مدل کنترل دسترسی پویای حافظ حریم خصوصی با قابلیت وکالت دسترسی در سلامت الکترونیکی

فائقه غفرانی و مرتضی امینی*

دانشکده مهندسی کامپیوتر، دانشگاه صنعتی شریف، تهران، ایران

چکیده

گسترش استفاده از فناوری اطلاعات و به‌طور خاص اینترنت اشیا در حوزه سلامت الکترونیکی، مسائل مختلفی را به‌همراه دارد که از مهم‌ترین آنها مسأله امنیت و کنترل دسترسی است. در این راستا نیازمندی‌های مختلفی از جمله مسأله دسترسی پزشک به پرونده بیمار بر اساس موقعیت فیزیکی پزشک، مسأله تشخیص شرایط اضطراری و اعطای پویای دسترسی موقت به پزشک حاضر، حفظ حریم خصوصی بیمار بر اساس ترجیحات وی و مسأله اعطای وکالت دسترسی به حقوق دسترسی پزشک دیگر مطرح است که در مدل‌های ارائه‌شده تاکنون پوشش داده نشده است. در این مقاله یک مدل کنترل دسترسی پویا و حافظ حریم خصوصی با قابلیت وکالت دسترسی در سلامت الکترونیکی با نام TbDAC ارائه شده است؛ به‌طوری‌که هنگام دسترسی پزشکان و پرستاران به پروندهٔ بیمار بتواند چالش‌های امنیتی مطرح در این محیط‌ها را برطرف‌کند. با پیاده‌سازی یک سامانه کنترل دسترسی بر اساس مدل پیشنهادی و بررسی سناریوهایی واقعی در محیط بیمارستانی با استفاده از آن، کاربرد عملی این مدل در محیط واقعی و کارایی آن نشان داده شده است.

واژگان کلیدی: سلامت الکترونیکی، اینترنت اشیا، کنترل دسترسی پویا، حفظ حریم خصوصی، وکالت دسترسی

Privacy Preserving Dynamic Access Control Model with Access Delegation for eHealth

Faegheh Ghofrani & Morteza Amini*

Department of Computer Engineering, Sharif University of Technology, Tehran, Iran

Abstract

eHealth is the concept of using the stored digital data to achieve clinical, educational, and administrative goals and meet the needs of patients, experts, and medical care providers. Expansion of the utilization of information technology and in particular, the Internet of Things (IoT) in eHealth, raises various challenges, where the most important one is security and access control. In this regard, different security requirements have been defined; such as the physician's access to the patient's EHR (electronic health record) based on the physician's physical location, detection of emergency conditions and dynamically granting access to the existing physician or nurse, preserving patients' privacy based on their preferences, and delegation of duties and related permissions. In security and access control models presented in the literature, we cannot find a model satisfying all these requirements altogether. To fill this gap, in this paper, we present a privacy preserving dynamic access control model with access delegation capability in eHealth (called TbDAC). The proposed model is able to tackle the security challenges of these environments when the physicians and nurses access the patients' EHR. The model also includes the data structures, procedures, and the mechanisms necessary for providing the access delegation capability.

The proposed access control model in this paper is in fact a family of models named TbDAC for access control in eHealth considering the usual hospital procedures. In the core model (called $TbDAC_0$), two

* Corresponding author

*نویسندهٔ عهده‌دار مکاتبات

• تاریخ ارسال مقاله: ۱۳۹۷/۰۷/۲۷ • تاریخ پذیرش: ۱۳۹۸/۱۱/۰۲ • تاریخ انتشار: ۱۳۹۹/۰۹/۱۵ • نوع مطالعه: پژوهشی

[DOI: 10.29252/jsdp.17.3.109]

primitive concepts including team and role are employed for access control in hospitals. In this model, a set of permission-types is assigned to each role and a medical team (including a set of hospital staff with their roles) is assigned to each patient. In fact the role of a person in a team determines his/her permissions on the health information of the patient. Since patients' vital information is collected from some IoT sensors, a dynamic access control using a set of dynamic and context-aware access rules is considered in this model. Detecting emergency conditions and providing proper permissions for the nearest physicians and nurses (using location information) is a key feature in this model.

Since health information is one of the most sensitive individuals' personal information, the core model has been enhanced to be a privacy preserving access control model (named $TbDAC_1$). To this aim, the purpose of information usage and the privacy preferences of the patients are considered in the access control enforcement procedure.

Delegation of duties is a necessity in medical care. Thus, we added access delegation capability to the core model and proposed the third member of the model family, which is named $TbDAC_2$. The complete model that considers all security requirements of these environments including emergency conditions, privacy, and delegation is the last member of this family, named $TbDAC_3$. In each one of the presented models, the therapeutic process carried out in the hospitals, the relational model, and the entities used in the model are precisely and formally defined. Furthermore in each model, the access control process and the dynamic access rules for different situations are defined.

Evaluation of the proposed model is carried out using three approaches; comparing the model with the models proposed in related research, assessing the real-world scenarios in a case study, and designing and implementing a prototype of an access control system based on the proposed model for mobile Android devices. The evaluations show the considerable capabilities of the model in satisfying the security requirements in comparison to the existing models which proposed in related research and also its applicability in practice for different simple and complicated access scenarios.

Keywords: eHealth, IoT, Dynamic Access Control, Privacy, Access Delegation

۱- مقدمه

واژهٔ سلامت الکترونیکی که از سال ۲۰۰۰ عمومیت یافته، مفهوم جدیدی است که به استفاده از فناوری اطلاعات و ارتباطات در حیطهٔ بهداشت اطلاق می‌شود. طبق تعریف سازمان جهانی بهداشت [1]، سلامت الکترونیکی به معنای انتقال منابع سلامت و مراقبت‌های بهداشتی از طریق وسایل الکترونیکی و شامل سه حوزهٔ اصلی است: (۱) ارائهٔ اطلاعات پزشکی به فرد متخصص از طریق اینترنت و ارتباطات راه دور (۲) استفاده از فناوری اطلاعات و تجارت الکترونیکی برای بهبود خدمات پزشکی از طریق آموزش افراد مرتبط (۳) استفاده از تجارت الکترونیکی و کسب‌وکار الکترونیکی در مدیریت نظام پزشکی.

استفاده از سامانه‌های الکترونیکی سلامت دارای مزیت‌هایی از جمله افزایش کیفیت سلامت و ایمنی بیماران، کاهش خطای پزشکی، کاهش زمان دسترسی به اطلاعات مورد نظر و کاهش هزینه است؛ همچنین پزشک می‌تواند از تداخل‌ها یا حساسیت‌های دارویی هنگام تجویز دارو [2] مطلع شود؛ به‌علاوه سامانه‌های الکترونیکی سلامت، جمع‌آوری و به اشتراک‌گذاری داده‌های بالینی الکترونیکی بین سازمان‌های مختلف مراقبت‌های بهداشتی را به‌سادگی امکان‌پذیر می‌سازند.

در سال‌های اخیر با کاربرد وسیع اینترنت اشیا (IoT[1]) در سلامت الکترونیکی مواجه هستیم. واژهٔ اینترنت اشیا نخستین‌بار توسط کوین اشتون [3] در سال ۱۹۹۹ در زمینهٔ مدیریت زنجیرهٔ تأمین مطرح، اما به‌مرور تعاریف وسیع‌تری از آن ارائه شد. طبق تعریف رابرت و همکارانش [4]، «به شبکه‌ای از تجهیزات دریافت داده مانند RFID، حس‌گرهای مادون قرمز، سامانه‌های موقعیت‌یاب جهانی(GPS)، پویش‌گرهای لیزری و دیگر ابزار سنجش اطلاعات که بر اساس پروتکل توافق‌شده برای اتصال همه‌چیز به اینترنت با یکدیگر ادغام می‌شوند، اینترنت اشیا می‌گوییم. هدف از ارائهٔ این مجموعه رسیدن به مدیریت و شناسایی آسان این تجهیزات است».

