CONTEXT-AWARE SECURITY IN CLOUD EMERGENCY MEDICAL SERVICES

Vassiliki Koufi, Flora Malamateniou and George Vassilacopoulos
Department of Digital Systems, University of Piraeus, 80 Karaoli & Dimitriou Str., 18534 Piraeus, Greece

Keywords: Emergency care, Personal Health Records, Cloud Computing, Web Services, Context-aware Security.

Abstract: Recently, there has been a remarkable upsurge in activity surrounding the adoption of Personal Health Records (PHRs). Since PHRs contain global patient information and not certain pieces collected by individual healthcare providers, they can be used as basic infrastructures for building and operating several important systems for both healthcare and the tax payers. Emergency medical systems (EMS) are among the most crucial ones as they involve a variety of activities which are performed from the time of a call to an ambulance service till the time of patient's discharge from the emergency department of a hospital and are closely interrelated so that collaboration and coordination becomes a vital issue for patients and for emergency healthcare service performance. This paper is concerned with the development of a PHR-based EMS in a cloud computing environment and focuses on the security aspect of delivering this particular service. Although cloud-based services can prove important in healthcare delivery, the inherent nature of medical service delivery underscores the need for ensuring that data security is better maintained. Moreover, high expectations for emergency care delivery can be achieved only if provider organizations select systems with the appropriate features, security being among the most prominent ones. Thus, the proposed EMS system comes with a suitable security mechanism in order to ensure secure access to medical information when and where needed. To this end, context-aware authorization has been embedded into the emergency care process, enabling authorization to be based not only on static rules and roles but also to be influenced by the process execution context to ensure precise and tight access control.

1 INTRODUCTION

Recent years have seen a remarkable upsurge in activity surrounding the adoption of Personal Health Records (PHR) to enable access to integrated medical information that may entail to increased patient satisfaction and continuity of care (Tang, Ash, et.al., 2006; Wiljer, Urowitz, et.al., 2008). A PHR is a consumer-centric approach to making available comprehensive healthcare information about a patient at the point of care while fully protecting patient privacy (Lauer, 2009; Win, Susilo, et.al., 2006). Unlike traditional electronic healthcare records (EHRs) that are based on the "fetch and show" model, PHR architectures are based on the fundamental assumptions that the complete records are held on a central repository (e.g. a data center) and that each patient retains authority over access to any portion of his/her record (Lauer, 2009; Wiljer, Urowitz, et.al., 2008).

Although patients are the primary beneficiaries and users of PHRs, healthcare providers may benefit from their use as well as they have both economic and quality impact (U.S. Department of Health and Human Services, 2006; Shimrat, 2009; Van der Burg and Dolstra, 2009). In particular, since patients may receive care by various healthcare providers and under various circumstances, there is a need for ubiquitous, context-aware access to relevant and timely patient information (Tentori, Favela, et.al., 2006). Moreover, several healthcare applications can be built around the PHR concept based on the integration of leading-edge networking technologies, such as cloud-based services and mobile communications, to meet healthcare needs by enabling easy and immediate access to patient data from anywhere and via almost any device. Thus, healthcare providers and organizations are increasingly considering migrating to cloud computing in an attempt to increase flexibility and agility of their healthcare systems and services and

Koufi V., Malamateniou F. and Vassilacopoulos G..
CONTEXT-AWARE SECURITY IN CLOUD EMERGENCY MEDICAL SERVICES.
DOI: 10.5220/0003106001210130
In *Proceedings of the International Conference on Health Informatics* (HEALTHINF-2011), pages 121-130
ISBN: 978-989-8425-34-8

enhance quality of patient care (Shimrat, 2009; Van der Burg and Dolstra, 2009).

Cloud computing may be able to provide a solution to the need for sharing geographically dispersed healthcare information. Cloud computing concepts may assist in accomplishing some of the goals that have been articulated by government healthcare IT policy committees. Example goals include the development of software that improves interoperability and connectivity among health information systems; infrastructure and tools for telemedicine; the promotion of interoperability of clinical data repositories; the development of self-service technologies that facilitate the use and exchange of patient information and reduce waiting times; technologies that facilitate home healthcare and patient monitoring; technologies that facilitate the continuity of care among healthcare settings; and technologies for developing mission critical applications for healthcare delivery in all levels of care (Rosenthal, Mork, et.al, 2010; Van der Burg and Dolstra, 2009). This paper is concerned with the development of emergency medical service (EMS) systems and focuses on the security of medical information stored and exchanged in dealing with emergency cases.

Emergency medical services are concerned with the provision of pre-hospital and in-hospital emergency care and their operations typically involve a wide range of interdependent and distributed activities, performed by cooperating individuals (administrative, paramedical, nursing and medical) who differ on levels of background, skill, knowledge and status. Conceptually, these activities can be interconnected to form emergency healthcare processes within and between the participating organizations (i.e. ambulance services and hospitals), thus comprising a virtual emergency healthcare enterprise within the area covered by each ambulance service. Thus, in developing an information system that supports EMS processes, it is essential to place particular emphasis on supporting individual process activities as well as on the collaboration and coordination needs among them.

