M., Stinčić, S.: A semantic web services GIS based emergency management application. In: Cruz, I., Decker, S., Allemang, D., Preist, C., Schwabe, D., Mika, P., Uschold, M., Aroyo, L.M. (eds.) ISWC 2006. LNCS, vol. 4273, pp. 959–966. Springer, Heidelberg (2006)
20. Thomas, M., Andoh-Baidoo, F., George, S.: Evresponse - moving beyond traditional emergency response notification. In: Proceedings of the Eleventh Americas Conference on Information Systems (2005)
21. van der Aalst, W.M.P., ter Hofstede, A.H.M., Weske, M.: Business Process Management: A Survey. In: van der Aalst, W.M.P., Weske, M. (eds.) BPM 2003. LNCS, vol. 2678, pp. 1–12. Springer, Heidelberg (2003)
22. Van der Aalst, W.M.P.: Formalization and verification of event-driven process chains Inform. Software Technol. 41(10), 639–650 (1999)
23. Xiaofeng, Y., Sommestad, T., Fung, C., Hung, P.C.K.: Emergency Response Framework for Aviation XML Services on MANET. In: Web Services, ICWS 2008, pp. 304-311 (2008)
24. Xu, W., Zlatanova, S.: Ontologies for Disaster Management Response. In: Li, J., Zlatanova, S., Fabbri, A. (eds.) Geomatics Solutions for Disaster Management, pp. 185–200 (2010)