با کاربرد اینترنت اشیا در سلامت الکترونیکی، هنگامی‌که بیمار در بیمارستان یا دور از آن است، حس‌گرهای متصل به بدن بیمار اطلاعات سلامت وی از جمله ضربان قلب، فشار خون و تنفس را اندازه‌گیری کرده و از طریق دستگاه‌هایی همچون تلفن همراه به شبکه ارسال می‌کنند [5]. این اطلاعات باید به‌صورت امن به پایگاه دادهٔ بیمارستان برسند [6]. برای هر بیمار در پایگاه داده یک پروندهٔ الکترونیکی سلامت (EHR[2]) ایجاد می‌شود که طبق

[1] Internet of things
[2] Electronic Health Records

[DOI: 10.29252/jsdp.17.3.109]

تعریف لاکویدیس [7]، EHR عبارت است از «اطلاعات سلامت ذخیره‌شده به‌صورت دیجیتال در طی زندگی یک فرد با هدف حمایت از تداوم مراقبت، آموزش، پژوهش و حصول اطمینان از محرمانه‌بودن اطلاعات در همهٔ زمان‌ها».

از آنجایی‌که اطلاعات سلامت جزء مهم‌ترین اطلاعات هر فرد شناخته می‌شود و افشای آن به افراد غیر مجاز ممکن است، باعث ایجاد خطرات امنیتی یا حتی جانی برای فرد شود، وجود یک سازوکار کنترل دسترسی پویا با لحاظ‌کردن ملاحظات حریم خصوصی بیماران امری ضروری است.

بر اساس مطالعات انجام‌شده توسط پژوهش‌گران این حوزه و بررسی‌های میدانی انجام‌شده در دو بیمارستان بزرگ ایران، توسط نویسندگان این مقاله، می‌توان نیازمندی‌های کنترل دسترسی در محیط‌های سلامت را به سه دسته تقسیم کرد. توضیح این‌که در این بررسی میدانی مجموعه فرآیندهای بیمارستانی، قوانین و مقررات حاکم بر این بیمارستان‌ها (مطابق شیوه‌نامه‌های ابلاغی وزارت بهداشت، درمان و آموزش پزشکی) و استانداردهای بین‌المللی مطرح در این خصوص از طریق مصاحبه با بخش‌های مختلف بیمارستانی استخراج و مورد بررسی و تحلیل قرار گرفت.

۱- نیازمندی‌های عمومی کنترل دسترسی

- *رعایت اصل کمینه مجوزها:* فقط اطلاعاتی که به‌طور خاص برای کاربر ضروری است در اختیارش قرار داده شود و سایر اطلاعات از دید کاربر پنهان شود [8].
- *رعایت اصل تفکیک وظایف:* مجموعه مجوزها و نقش‌های داده‌شده به یک فرد نباید طوری باشد که منجر به تضعیف خط‌مشی‌های مرکز بهداشتی-درمانی شود یا حریم خصوصی بیمار را به مخاطره بیاندازد [9].
- *کنترل دسترسی ریزدانه:* سطح دسترسی به اطلاعات بر روی منابع به‌صورت جزئی مشخص شود [10].

۲- نیازمندی‌های بیماران در کنترل دسترسی

- بیمار باید حق کنترل روی پرونده‌های سلامت خود را داشته باشد، همچنین بتواند تعیین کند که چه کسی حق استفاده از اطلاعاتش را دارد [11].
- بیمار باید توانایی مشاهدهٔ این‌که چگونه و چه وقت اطلاعاتش مورد دسترسی کاربران قرار می‌گیرد و چه کسانی این حق دسترسی را با چه هدف دسترسی به آن‌ها می‌دهند، داشته باشد [11].

۳- نیازمندی‌های سازمانی در کنترل دسترسی

- *امکان اعطای حق وکالت و بازپس‌گیری آن:* ممکن است کاربری مانند پزشک یا پرستار در شرایطی (مانند مسافرت) مجبور باشد مجوزهای خود را به پزشک یا پرستار دیگری منتقل کند و در زمان مناسب آن را بازپس‌گیرد [12].
- *دسترسی در موارد اضطراری (اورژانس):* مدل و سازوکار کنترل دسترسی باید به‌صورت پویا به‌گونه‌ای عمل کند که در موارد اضطراری بتواند به افراد مورد نیاز (مانند پزشک حاضر در صحنه) مجوزهایی اعطا کند که در شرایط عادی، آن مجوزها را ندارند [13].
- *همکاری با سازمان‌های دیگر:* از آنجایی‌که در کاربرد سلامت الکترونیکی، بیمارستان‌ها و یا مراکز بهداشتی-درمانی با سازمان‌های دیگر از جمله سازمان‌های بیمه، تأمین‌کنندگان دارو، مراکز پژوهشی در حوزهٔ پزشکی و سلامت یا بیمارستان‌های دیگر در ارتباط هستند و اطلاعات بیمار بین این سازمان‌ها به اشتراک گذاشته می‌شود، ممکن است هر یک از آن‌ها خط‌مشی‌های منابع خود را بر اساس ترجیحات بیماران داشته باشند؛ به همین دلیل چارچوب کنترل دسترسی باید بتواند سازگاری بین این خط‌مشی‌ها را برای همکاری بهتر فراهم کند [14].
- *امکان اعمال محدودیت‌های زمینه‌ای:* هنگامی‌که یک پزشک یا پرستار درخواست دسترسی به اطلاعات بیماران را دارد، این دسترسی باید بر اساس اطلاعات زمینه‌ای مانند زمان و مکان درخواست‌کننده، به شکل پویا قابل کنترل باشد [15].

مسأله حریم خصوصی که به‌عنوان یکی از نیازمندی‌های مهم بیماران در کنترل دسترسی به آن اشاره شد به اندازه‌ای قابل توجه است که برای حفظ آن طی سالیان مختلف قوانین و استانداردهای متعددی از جمله استاندارد HIPAA تدوین شده است. برخی از اصول اساسی که برای سامانه‌های حافظ حریم خصوصی بیان شده عبارت‌اند از:

- *آگاهی:* هیچ داده‌ای نباید بدون اطلاع مالک آن جمع‌آوری شود و هرگونه دسترسی به داده‌های خصوصی باید به اطلاع آن‌ها برسد.
- *انتخاب و رضایت:* جمع‌آوری داده‌های خصوصی بدون جلب رضایت صریح مالک آن‌ها مجاز نیست.

[DOI: 10.29252/jsdp.17.3.109]

- *مجاورت و محلی‌بودن:* داده‌ها و اطلاعات از مرزهای فیزیکی یک مکان مورد اعتماد خارج نشوند.
- *الزامات امنیتی:* حفاظت از حریم خصوصی مستلزم ایجاد یک بستر امن برای داده‌های خصوصی است، مانند رمزگذاری داده‌ها.

یکی دیگر از نیازمندی‌های بیماران در کنترل دسترسی، توجه به مسألهٔ وکالت دسترسی است که با وجود اینکه در سناریوهای واقعی در محیط سلامت بسیار مطرح است، اما در محیط پژوهشی کمتر به آن توجه شده است. وکالت دسترسی زمانی مطرح می‌شود که هر یک از عوامل بیمارستانی (مانند پرستار یا پزشک) که در تیم پزشکی یک فرد هستند به هر دلیل نتوانند وظایف خود را (برای مثال به‌دلیل مرخصی یا مسافرت) در قبال بیمار به انجام رسانند و لذا بخواهند که آن را به فرد مجاز دیگری طی یک فرآیند قانونی واگذار کنند. نحوه اعطای وکالت دسترسی به کاربران دیگر و بازپس‌گیری آن در عین حفظ حریم خصوصی بیمار و همچنین عدم تداخل بین وکالت‌های اعطاشده از دیگر جزییاتی است که در وکالت دسترسی لازم است، مدنظر قرار گیرند.