The development of an EMS system as a cloud computing application which interfaces with a PHR enables immediate access to critical medical information concerning an emergency case either by authorized ambulance center personnel on site of incident and during patient transfer to a hospital or by emergency department personnel allowing them to check patient medical histories, patient medication history, patient allergies and much more to ensure that the treatment provided is the safest and most effective choice for the patient (Buyya, Yeoa, et.al., 2009).

Service-oriented architectures (SOA) can make system-to-system interfaces consistent in the enterprise architecture, thus saving resources on future integration and hopefully improving the speed at which integration can occur. The emphasis of cloud computing is to leverage the network to outsource IT functions across the entire stack. While this can include software services as in an SOA, it goes much further. Cloud computing allows the marketplace to offer many IT functions as commodities, thus lowering the cost to consumers when compared to operating them internally. On these grounds, cloud computing platform and storage service offerings can provide a value-added underpinning for SOA efforts. (Raines, 2009) Hence, combining cloud computing with SOA presents a new way for service-oriented integration (SOI) of existing healthcare systems and for developing distributed applications within and between healthcare organizations. On these grounds, ambulance services and hospital emergency departments can integrate and automate their operations by making information available where and when needed and by providing an infrastructure for the integration of pre-hospital and in-hospital emergency medical care.

One important consideration in developing an EMS system as a cloud application is security (Bruening and Treacy, 2009; U.S. Department of Health and Human Services, 2004). In addition to the usual challenges of developing secure systems, cloud computing presents an added level of risk because essential services are externalized. Thus, data security and confidentiality needs to be examined and methods developed to minimize risks and maintain privacy. For example, patients need assurances that emergency care data will not be used to harm them through disclosure to a prospective employer. Thus, there is need for adhering to appropriate privacy and security rules to provide the necessary protections and, to this end, audit trails and role-based access controls are strongly recommended (Bruening and Treacy, 2009).

This paper focuses on a role-based, context-aware authorization mechanism that is incorporated into a prototype EMS application developed as a cloud service which interacts with a cloud-based PHR and is provided to authorized users on demand. In particular, the EMS application has been implemented in the framework of NefeliPortal, a prototype medical portal which provides a web

interface to healthcare applications that are implemented in a SOA architecture over a cloud computing infrastructure. The proposed access control mechanism incorporates the advantages of role-based access control (RBAC) and yet provides the flexibility for adjusting role permissions on web service invocations and web service method executions according to context (OASIS Standards, n.d.). Thus, at run time contextual information is collected to adapt user permissions to the minimum required for completing a job.

2 CLOUD-BASED HEALTHCARE SERVICES

Cloud computing is an on-demand service model for IT provision, often based on virtualization and distributed computing technologies (IBM Corporation, 2009). It may be divided into software as a service (SaaS), which allows software offered by a third party provider to be available on demand, usually via the Internet, platform as a service (PaaS), which allows customers to develop new applications using APIs deployed and configurable remotely, and infrastructure as service (IaaS), which provides virtual machines and other abstracted hardware and operating systems which may be controlled through a service API (Shimrat, 2009; van der Burg and Dolstra, 2009). Clouds may also be divided into public, which are available publicly (i.e. any organization may subscribe), private, which are services built according to cloud computing principles, but accessible only within a private network, and partner, which are cloud services offered by a provider to a limited and well-defined number of parties.

Cloud computing provides a new information delivery and consumption model in which applications and information are accessed from a web browser while software and data are stored on servers (IBM Corporation, 2009). Cloud components communicate with one another over application programming interfaces, which are usually web services. Service computing focuses on the linkage between business processes and IT services so that business processes can be seamlessly automated using IT services. Examples of services computing technologies include SOA and web services. SOA facilitates interoperable services between distributed systems in order to communicate and exchange data with one another while web services provide the capability for self-contained business functions to operate over the Internet (Communications of the ACM, 2003).

In addition, cloud computing may be assumed a disruptive technology that has the potential to affect not only Internet services but also IT as a whole since it enables organizations to increase hardware utilization rates dramatically and scale up to massive capacities in an instant — without having to invest in new infrastructure, train new personnel or license new software. It also creates opportunities to build a better breed of network services in less time and for less money (Buyya, Yeoa, et.al., 2009; IBM Corporation, 2009). Cloud computing may be seen as an extension of the paradigm wherein the capabilities of business applications are exposed as sophisticated services that can be accessed over a network. Cloud service providers are incentivized by the profits to be made by charging consumers for accessing these services. Consumers, such as healthcare enterprises, are attracted by the opportunity for reducing or eliminating costs associated with "in-house" provision of these services. However, since cloud applications may be crucial to the core business operations of the consumers, it is essential that the consumers have guarantees from providers on service delivery, including the appropriate levels of security (Bruening and Treacy, 2009; Muttig and Burton, 2009).