در سال‌های اخیر مدل‌ها و سازوکارهای کنترل دسترسی مختلفی با هدف رفع این نیازمندی‌ها ارائه شده است و تا حدی توانسته‌اند مشکلات مربوط به حریم خصوصی و یا وکالت را به‌صورت جداگانه برطرف کنند؛ اما روشی که در آن همهٔ این نیازمندی‌ها برطرف شده باشند، ارائه نشده است. هدف ما در این مقاله ارائهٔ یک مدل و سازوکار کنترل دسترسی با قابلیت وکالت دسترسی در سلامت الکترونیکی است؛ به‌طوری‌که هنگام دسترسی پزشکان و پرستاران به اطلاعات دریافتی از حس‌گرها و پروندهٔ بیمار، بتواند چالش‌های امنیتی مطرح در این محیط‌ها از جمله مسألهٔ دسترسی به پروندهٔ بیمار توسط پزشک بر اساس موقعیت فیزیکی پزشک، مسألهٔ تشخیص شرایط اضطراری و اعطای دسترسی موقت به پزشک حاضر و به‌خصوص مسألهٔ اعطای وکالت دسترسی به پزشک دیگر را برطرف کند. همچنین داده‌ساختارها، پروتکل‌ها و سازوکارهای لازم را برای برخورداری از قابلیت وکالت دسترسی نیز داشته باشد.

پس از مقدمهٔ بیان‌شده، در ادامهٔ این مقاله در بخش دوم به مرور کارهای پیشین در زمینهٔ کنترل دسترسی در سلامت الکترونیکی می‌پردازیم. در بخش سوم مدل کنترل دسترسی پیشنهادی با قابلیت اعطای وکالت دسترسی برای رفع نیازمندی‌های کنترل دسترسی در محیط سلامت الکترونیکی ارائه می‌شود. بخش چهارم به ارایه نتایج حاصل از ارزیابی‌های کیفی و کمی انجام‌شده بر روی مدل و سازوکار پیشنهادی پرداخته می‌شود و درنهایت در بخش پنجم به جمع‌بندی نتایج حاصل از این مقاله می‌پردازیم.

۲- کارهای پیشین

مدل‌ها و سازوکارهای مختلفی جهت کنترل دسترسی در محیط‌های سلامت الکترونیکی ارائه شده است که هر کدام توانسته‌اند فقط بخشی از نیازمندی‌های کنترل دسترسی در این محیط‌ها را برطرف کنند. در این بخش به بررسی این مدل‌ها پرداخته شده است.

ابتدا سه مدل کنترل دسترسی اختیاری، اجباری و نقش‌مبنا برای استفاده در محیط‌های سلامت الکترونیکی مطرح شد که به‌دلیل معایبی که داشتند، قادر نبودند به‌تنهایی نیازمندی‌های موجود در این محیط‌ها را برطرف کنند. در مدل کنترل دسترسی اختیاری (DAC)، هر کاربری که مسئول جمع‌آوری اطلاعات است، مالک اطلاعات یا منابع موردنظر می‌شود؛ درصورتی‌که در کاربرد سلامت الکترونیکی، به‌دلیل تعداد زیاد افرادی که اطلاعاتشان را وارد می‌کنند، هیچ‌کس نمی‌تواند ادعا کند که مالک این اطلاعات است. در مدل کنترل دسترسی اجباری (MAC)، با دادن برچسب امنیتی، سعی در رفع این مشکل داشته است؛ اما از آنجایی‌که هر سند بسته به بیمار یا سازمان مراقبت بهداشتی مسئول داده، سطح امنیتش مشخص می‌شود، استفاده از این مدل برای سامانه‌های پرونده الکترونیکی سلامت دشوار است؛ درضمن این مدل انعطاف‌پذیری لازم برای کاربرد در سلامت الکترونیکی را ندارد [11]. در مدل کنترل دسترسی نقش‌مبنا (RBAC) به‌دلیل ایستابودن مجوزها و ارتباط بین نقش‌ها، عملیات و اشیا، امکان تعریف و اعطای مجوزهای پویا را (که در کاربرد سلامت الکترونیکی به آن‌ها بسیار نیازمندیم) ندارد. مدل کنترل دسترسی خصوصیت‌مبنا (ABAC)، این معایب را حل کرده اما همچنان نیازی مثل وکالت دسترسی در آن برطرف نشده است. پژوهش‌گران در مدل‌های بعدی با ترکیب این مدل‌های پایه یا گسترشی بر مدل نقش‌مبنا سعی کردند یک مدل کنترل دسترسی ارائه دهند که قادر باشد نیازمندی‌های مطرح در محیط‌های سلامت الکترونیکی را برطرف سازد.

[DOI: 10.29252/jsdp.17.3.109]

۲-۱- مدل‌های کنترل دسترسی آگاه از زمینه

جرجیدیس[1] و همکارانش [16]، از ترکیب مدل RBAC و مدل کنترل دسترسی مبتنی بر تیم (TMAC)، برای رفع نیازمندی‌های زمینه‌ای استفاده کردند. مؤلفهٔ تیم همانند مؤلفهٔ نقش، واسطه‌ای است بین کاربر و زمینه که در آن کاربران و نقش‌ها می‌توانند در یک نشست، به عنصر تیم دسترسی پیدا کنند. به هر تیم براساس زمان و مکان مجوزهایی داده می‌شود و هر فردی که عضو یک تیم باشد می‌تواند به مجوزهای همان تیم دسترسی پیدا کند. در این مدل به حریم خصوصی بیمار و نیازمندی‌های آن و همچنین کنترل دسترسی به اطلاعات بیماران در شرایط اضطراری و وکالت دسترسی پرداخته نشده است.

یارمند [17][2]، با بهره‌گیری از مدل کنترل دسترسی مبتنی بر رفتار، یک معماری را طراحی کرد تا بتواند نیازمندی زمانی و مکانی را رفع و همچنین با این مدل ویژگی قابلیت همکاری بیمارستان با دیگر سازمان‌ها را ارضا کند؛ اما در این مدل نیز به نیازمندی‌های مربوط به حریم خصوصی و وکالت دسترسی توجه نشده است.

جورجیکاکیس [18][3]، با گسترش‌دادن مدلی با عنوان STEM-RBAC توانست سه نیازمندی محدودیت مکانی، زمانی و وضعیت اضطراری را بیان کند. در این معماری از مؤلفه‌هایی مانند مؤلفهٔ نظارت بر موارد اضطراری و مؤلفهٔ نظارت امنیت استفاده شده و برای هر یک از این مؤلفه‌ها الگوریتم تصمیم‌گیری به‌صورت صوری بیان شده است. در این مدل از وکالت دسترسی و نیازمندی‌های آن صحبتی نشده است.

۲-۲- مدل‌های مرتبط با نیازمندی‌ها و حریم خصوصی بیمار

مدل‌های مرتبط با نیازمندی‌های بیمار و حریم خصوصی با مؤلفه‌ای به نام هدف که درواقع اهداف دسترسی را در نظر می‌گیرد، مورد بررسی قرار می‌گیرند. در مدل P-RBAC، نی[4] و همکارانش [19] با توسعه مدل نقش‌مبنا، خانواده‌ای از مدل‌های آگاه به حریم خصوصی ارائه دادند تا بتوانند به‌طور کامل از بیان خط‌مشی‌های حریم خصوصی بسیار پیچیده پشتیبانی کنند. در این مدل مؤلفه‌های هدف، تعهد و شرایط اضافه شده است که برای تعریف مجوزهای حافظ حریم خصوصی از آن‌ها استفاده می‌شود. در مدلی دیگر یانگ [5] و همکارانش [20]، هدف را به دو شکل در مدل خود مورد استفاده قرار دادند. هدف مالک داده و هدف دسترسی که درواقع در این مدل خط‌مشی‌های حریم خصوصی این اطمینان را می‌دهند که داده‌ها فقط برای اهدافی مطابق با اهداف تعیین‌شده توسط مالک داده مورد دسترسی قرار می‌گیرند.

سیکورانزا[6] و همکارش [11]، با استفاده از مدل خصوصیت‌مبنا و اضافه‌کردن مؤلفه‌هایی، یک مدل خصوصیت‌مبنای چندسطحی با مدیریت پویای فهرست کاربران ارائه داده است. هدف مدل ارایه‌شده در این مقاله، رسیدن به بیشترین مطابقت بین آنچه خط‌مشی‌های دسترسی به ما اجازه می‌دهند تا تعریف کنیم و آنچه بیماران می‌خواهند تا تعریف شود، است. در این مدل هر بیمار سطح دسترسی مجوزهایش را برای کاربران با توجه به مؤلفهٔ زمان، شرایط و اهداف دسترسی آن کاربر تعیین می‌کند. این نویسندگان همچنین با توسعهٔ همین مدل، مدل دیگری [8] ارائه دادند که با اضافه‌کردن سطح امنیتی به اشیا یا مستندات هر بیمار و همچنین تعریف مفهوم دید[7]، به بیماران اجازه می‌دهد که برای هر کاربر یک دید تعریف کنند و به آن کاربر اجازهٔ دسترسی به بخشی از مستنداتشان را بدهند و یا دسترسی یک کاربر به یک دید را از وی سلب کنند؛ اما با وجود درنظرگرفتن نیازمندی‌های حریم خصوصی در محیط بیمارستانی در این مدل، همچنان به وکالت دسترسی و کنترل دسترسی در شرایط اضطراری در این مدل‌ها پرداخته نشده است. سئول و همکارش [21]، یک مدل کنترل دسترسی مبتنی بر ابر برای رکوردهای سلامت الکترونیکی (EHR) ارائه داده‌اند. در این مدل که مبتنی بر ویژگی است، برای حفظ حریم خصوصی از روش‌های رمزنگاری و امضای دیجیتال XML استفاده شده، اما در این روش به مسألهٔ وکالت دسترسی پرداخته نشده است. عبدالمجید [22]، یک مدل گمنام‌سازی جدید برای حفظ حریم خصوصی داده‌های پرونده‌های سلامت الکترونیکی ارائه داده است که توانایی آن برای جلوگیری از افشای هویت در برابر مهاجمان دارای دانش پیش‌زمینه نیز مناسب است؛ اما این مدل نیز مانند سایر مدل‌های این دسته مسألهٔ وکالت دسترسی و کنترل دسترسی به اطلاعات بیماران در شرایط اضطراری را که از ضروریات کنترل دسترسی در محیط‌های سلامت الکترونیکی است، پوشش نمی‌دهد.

[1] Georgiadis
[2] Yarmand
[3] Georgakakis
[4] Ni
[5] Yang
[6] Sicuranza
[7] Vicw

[DOI: 10.29252/jsdp.17.3.109]

۳-۲- مدل‌های مرتبط با سلامت الکترونیکی

گوپه[1] و همکارش [23]، مدل کنترل دسترسی مبتنی بر موقعیت برای دسترسی به داده‌های پرونده‌های الکترونیکی سلامت بیماران ارائه دادند که در آن مشکل نقض نیازمندی‌های امنیتی هنگام مواجهه با شرایط اضطراری حل شده است. درواقع در شرایط اضطراری سازوکارهای کنترل دسترسی استفاده‌شده در سلامت با رویکردی به نام شکستن شیشه[2] باعث می‌شوند که یک کاربر مخرب بتواند با استفاده از این رویکرد به امتیازات و دسترسی‌های غیر مجاز دست یافته و به امنیت پرونده‌های سلامت بیماران آسیب رساند. برای جلوگیری از این قبیل رویدادها سامانه کنترل دسترسی باید در هر لحظه حتی در موارد اضطراری، دست‌کم یک نیاز امنیتی را حفظ کند. در این روش از مدل نقش‌مبنا و مدل کنترل دسترسی اجباری استفاده شده است. در این مدل همچنان به نیازمندی‌های وکالت دسترسی به اطلاعات بیماران پرداخته نشده است. نرایانان[3] [24] نیز با استفاده از مدل کنترل دسترسی مبتنی بر وظایف (TBAC) به ارضای نیازمندی‌های زمینه‌ای، اعطای کمینه مجوزها و اعطای حق وکالت می‌پردازد و سازوکار مبتنی بر این مدل پیشنهاد می‌کند. در مدلی دیگر خن[4] و همکارش [13]، یک سامانه کنترل دسترسی مبتنی بر مدلی توسعه‌یافته از مدل نقش‌مبنای RBAC برای کاربرد سلامت الکترونیکی ارائه دادند که در آن شرایط اضطراری به‌عنوان زمینه و خصوصیت روی RBAC اضافه شده است. برای برطرف‌کردن نیازمندی وکالت نیز از چارچوب مبتنی بر مدل کنترل دسترسی اختیاری که شامل سه عملیات ساخت، انتقال و تأیید است، استفاده کرده‌اند. در این مدل با وجود درنظرگرفتن وکالت دسترسی و کنترل دسترسی به اطلاعات بیماران در شرایط اضطراری، همچنان حریم خصوصی بیمار به‌خوبی در نظر گرفته نشده است.

تمام این مدل‌های گفته‌شده در جدول (۲) در بخش ۴-۱ با هم مقایسه شده‌اند. همان‌طورکه در توضیحات مربوط به مدل‌ها گفته‌شده و همچنین با توجه به جدول مقایسهٔ این مدل‌ها، می‌توان دریافت هر کدام از این روش‌ها توانسته‌اند تنها بخشی از نیازمندی‌های مربوط به حریم خصوصی، وکالت دسترسی به اطلاعات بیماران و کنترل دسترسی را

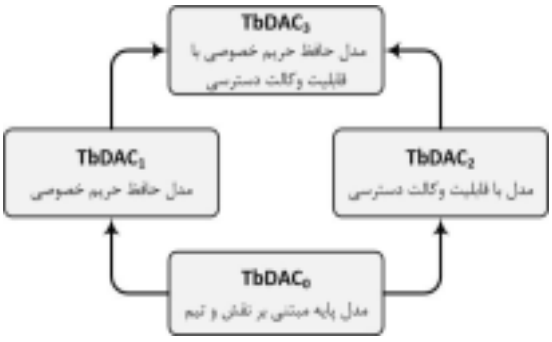
[1] Gope
[2] Break the glass
[3] Narayanan
[4] Khan

هنگامی که بیمار در شرایط اضطراری است، برطرف کند و مدلی که بتواند تمامی این نیازمندی‌ها را به‌صورت هم‌زمان و عملیاتی برطرف سازد، وجود ندارد. در همین راستا در این مقاله مدلی ارائه شده است که بتواند ضمن برطرف‌کردن کلیهٔ نیازمندی‌های کنترل دسترسی ضروری، امکان پیاده‌سازی یک سازوکار عملی، مبتنی بر مدل ارایه‌شده را نیز فراهم کند.

۳- مدل کنترل دسترسی پیشنهادی

در این مقاله برای برطرف‌کردن مسألهٔ دسترسی به پروندهٔ بیمار توسط پزشک براساس موقعیت فیزیکی پزشک، مسألهٔ تشخیص شرایط اضطراری (اورژانس) و اعطای دسترسی موقت به پزشک حاضر و همچنین مسألهٔ اعطای وکالت دسترسی به همه یا بخشی از حقوق دسترسی یک عامل بیمارستانی به عامل بیمارستانی دیگر، یک خانواده مدل به نام TbDAC[5] ارائه شده که در هر مرحله با اضافه‌شدن مؤلفه‌هایی تکمیل شده است. شکل (۱) خانواده مدل‌های پیشنهادی TbDAC را به‌همراه ارتباطات بین آنها نمایش می‌دهد.

در هر کدام از مدل‌های ارائه‌شده ابتدا فرآیند درمانی که در بیمارستان طی می‌شود، توضیح داده می‌شود و سپس به تعریف مدل رابطه‌ای آن و موجودیت‌هایی که در مدل استفاده‌شده، پرداخته می‌شود. در ادامه، فرآیند کنترل دسترسی و قواعد دسترسی تعریف‌شده در آن مدل در شرایط مختلف بیان و در آخر مدل با درنظرگرفتن شرایط اضطراری تکمیل می‌شود.



(شکل-۱): خانواده مدل‌های کنترل دسترسی پیشنهادی TbDAC
(Figure-1): Proposed TbDAC access control model family

[5] Team-based Delegation Access Control

[DOI: 10.29252/jsdp.17.3.109]

۱-۳- مدل هستهٔ $TbDAC_0$

مدل هسته شامل مدلی ساده برای کنترل دسترسی در سلامت الکترونیکی است که در آن رویه‌های معمول بیمارستانی مدنظر قرار گرفته شده است. در این مدل امکاناتی همچون تعیین ترجیحات بیمار در دسترسی به پرونده پزشکی وی و همچنین وکالت دسترسی لحاظ نشده است. در مدل هسته از مفاهیم تیم و نقش در مدیریت دسترسی‌ها بهره گرفته شده است.