There is considerable excitement over the potential benefits of operating in a cloud computing environment. In fact, several reports highlight the potential benefits of cloud computing for health – and leading the way by using it to develop new healthcare services – but they also identify at least one major stumbling block. For example, the report by the European Network and Information Security Agency says that although health agencies can see the benefits of cloud computing in terms of increased flexibility and lower cost, they are concerned about security (Bruening and Treacy, 2009; Muttig and Burton, 2009). It also uses the analysis of an actual ehealth application that uses the cloud to identify real issues about who is responsible for infrastructure faults and information governance. The agency suggests that there is a need to clarify the obligations of cloud providers to report faults and security breaches to customers and in setting minimum data protection standards.

Healthcare delivery, consumption, cost and quality as well as healthcare IT in general can benefit from this new approach to computing. Interoperability, open standards and open-source software are critical to the growth of cloud

computing (Buyya, Yeoa, et.al., 2009). Sharing patient data across the multiple institutions from which patients receive healthcare services is a problem for which no good solution currently exists. Multisite institutions with business relationships may invest in network connections and virtual private networks to perform electronic data transfers. However, such an approach is problematic and costly and adversely affects the quality of care. In a cloud computing environment, medical data could be stored in a virtual generic archive and accessed by healthcare providers as needed through the cloud. This could facilitate the sharing of medical data and significantly reduce local storage requirements. In this context data security and confidentiality will need to be examined and methods developed to minimize risks and maintain privacy (Bruening and Treacy, 2009).

Potential developments in the healthcare field include health IT architectures supporting electronic exchange or perhaps facilitate regional health information organizations or even just multiple healthcare systems wanting to share data (Lauer, 2009). The current implementations of regional healthcare information organizations are not practical for adoption as a standard approach, but cloud computing may be able to provide a solution to healthcare information sharing without geographical boundaries (Lauer, 2009). A cloud could be built to provide a way to input, store and access medical information without the need to build complex infrastructures to support outside medical record numbers or patient identifiers, dictionaries and user accounts, different databases and archive protocols, and so on.

A scenario in which patients and healthcare providers plug into front-end web services to input all of patient's information, including medications, allergies, laboratory results, medical images and so on, from wherever that patient has received medical care might be envisioned for healthcare environments of the future by evolving toward the cloud (Shimrat, 2009; Van der Burg and Dolstra, 2009). Moreover, a cloud infrastructure provides the ability of any authorized user to access web services on demand in order to retrieve patient information at the point of care as if all the information was stored in one system. One realization of this scenario constitutes the implementation of an EMS system (Anantharaman and Han, 2001).

Emergency healthcare delivery involves a variety of activities (administrative, paramedical and medical) that are performed from the time of a call for an ambulance to the time of patient's disposal from the emergency department of a hospital (Reddy, Paul, et.al. 2009). As these activities are performed in at least two organizations (i.e. ambulance service and hospital) and they are interrelated to form inter-organizational healthcare processes, collaboration and coordination become a vital issue for patients and for EMS performance. Such activities may involve basic life support (BLS) and advanced life support (ALS). For example, in the case of a cardiac patient BLS emphasizes prompt recognition of the case, treatment with oxygen and rotating tourniquets for patients in pulmonary edema. On the other hand, ALS adds skills in electrocardiogram (ECG) arrhythmia pattern recognition, antiarhythmic drug and/or defibrillation treatments, intravenous therapy and airway management with entrotracheal and/or esophageal treatment. ALS activities impose increased support requirements on an EMS: triage at the point of dispatch (i.e. assessing patient's condition), on-line medical control, ECG transmission to a hospital base for medical control and broadband wireless communications.

Conceptually, EMS activities can be interconnected to form EMS processes within and between the participating organizations (i.e. ambulance services and hospitals), thus comprising a virtual healthcare enterprise. Hence, it is important to define and automate EMS processes that span organizational boundaries so that to create and empower collaboration and coordination among the participating organizations. Standard workflow technology such as Business Process Execution Language (BPEL) and SOA provide an appropriate technological infrastructure for this purpose. They enable easy integration of possibly heterogeneous existing applications of the participating organizations by orchestrating web services through the use of BPEL (OASIS, 2007). Hence, cloud applications that are based on a number of BPEL-orchestrated web services present a new way for service-oriented integration (SOI) of existing systems and for developing distributed applications within and between healthcare organizations. Thus, through process automation and the use of web services in the context of a cloud application, ambulance service and hospital emergency departments can automate their operations by making information available where and when needed and by providing an infrastructure for the integration of pre-hospital and in-hospital emergency healthcare. A prototype implementation of this approach is considered in this paper.