۱-۱-۳- فرآیندهای درمانی

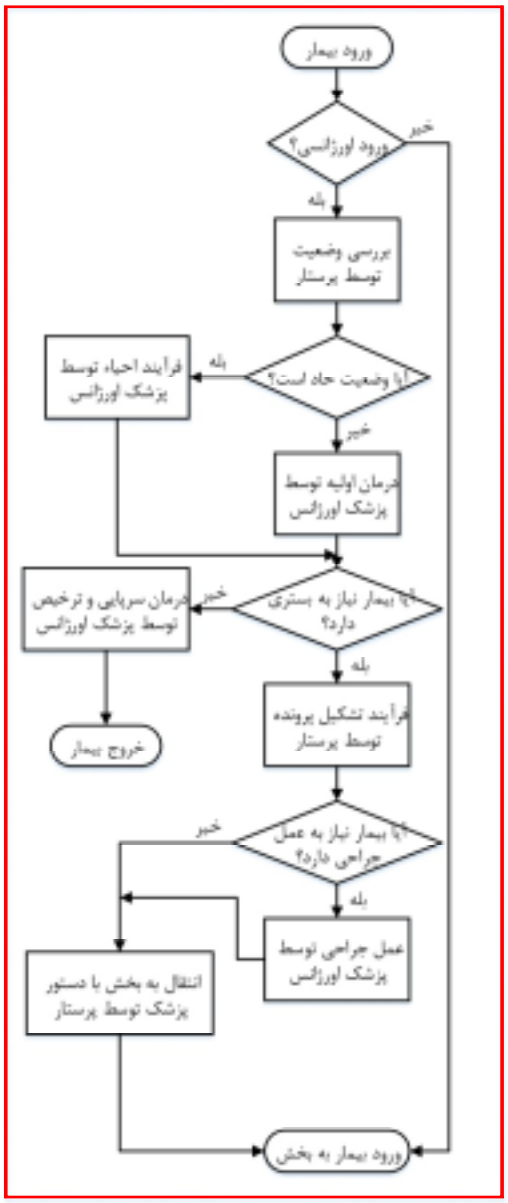
با توجه به تأثیر فرآیندهای درمانی در تبیین فرآیندهای مدیریت کنترل دسترسی لازم است ابتدا این فرآیندها تشریح شوند.

فرآیندهای درمانی با ورود بیماران به بیمارستان آغاز می‌شود (شکل ۲). ورود بیماران به بیمارستان به دو شکل صورت می‌گیرد:

- بیمارانی که از قبل به درمانگاه مراجعه کرده و با هماهنگی پزشک بیمارستان و با دریافت درخواست بستری و انجام مشاوره‌های لازم وقت بستری گرفته و در روز تعیین‌شده به پذیرش مراجعه و تشکیل پرونده می‌دهند.
- بیماران اورژانسی که به‌صورت اضطراری وارد بخش اورژانس شده و به‌طورموقت در این بخش بستری و بعد از خالی‌شدن تخت در بخش مربوطه به آن بخش انتقال داده می‌شوند.

بیمارانی که از طریق اورژانس وارد بیمارستان می‌شوند ابتدا توسط سرپرستار در یکی از تخت‌های خالی بستری می‌شوند (هر تخت به RFID تجهیز شده) و از آنجایی‌که هر پرستار مسئول رسیدگی به بیماران مجموعه‌ای از تخت‌های مشخص است، پس از بستری‌شدن بیمار، پرستار مسئول آن تخت بررسی می‌کند که بیمار در چه وضعیتی قرار دارد. اگر وضعیت بیمار حاد باشد، فرآیند احیا توسط پزشک اورژانس برای او انجام، در غیر این صورت پس از درمان اولیهٔ بیمار، بررسی می‌شود که بیمار نیاز به بستری دارد یا نه. اگر نیاز به بستری نباشد که به‌صورت سرپایی توسط پزشک اورژانس درمان انجام و در غیر این صورت فرآیند تشکیل پرونده برای بیمار اجرا می‌شود.

در فرآیند تشکیل پرونده کافی است پرونده سلامت بیمار که از قبل وجود دارد، به‌روز شود؛ یعنی روند درمان او از زمان ورود تا آن لحظه شامل آزمایش‌ها و تجویزها به پرونده اضافه می‌شود؛ پس از آن اگر بیمار احتیاج به عمل جراحی داشته باشد، پس از گرفتن رضایت، جراحی توسط پزشک انجام می‌شود؛ اگر نیاز به عمل نیز وجود نداشته باشد، بیمار به بخش مربوطه منتقل شده و در آنجا بستری می‌شود.



(شکل-۲): روند ورود و درمان بیماران در اورژانس
(Figure-2): Patient entrance and treatment process in hospital Emergency room

فرآیند انتقال بیمار از اورژانس به بخش (شکل ۳) نیز به‌این‌ترتیب است که پزشک اورژانس دستور انتقال را صادر و پرستار مسئول شیفت با بررسی پرونده و هماهنگی با واحد

[DOI: 10.29252/jsdp.17.3.109]

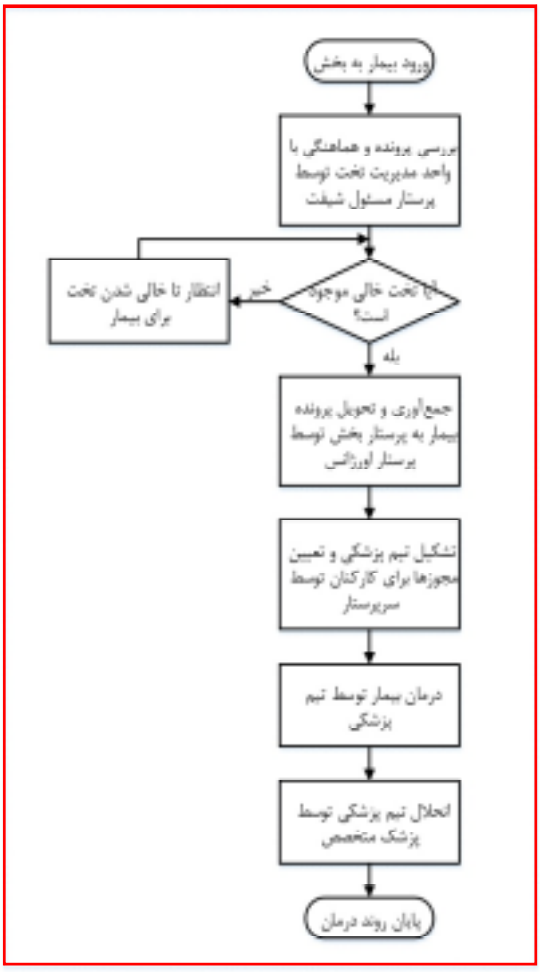
مدیریت تخت جهت گرفتن تخت خالی برای انتقال بیمار بررسی می‌کند که آیا تخت خالی در بخش موردنظر موجود است یا خیر. اگر وجود نداشته باشد که بیمار تا خالی‌شدن تخت در اورژانس می‌ماند؛ اما اگر تخت خالی وجود داشت، پرستار پرونده بیمار را همراه بیمار به رزیدنت یا پرستار مسئول بیمار در بخش مربوطه تحویل می‌دهد. گفتنی است تمامی این فرآیندها تحت نظارت و دستور سرپرستار انجام می‌گیرد.

در بخش مربوطه سرپرستار برای بیمار یک تیم پزشکی تشکیل می‌دهد (در این بخش هر بیمار به RFID مجهز شده است) و مجوزهای لازم را برای هرکدام از افراد تیم پزشکی تعیین می‌کند. باید توجه شود نقشی که هر عامل بیمارستانی در تیم پزشکی عهده‌دار می‌شود زیرمجموعه‌ای از نقش‌های مجاز او باشد.