The benefits accrued from the implementation of an EMS system are manifold: For example, the system puts eligibility, insurances and medical information at the physician's and other healthcare professional's fingertips when and where needed. This enables healthcare professionals to exert best practice approaches in emergency care delivery provided by the insurance scheme (Reddy, Paul, et.al. 2009). It also informs physicians of lower cost alternatives. In addition, physicians can access a timely and clinically sound view of a patient's medical history at the point of care, decreasing the risk of preventable medical errors (Anantharaman and Han, 1998; Reddy, Paul, et.al. 2009). Also, in some circumstances medical instruction routing from ambulance service physicians to ambulance paramedics electronically during patient transfer reduces the risk of medical errors associated with uninformed ordering.

One aspect of the EMS service that needs particular attention concerns home care, where physicians may need to provide medical care during home visits and cases where physicians may need to provide pharmaceutical treatment during patient transfer to a hospital by an ambulance (en-route treatment). In such cases, there is a need to ensure that medical information regarding the case (e.g. health problems, allergies, medication history) is automatically made available to the physician before prescribing and/or administering the medications needed. Thus, care inefficiencies are eliminated resulting in enhanced quality of care and cost containment (Bates, Leape, et.al. 1998).

3 MOTIVATING SCENARIO

The basic motivation for this research stems from our involvement in a recent project concerned with developing a prototype EMS system for the needs of the Greek National Health Service with the objective to improve quality of care while containing cost. To illustrate the main principles of the security architecture incorporated into the NefeliEMS, consider an EMS process scenario that shows an example of how an EMS may work. Figure 1 shows a broad view of the EMS process.

In the EMS process of Figure 1, where the ambulance service and a hospital emergency department are involved, five user roles are identified: ambulance communication operators, ambulance service physician, ambulance paramedics, emergency department physician and emergency department nurse.

Ambulance communication operators - Ambulance communication operators are located in the ambulance center premises and use an EMS application to write into a PHR system emergency case data which is provided by either the patient or another person and to pass this data to ambulance personnel.

Ambulance service physician - Ambulance service physicians are usually located in the ambulance center premises and use an EMS application to read from and write into a PHR system relevant medical data of their current patients (e.g. medical history, patient allergies and other critical health factors) so that to give appropriate medical instructions to ambulance paramedics, regarding en route treatment, that are also recorded.

Ambulance paramedics - Ambulance paramedics use an EMS application, via a smart handheld device, to read authorized portions of medical data from a PHR system and write data regarding the paramedic activities performed on the patient at the site of incident and en route.

Emergency department physician - Emergency department physicians use an EMS application to read from and write into a PHR system relevant medical data of their current patients (e.g. medical history, patient allergies and other critical health factors).

Emergency department nurse - Emergency department nurses use an EMS application to read authorized portions of patient data from a PHR system, to write a nursing assessment of patient's condition (triage) and to write data of the nursing activities performed on the patient.

From a role-based authorization perspective in a process-oriented environment, the business process of Figure 1 surfaces several requirements with regard to task execution and associated data accesses. These requirements include the following:

- **Task Execution -** Task execution specified by a role-to-task permission assignment may be further restricted dynamically during EMS process execution and be a subset of the authorized role holders. For example, medical instructions to ambulance personnel may only be provided by physicians who are currently at the ambulance service premises and are assigned to deal with the particular case (having access to the "Provide & Write Medical Instruction" task).
- **Data Access -** Some role holders are allowed to exercise a set of permissions on certain data objects only and/or for a limited duration. For

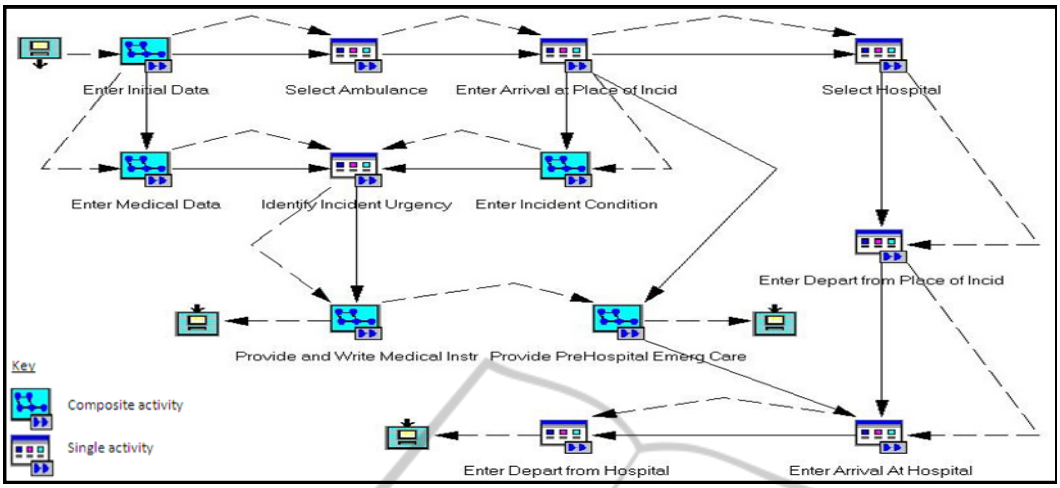

Figure 1: A high level model of an emergency care process.

example, during the execution of the "Provide & Write Medical Instruction" task, a physician may be allowed to read patient records only for his/her patients and the permission to read patient records may be revoked upon successful task execution.

Table 1 shows an extract of authorization requirements regarding task execution and related data access privileges assigned to the roles of "ambulance communication operators", "ambulance service physicians" and "ambulance service paramedics", "emergency department physicians" and "emergency department nurses", respectively. These requirements suggest that certain task execution and associated data access permissions of the EMS process participants depend on the EMS process execution context. In particular, contextual information available during process execution, like user/patient relationship, location or time, can influence the authorization decision that allows a user to perform a task and access associated data objects. This enables a more flexible and precise authorization policy specification that incorporates the advantages of having broad, role-based permissions across process tasks and object classes, like RBAC, yet enhanced with the ability to simultaneously support the above requirements.

Given a cloud PHR architecture, where relevant medical data are accessed via web services, the above authorization requirements of the EMS process can be translated into authorization requirements with regard to web service invocations and associated method executions as follows:

- **Web Service Invocation:** Web service invocations for EMS and PHR access may be specified by a role-to-web service permission assignment.
- **Method Execution:** Given an authorization for invoking a web service, role holders can execute a dynamically determined set of web service methods subject to contextual constraints (e.g. user/patient proximity, time and location of method execution).

Table 1: Extract of authorization requirements for the emergency process.

1	Ambulance communication operators may write current patient data into relevant portions of PHRs from within ambulance center premises only.
2	Ambulance service physicians may read and write relevant portions of PHRs of their current patients and from within ambulance center premises only.
3	Ambulance service paramedics may read and write relevant portions of PHRs of their current patients and from within ambulances only.
4	Emergency department physicians may read and write relevant portions of PHRs of their current patients and from within hospital premises only.
5	Emergency department nurses may read and write relevant portions of PHRs of their current patients and from within hospital premises only.

Thus, permission is defined as the authority to invoke a specific web service and/or to execute a web service method on a class of objects. A role is then defined as a collection of such permissions. A user may be granted membership of a role, but the role membership is only valid within a certain context that limits the applicability of the role's permissions to a subset of the process instances. The advantage of this approach is that the role context can be specified by the system administrator at the time of role creation and remains valid unless the role definition itself changes.

4 SYSTEM ARCHITECTURE

The EMS system comprises a number of BPEL-orchestrated web services that are called either by the ambulance service personnel or by the physicians and nurses of a hospital emergency department. The whole process starts when the telephone operator of the ambulance service receives an emergency call and records the case's demographic and medical data. If a physician of either the ambulance service or the emergency department of a hospital requests past medical data of the current patient, the appropriate web service is invoked. This takes as input the doctor's role and the patient's code or name and searches the patient's PHR to retrieve authorized portions of medical data. Case data collected by the ambulance service personnel and by the personnel of the emergency department of a hospital form two separate XML documents that are recorded into the cloud storage. These XML documents are formed automatically upon recording ambulance arrival at the emergency department of a hospital and when the patient is discharged from the emergency department, respectively.

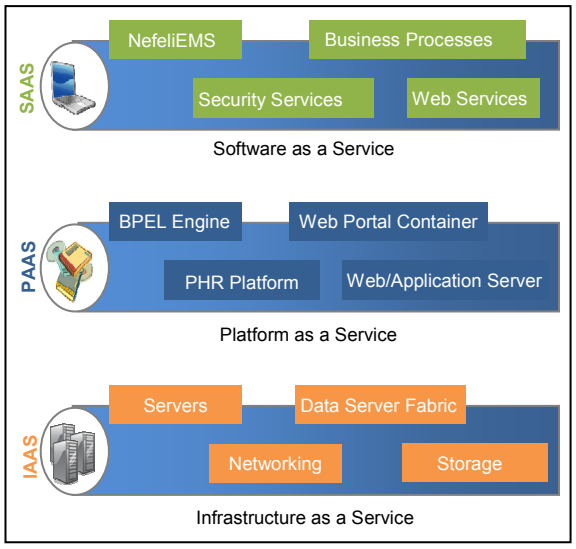

Figure 2: System Architecture.

Figure 2 shows a high-level architectural view of the prototype NefeliPortal cloud computing environment. In essence, this architecture refers to both the PHR system and the EMS application delivered as services over the Internet and the hardware and systems software in the data centres that provide those services. Thus, central to the cloud architecture is the PHR component which is accompanied by a number of peripheral applications such as the EMS system component. These applications are licensed for use as services and are provided to authorized users on demand. The application software of both the PHR and the EMS component consists of a number of web services which are deployed and orchestrated using BPEL. Authorized users interact with NefeliPortal through either a desktop workstation or a mobile device such as a Personal Digital Assistant (PDA) that run an HTTP(S)-based client.