برای بیمارانی که از قبل به درمانگاه مراجعه کرده و با هماهنگی با پزشک خود وقت بستری می‌گیرند، در روز تعیین‌شده، به پذیرش مراجعه و پس از به‌روزرسانی پرونده الکترونیکی سلامت در بخش مربوطه بستری می‌شوند و تیم پزشکی برای آن‌ها تشکیل می‌شود.

در روند درمان بیماران هرکدام از عوامل بیمارستانی وظایفی را بر عهده دارند که با توجه به نقش‌های اصلی‌شان عهده‌دار این وظایف می‌شوند.

- سرپرستار وظیفه دارد ترجیحات خصوصی بیماران را ثبت کند، در بخش اصلی با بررسی پروندهٔ بیمار مکان مناسب را تعیین کند و همچنین تیم پزشکی را برای بیماران تشکیل دهد.
- پزشک اورژانس وظیفهٔ درمان اولیهٔ بیمار، عمل جراحی اورژانسی یا احیای بیمار در اورژانس را بر عهده دارد. همچنین دستور انتقال بیمار از اورژانس به بخش مربوطه توسط پزشک اورژانس صورت می‌گیرد.
- پزشک بخش (متخصص) وظیفهٔ درمان بیمار در تیم پزشکی و انحلال تیم را برعهده دارد.
- پرستار، دستیار و کارورز در اورژانس وظیفهٔ بررسی وضعیت اولیهٔ بیمار را برعهده دارند. قبل از تحویل بیمار به سرپرستار در بخش اصلی، پرونده بیمار را به‌روزرسانی می‌کنند. همچنین در بخش اصلی با توجه به تیم پزشکی که در آن عضو هستند، به اطلاعات بیمار دسترسی دارند.



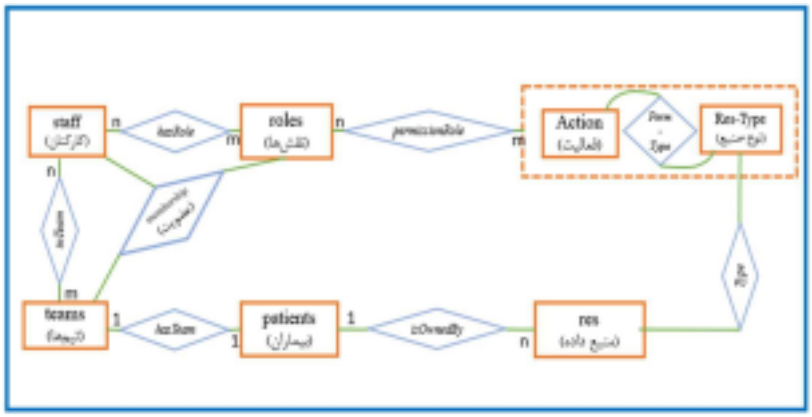
(شکل-۳): فرآیند درمان بیمار در بخش‌های بیمارستانی

(Figure-3): Patient treatment process in hospital departments

۲-۱-۳- تعریف مدل داده‌ای $TbDAC_0$

در مدل هسته ($TbDAC_0$) که در آن از مفاهیم مطرح در دو مدل کنترل دسترسی مبتنی بر نقش (RBAC) و مدل مبتنی بر تیم (TMAC) استفاده شده، هدف، کنترل دسترسی در محیط بیمارستان با توجه به الکترونیکی‌شدن پروندهٔ بیماران است. در این مدل، که در شکل (۴) نشان داده شده است، موجودیت‌ها شامل بیماران، کارکنان یا عوامل بیمارستانی، نقش‌ها، منابع داده، فعالیت‌ها، نوع منبع‌ها و تیم‌ها هستند و محدودیت‌های زمینه‌ای مانند زمان و مکان بر روی دسترسی تأثیر می‌گذارند. بر اساس توصیف کلی ارائه‌شده از شرایط حاکم در محیط بیمارستان و دسترسی‌های مطرح در آن، تعریف صوری موجودیت‌ها و روابط بین آنها در مدل کنترل دسترسی ارایه‌شده، در ادامه آمده است.

[DOI: 10.29252/jsdp.17.3.109]



(شکل-۴): مدل داده‌ای کنترل دسترسی پایه در سلامت الکترونیکی

(Figure-4): Basic access control data model for e-health

(۱) بیماران: کاربرانی هستند که وارد بیمارستان شده و از خدمات آن استفاده می‌کنند. اگر مجموعهٔ همه بیماران با patients نمایش داده شوند و مسند معادل مورد استفاده Patient نام‌گذاری شود، رابطهٔ این دو نماد به‌صورت صوری به‌شکل زیر بیان می‌شود:

- $Patient(x) = True \leftrightarrow x \in patients$

(۲) کارکنان (عوامل بیمارستانی): کاربرانی هستند که در بیمارستان کار می‌کنند و می‌توانند نقش‌های مختلفی داشته باشند. اگر مجموعهٔ همه کارکنان با staff نمایش داده شود و مسند معادل مورد استفاده Staff نام‌گذاری شود، رابطهٔ این دو نماد به‌صورت صوری به‌شکل زیر بیان می‌شود:

- $Staff(x) = True \leftrightarrow x \in staff$

(۳) نقش‌ها: نقش‌هایی که در بیمارستان وجود دارد و به کارکنان منتسب می‌شود. به‌طورکلی می‌توان نقش‌ها را در این مدل به دو دستهٔ مجزا تقسیم کرد: نقش‌های مدیریتی و نقش‌های بیمارستانی. نقش‌های مدیریتی به‌طور ثابت شامل دو نقشِ مدیر ارشد امنیتی (SU) و مدیر امنیتی بخش (DSO) است؛ امّا نقش‌های بیمارستانی می‌توانند در هر محیط تعریف شوند و مجموعه این نقش‌ها به‌طورعمومی در بیمارستان‌ها دست‌کم شامل رییس بیمارستان، پزشک متخصص، سرپرستار، پرستار، دستیار و کارورز است. هر نقش با انتساب به مجموعه‌ای از نوع‌مجوزها تعریف می‌شود. باید در نظر داشت که هر عامل بیمارستانی اجازه دارد نقش‌های خاصی را با توجه به مدارک و گواهی‌های مورد تأیید وزارت بهداشت، درمان و آموزش پزشکی (مانند پزشکی یا پرستاری) عهده‌دار شود. در این مدل، مجموعهٔ نقش‌های قابل انتساب به کارکنان roles نامیده شده و مسند معادل آن نیز Role نام‌گذاری شده است.

(۴) تیم‌ها: برای هر بیمار با توجه به نوع بیماری او یک تیم پزشکی تعیین می‌شود که این تیم از تعدادی پزشک با تخصص‌های مختلف، پرستار و کارورز تشکیل شده است. مجموعهٔ تیم‌های تشکیل‌شده از کارکنان با teams نمایش داده شده و مسند معادل مورد استفاده نیز Team نام‌گذاری شده است.

(۵) منبع داده: پروندهٔ هر بیمار از داده‌های مختلفی تشکیل شده که دسترسی به هرکدام از این داده‌ها با توجه به ماهیتشان متفاوت است. هرکدام از این داده‌ها ممکن است به سه صورت دسته‌بندی شود:

- اطلاعاتی که یا ثابت هستند یا بازه تغییر آن‌ها بسیار طولانی است مانند نام یا سن بیمار.
- اطلاعاتی که در بازهٔ کوتاه‌تری تغییر می‌کنند. اطلاعات درمانی شامل آزمایش‌های انجام‌شده و تجویزها در این دسته جای می‌گیرند.
- اطلاعاتی که در بازهٔ کوتاهی از زمان تغییر می‌کند و شامل همان اطلاعاتی است که از حس‌گرها به‌صورت مداوم در حال اندازه‌گیری است.

در این مدل، مجموعه‌ی منابع دادهٔ قابل انتساب به بیماران res نامیده شده و مسند معادل آن نیز Res نام‌گذاری شده است.