In our implementation, process models were used for the definition of web services and web services were used for process activity implementations. Specifically, there exists a web service of the mechanism for retrieving past medical data of a patient by authorized users. This web service is used by the ambulance service and the emergency department of a hospital on demand as a BPEL activity implementation. The system architecture is illustrated on Figure 3.

In broad terms, the architecture of the prototype NefeliPortal cloud computing environment consists of the following main components:

- **PHR Application:** PHR architectures are based on the fundamental assumptions that the complete patient records are centrally stored and that each patient retains authority over access to any portion of his/her record. Hence, the PHR platform consists of a *data repository* which stores patient data and a *user interface* which allows patients to access their own information and authorized healthcare professionals to access appropriate parts of patient information.
- **EMS Application:** The EMS application consists of a data repository which stores emergency medical data and the *application software* comprised by a number of BPEL-orchestrated web services that are accessed by authorized personnel of the ambulance service and the emergency department. Users which are authorized to use the EMS system for some patients are also authorized to access certain portions of the PHR of these patients.
- **Portal:** The portal component provides a web-based front end to PHR and EMS processes. Authorized users enter the portal to interact with either the PHR or the EMS system. The portal is flexibly sized so that to fit in PDA or mobile phone screen, which is particularly useful in cases where there is a need for remote

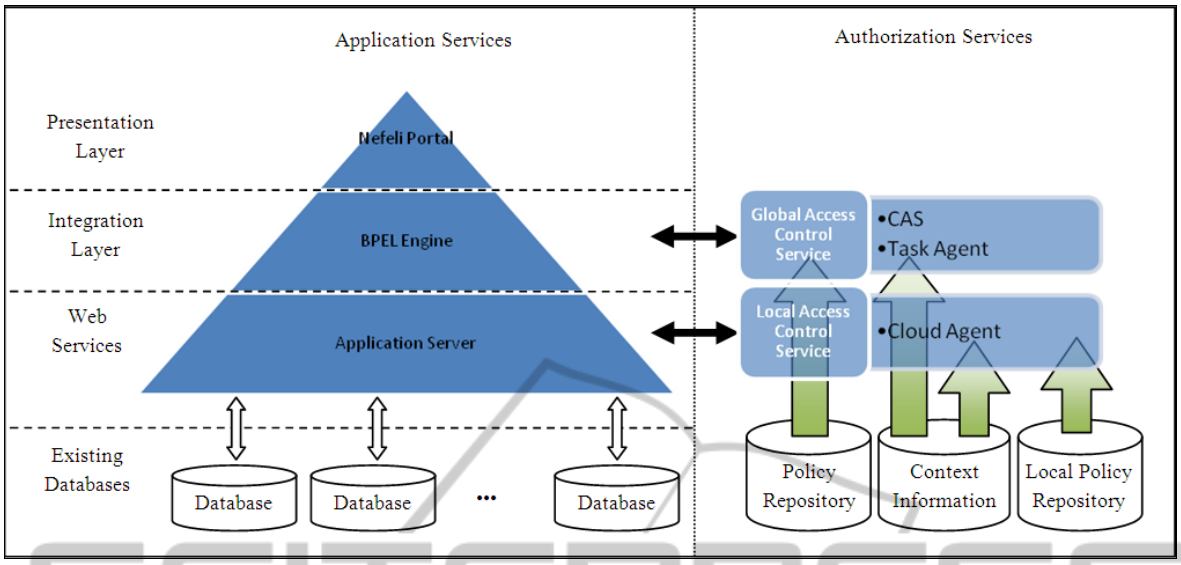

Figure 3: Security Architecture of NefeliEMS Service.

access to these applications (e.g. in emergency cases where the patient's PHR is accessed through a wireless network either from the place of incident or from the ambulance en route).

5 AUTHORIZATION ARCHITECTURE

A significant issue in cloud computing is the lack of delegated authorization. While some cloud services provide for delegated strong authentication that enables access control based on user identity, few, if any, provide delegated authorization to enable access control based on contextual information and user roles. This capability is turning out to be increasingly important as fine-grained entitlements for authorization management and control will be most essential. Hence, more granular authorization is needed. Authorization can be coarse-grained within an enterprise or even a private cloud, but in order to handle sensitive (such as medical) data and compliance requirements, public clouds will need granular authorization capabilities (such as role-based access controls and IRM) that can be persistent throughout the cloud infrastructure and the data's lifecycle (Bruening and Traecy, 2009; IBM Corporation 2009).

As the number of partners and shared resources increase, one will face extra labour to manage permissions. There is also extra risk of inappropriate data release, due to having more users who may misunderstand policy or be careless or malicious. Hence, a security system must be implemented that reduces the possibility of breaching patient privacy under any circumstances. To this end, one important issue is to define and enforce authorization constraints that are both effective and efficient.

Figure 3 shows a high-level view of the authorization architecture implemented into NefeliPortal. The access control mechanism uses collected contextual information to mediate between subjects (healthcare professionals) and objects (web services and associated tasks) to decide whether execution of an object by a given subject should be permitted or denied. The access control mechanism is certificate-based as it relies on Community Authorization Service (CAS) certificates issued to healthcare professionals by a CAS server. These certificates specify user-to-role assignments in the form of security assertions, expressed in Security Assertion Markup Language (SAML) (Pearlman, Welch, et.al., 2002). The role-to-permission (role-to-web service invocation and role-to-task execution) mapping is performed by means of access control policies expressed by using the RBAC profile of eXtensible Access Control Markup Language (XACML) (OASIS Standards, n.d).

In the NefeliPortal prototype, the contextual information is determined by a pre-defined set of attributes related to the user (e.g. user certificate, user/patient relationship), to the environment (e.g. location and time of attempted access) and to the client or healthcare organization (e.g. local security policy). Contextual information is collected by a Context Manager which consists of two kinds of

agents developed in JADE (Java Agent Development Framework, n.d.):

- **Cloud Agent:** Hosted on a cloud server and manages user permissions on web services.
- **Task Agent:** Hosted on a cloud server and manages user permissions on web service methods.

Each agent uses context collection services to monitor context and interacts with a state machine that maintains the permission subset of each role. The state machine consists of variables that encode state (permissions assigned to each role) and events that transform its state. Upon an attempted access (either to a web service or to an associated task), the relevant agent generates an event to trigger a transition of the state machine. Changes in user and environmental context are sensed by both agents, whereas changes in client context are sensed and dealt with by the cloud agent of each client node.

6 IMPLEMENTATION ISSUES

The prototype implementation of the EMS system and its authorization architecture has been developed on a laboratory cloud computing infrastructure. The system has been developed as a web application using the Apache/Tomcat as Web/Application Server. The platform used for the generation of sample patient PHRs is Care2X Integrated Healthcare Environment (Care2X Integrated Healthcare Environment, n.d.). Although Care2X is not a PHR platform but an open source Web based hospital information system, it has been considered sufficient for the purpose of our research. In order to enable access to data stored in Care2X repository a number of web services have been implemented which make use of the Care2X Application Programming Interface (API). The BPEL engine used for the execution of BPEL healthcare processes is ActiveBPEL, an open source BPEL Engine (Active Endpoints, n.d.). NefeliPortal that provides access to this engine is based upon IBM WebSphere portal framework (IBM, n.d.), a JSR-168 compliant portal (JSR-168 Portlet Specification, n.d.).

Development of cloud computing applications that provide readily access to integrated healthcare information at the point of care introduces security risks especially with regard to authorization and access control. To this end, a suitable security mechanism is embedded into the proposed cloud portal application, which ensures authorized data access through the invocation of relevant web services. Authorization decisions are made subject to the constraints imposed by the execution context.

With regard to web service invocation, the security mechanism acts as follows: Upon submitting a request for invoking a web service, the roles contained in the CAS certificate accompanying the request are extracted and their permissions regarding web service invocations are specified using a file where XACML policies have been stored. Then, during web service execution, a request for executing one of the associated tasks is issued which is accompanied by the same CAS certificate. The roles extracted from this certificate are used in order to specify the permissions regarding BPEL task executions using XACML policies which are stored at each client node (i.e. healthcare organization). Permissions on both web services and associated BPEL tasks are dynamically adapted by the constraints imposed by the current context.

7 CONCLUDING REMARKS

Healthcare organizations are faced with the challenge to improve quality by preventing medical errors, to reduce costs by improving administrative efficiencies, to reduce paperwork and to increase access to affordable healthcare. One important healthcare delivery application is EMS system which has been modeled as an inter-organizational process involving ambulance services and hospital emergency departments based on the need for integrating pre-hospital and in-hospital emergency care activities into a virtual healthcare enterprise.

Cloud computing and SOA convergence can be used to meet the increased collaboration and coordination requirements between emergency healthcare process participants by facilitating relevant information access by authorized people where and when needed. Cloud computing was used to produce a flexible and scalable system, supporting interoperability and execution of platform independent applications while providing secure access to sensitive data. This paper presents a cloud EMS system, within the context of a prototype healthcare portal, namely NefeliPortal. One important characteristic of the proposed system specifically calls for the integration of EMS systems with PHRs and, possibly, other external systems since systems integration is a prerequisite for accurate safety alerts, patient monitoring, and other recommended capabilities.