(۶) نوع‌منبع: هرکدام از منابع داده دارای نوعی است که این نوع منابع شامل اطلاعات ورودی و خروجی بیمار (اطلاعات هویتی، اطلاعات حس‌گرها و اطلاعات بیمه درمانی)، اطلاعات تشخیص، اطلاعات اولیه پزشکی، برگهٔ مشورت با دیگر پزشکان، اطلاعات علائم حیاتی، اطلاعات نتایج آزمایش‌ها، اطلاعات شرح‌حال بیمار، اطلاعات جراحی، ارزیابی اولیه بیمار

[DOI: 10.29252/jsdp.17.3.109]

(اطلاعات خاص در زمان نخستین بازدید)، گزارش پرستار و داروهای تجویزشده است. مجموعهٔ نوع‌منبع‌های قابل انتساب به منابع داده‌ای با res-type **مشخص شده** و مسند معادل آن نیز Res-type نام‌گذاری شده است.

(۷) فعالیت‌ها: اعمالی هستند که بر روی نوع منبع‌ها می‌توانند اجرا شوند؛ مانند خواندن و نوشتن. در این مدل مجموعهٔ اعمال قابل اجرا بر روی نوع منابع با actions نمایش داده شده و مسند معادل ان Action نامیده شده است.

(۸) نوع مجوز: هر نوع‌مجوز به‌صورت مجموعه‌ای از اعمال بر روی نوع منابع تعریف می‌شود؛ لذا مجموعه کل نوع‌مجوزهای ممکن در این مدل (که Perm-Type نامیده شده) به‌صورت زیر تعریف می‌شود. توجه کنید که 2^X نماد مجموعه توانی X است:

- $\text{Perm-Type} = 2^{(\text{actions} \times \text{res-Type})}$

علاوه‌بر مفاهیم یا موجودیت‌های بالا، روابطی در این مدل تعریف شده است که ارتباط بین موجودیت‌های مدل با یکدیگر را بیان می‌کند. این روابط در ادامه تعریف و به شکل صوری توصیف شده‌اند.

۱. رابطهٔ بین کارکنان و نقش‌ها یک رابطهٔ چند به چند است. یعنی هر یک از کارکنان ممکن است، نقش‌های مختلفی داشته باشند و هر نقشی به کارکنان مختلف منتسب شود. این رابطه hasRole نامیده می‌شود. تابع assignedRole هم مجموعه نقش‌های منتسب به هر یک از کارکنان بیمارستانی را طبق رابطه hasRole مشخص می‌کند:

$$\text{hasRole} \subseteq \text{staff} \times \text{roles} \quad (۱)$$

$$\text{HasRole}(s, r) = \text{True} \leftrightarrow (s, r) \in \text{hasRole}$$

$$\text{assignedRole} : \text{staff} \rightarrow 2^{\text{roles}}$$

$$\text{assignedRole}(s) = \{r \in \text{roles} \mid (s, r) \in \text{hasRole}\}$$

۲. رابطهٔ بین تیم‌های پزشکی و کارکنان (با نام inTeam) یک رابطهٔ چند به چند است. یعنی هر یک از کارکنان ممکن است، عضو چند تیم پزشکی باشند و هر تیم پزشکی مربوط به هر بیمار نیز از تعدادی عامل بیمارستانی تشکیل شده باشد.

$$\text{inTeam} \subseteq \text{staff} \times \text{teams}$$

$$\text{InTeam}(s, tm) = \text{True} \leftrightarrow (s, tm) \in \text{inTeam} \quad (۲)$$

$$\text{assignedTeam} : \text{staff} \rightarrow 2^{\text{teams}}$$

$$\text{assignedTeam}(s) = \{tm \in \text{teams} \mid (s, tm) \in \text{inTeam}\}$$

۳. رابطهٔ بین تیم و بیمار یک رابطهٔ یک‌به‌یک است. درواقع به هر بیمار (با توجه به حضور در بخش و تشخیص سرپرستار) یک تیم پزشکی اختصاص داده می‌شود. تابع hasTeam، تیم پزشکی منتسب به هر بیمار را مشخص می‌نماید.

$$\text{hasTeam}: \text{patients} \rightarrow \text{teams}$$

$$\text{HasTeam}(p, tm) = \text{True} \leftrightarrow \text{hasTeam}(p) = tm \quad (۳)$$

۴. هر منبع داده، متعلق به یک بیمار است.

$$\text{isOwnedBy}: \text{res} \rightarrow \text{patients}$$

$$\text{IsOwnedBy}(d, p) = \text{True} \leftrightarrow (d, p) \in \text{isOwnedBy} \quad (۴)$$

۵. رابطهٔ permissionRole یک رابطهٔ چندبه‌چند است که نوع‌مجوزهای (Perm-Type) منتسب به نقش‌ها را مشخص می‌کند. توجه کنید که مفهوم **نوع‌مجوز** با مفهوم **مجوز** که در مدل‌های نقش‌مبنا تعریف شده، متفاوت است. درواقع نوع‌مجوز انواع اعمال ممکن بر روی انواع منابع (یا انواع اشیا) را توصیف می‌کند؛ در صورتی‌که مجوز، مجازبودن عمل بر روی خود منابع (اشیا) را مشخص می‌کند. در این مدل درواقع نوع‌مجوزها (و نه خود مجوزها) به نقش‌ها منتسب می‌شوند؛ سپس بر اساس نوع‌مجوزها و تیمی که فرد در ان عضویت دارد، مجوزهای روی منابع استنتاج می‌شوند:

$$\text{PermissionRole} \subseteq \text{Perm-Type} \times \text{roles}$$

$$\text{assignedPermission} : \text{roles} \rightarrow 2^{\text{Perm-Types}}$$

$$\text{assignedPermission}(r) = \{pt \in \text{Perm-Type} \mid (pt, r) \in \text{PermissionRole}\}$$

$$\text{AssignedPermission}(r, a, t) = \text{True} \leftrightarrow (a, t) \in \text{assignedPermission}(r) \quad (۵)$$

۶. رابطهٔ بین هر نوع‌منبع با منابع داده یک رابطه یک به چند است. یعنی هر منبع داده به یک نوع-منبع منتسب می‌شود و هر نوع-منبع شامل چندین منبع داده است.

$$\text{type}: \text{res} \rightarrow \text{res-Type}$$

$$\text{Type}(d, t) = \text{True} \leftrightarrow \text{type}(d) = t \quad (۶)$$

۷. رابطهٔ membership یک رابطه بین سه مؤلفهٔ کارکنان، تیم‌ها و نقش‌ها است که مشخص می‌کند هر عامل بیمارستانی در هر تیم با چه نقشی عضویت دارد:

$$\text{membership} \subseteq \text{staff} \times \text{team} \times \text{roles}$$