Development of cloud computing applications that provide readily access to healthcare information introduces security risks especially with regard to authorization and access control. Hence, this paper presented a context-aware security framework which can be embedded into the EMS cloud application to ensure authorized invocation of web services and execution of associated web service tasks subject to contextual constraints. The security framework proposed should aid EMS developers in comparing alternative systems and in prioritizing their development efforts. However, there is an obvious need for its real world validation before it is widely adopted. This requires setting up a cloud computing infrastructure for eHealth services, an endeavour that needs much more than proven technological feasibility.

REFERENCES

Communications of the ACM, 2003. Service-Oriented Computing, 46 (10).

Active Endpoints, ActiveBPEL Open Source Engine Project, http://www.activebpel.org/

Anantharaman, V., Han, L., 2001. Hospital and emergency ambulance link: IT to enhance emergency pre-hospital care, *International Journal of Medical Informatics*, 61: 147–161.

Ash, J. S., Berg, M., Coiera, E., 2004. Some Unintended Consequences of Information Technology in Health Care: The Nature of Patient Care Information System Related Errors. *Journal of American Medical Informatics Association*, 11(2): 104-112.

Bates, D. W., Leape, L. L., Cullen, D. J., Laird, N., Petersen, L. A., Teich, J. M., et.al., 1998. Effect of Computerized Physician Order Entry and a Team Intervention on Prevention of Serious Medication Errors. *Journal of the American Medical Association*, 280(15): 1311–1316.

Bruening, P., Treacy, B, 2009. Cloud Computing: Privacy, Security Challenges. *In The Bureau of National Affairs*.

Buyya, R., Yeoa, C. S., Venugopala, S., Broberga, J., and Ivona Brandicc, I., 2009. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25: 599-616.

Care2X Integrated Healthcare Environment, http://www.care2x.org/

IBM, IBM Websphere, www.ibm.com/websphere

IBM, 2009. IBM Point of View: Security and Cloud Computing, Cloud Computing White paper, ftp:// public.dhe.ibm.com/common/ssi/sa/wh/n/tiw14045usen/TIW14045USEN_HR.PDF

Java Agent Development Framework, http://jade. tilab.com/.

JSR-168 Portlet Specification, http://www.jcp.org/ aboutJava/communityprocess/final/ jsr168/

Lauer, G., 2009. Health Record Banks Gaining Traction in Regional Projects, http://www.ihealthbeat.org/ features/2009/health-record-banks-gaining-traction-in-regional-projects.aspx

Muttig I., Burton C., 2009. Cloud Security Technologies. *Information Security Technical Report*, 14: 1-6.

OASIS Standards, http://www.oasis-open.org/

OASIS, 2007. OASIS Web Services Business Process Execution Language (WSBPEL) v.2, http://docs.oasis-open.org/wsbpel/2.0/wsbpel-v2.0.pdf

Pearlman, L., Welch, V., Foster, I., Kesselman, C., Tuecke, S., 2002. A Community Authorization Service for Group Collaboration. *In the 3rd IEEE International Workshop on Policies for Distributed Systems and Networks*.

Raines, G., 2009. Cloud Computing and SOA. Service-Oriented Architecture (SOA) Series, Systems Engineering at MITRE.

Reddy, M. C., Paul, S. A., Abraham, J., McNeese,M., DeFlitch, C., Yen, J., 2009. Challenges to effective crisis management: Using information and communication technologies to coordinate emergency medical services and emergency department teams. *International Journal of Medical Informatics*, 78 (4): 259-269.

Rosenthal A., Mork, P., Lia, M. H., Stanforda, J., Koestera, D., Reynolds, P., 2010. Cloud computing: A new business paradigm for biomedical information sharing. *Journal of Biomedical Informatics*, 43: 342-253.

Shimrat, O., 2009. Cloud Computing and Healthcare, San Diego Physician.org.

Tang, P. C., Ash, J. S., Bates, D. W., Overhage, J. M., Sands, D. Z., 2006. Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. *Journal of American Medical Informatics Association*, 13 (2): 121-126.

Tentori, M., Favela, J., Rodriguez, M. D., 2006. Privacy-Aware Autonomous Agents for Pervasive Healthcare, *IEEE Intelligent Systems Magazine*, 21 (6): 55-62.

U.S. Department of Health and Human Services: Personal Health Records and Personal Health Record Systems, A Report and Recommendations from the National Committee on Vital and Health Statistics, 2006.

Van der Burg, S., Dolstra, E., 2009. Software Development in a Dynamic Cloud: From Device to Service Orientation in a Hospital. Environment, In *2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing*.

Wiljer, D., Urowitz, S., Apatu, E., DeLenardo, C., Eysenbach, G., Harth, T., Pai, H., Leonard, K. J., 2008. Patient accessible electronic health records: exploring recommendations for successful implementation strategies. *Journal of Medical Internet Research*,. 10 (4).

Win, K. T., Susilo, W., Mu, Y., 2006. Personal Health Record Systems and Their Security Protection. *Journal of Medical Systems*, 30: 309-315.