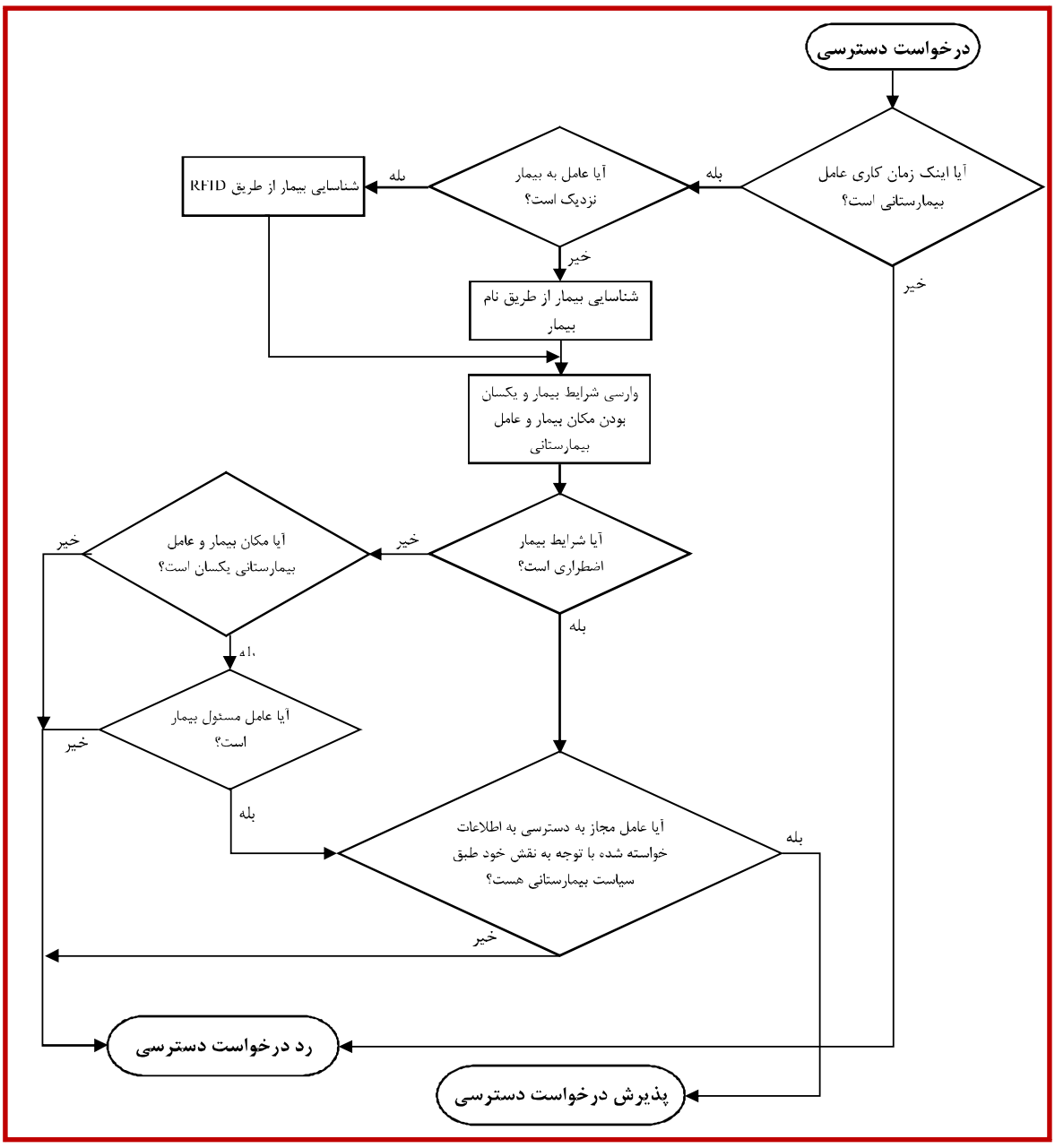
$$\text{membership}(s, tm, r) \rightarrow \text{HasRole}(s, r) \wedge \text{InTeam}(s, tm) \quad (۷)$$

$$\text{Membership}(s, tm, r) = \text{True} \leftrightarrow (s, tm, r) \in \text{membership}$$

[DOI: 10.29252/jsdp.17.3.109]

۸. تابع isMemberOfTeam بیمارانی را که یک عامل بیمارستانی در تیم پزشکی آن‌ها قرار دارد، مشخص می‌کند:

$$\begin{aligned} &\text{isMemberOfTeam}(s) = \{p \in \text{patients} \mid \\ &\qquad (s, \text{hasTeam}(p)) \in \text{inTeam}\} \\ &\text{IsMemberOfTeam}(s, p) = \text{True} \\ &\qquad \leftrightarrow (s, p) \in \text{isMemberOfTeam} \end{aligned} \qquad (۸)$$



(شکل-۵): فرآیند کنترل دسترسی

(Figure-5): Access control process

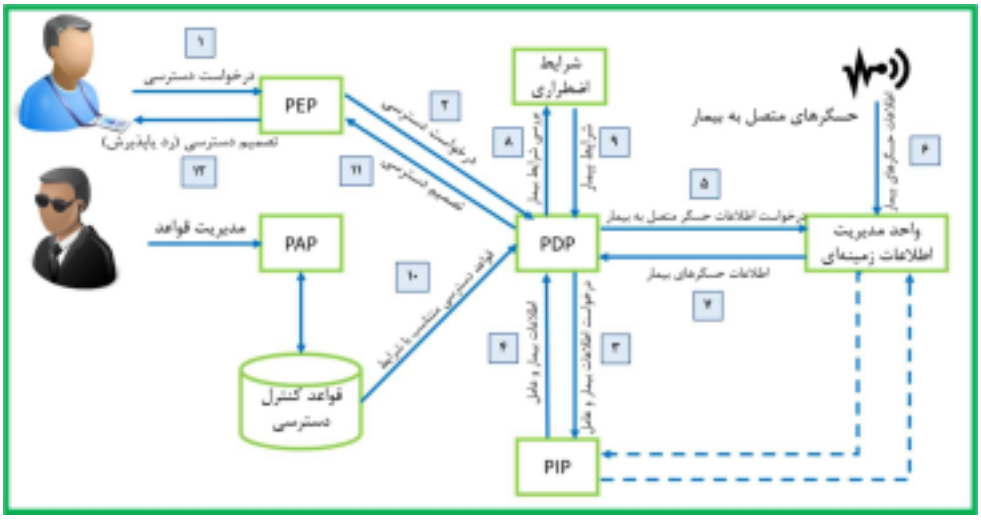
۳-۱-۳- فرآیند کنترل دسترسی

در این مدل فرض بر این است که بیمار در بیمارستان بستری است. با این فرض زمانی که هر عامل بیمارستانی درخواست دسترسی به اطلاعات بیمار را داشته باشد، ابتدا بررسی می‌شود که اینک زمان کاری عامل بیمارستانی هست یا نه؟ در صورت مثبت‌بودن نتیجه، بررسی می‌شود این عامل نزدیک بیمار است (شناسایی با خواندن RFID متصل به بیمار یا تخت بیمار) یا به‌صورت از راه دور درخواست

[DOI: 10.29252/jsdp.17.3.109]

دسترسی به اطلاعات بیمار را با استفاده از شناسه (یا نام) بیمار دارد؛ سپس مراحل زیر (همان‌طور که در شکل (۵) نمایش داده شده) طی می‌شود.

- اگر عامل دور از بیمار بخواهد به اطلاعات او دسترسی داشته باشد:
  - ابتدا مکان بیمار بررسی می‌شود که آیا در اورژانس است یا در بخش. همچنین بررسی می‌شود که آیا شرایط اضطراری است یا نه؛ سپس با توجه به یکسان‌بودن مکان عامل بیمارستانی (مکانی که عامل خدمت می‌کند) و مکان بیمار (برای مثال هر دو در اورژانس باشند یا در بخش) و همچنین بررسی وضعیت، درخواست وارسی می‌شود.
  - پس از بررسی یکسان‌بودن مکان‌ها، (۱) اگر هر دو در اورژانس بودند و عامل بیمارستانی مسئول همان تختی که بیمار درآن بستری است، باشد، بررسی می‌شود که آیا شرایط زمانی و مکانی مطابق با شرایط تعیین‌شده هست یا خیر. (۲) اگر هر دو در بخش باشند، باید بررسی شود عامل بیمارستانی عضو تیم پزشکی آن بیمار است یا نه. پس از آن شرایط زمینه‌ای مانند حالت اورژانس بررسی می‌شود.
  - اگر طبق قواعد کنترل دسترسی تعریف‌شده در پایگاه داده، همهٔ شرایط برقرار بود، دسترسی داده می‌شود در غیر این‌صورت دسترسی رد می‌شود.
- اگر عامل بیمارستانی در نزدیکی بیمار درخواست دسترسی به اطلاعات او را داشته باشد:
  - اگر در بخش اورژانس باشد با استفاده از RFID reader ای که در دستگاه عامل بیمارستانی قرار دارد RFID متصل به تخت بیمار خوانده و بررسی می‌شود جزء تخت‌هایی که عامل بیمارستانی مسئولیت آن را دارد هست یا نه؟ (درواقع با استفاده از RFID متصل به بیمار بررسی می‌شود عامل بیمارستانی جزو تیم بیمار هست یا نه).
  - شرایط اضطراری و شرایط مکانی و زمانی گفته‌شده در حالت قبل بررسی می‌شود.
  - اگر تمام این موارد با توجه به پایگاه قواعد کنترل دسترسی سازگار بود، دسترسی داده می‌شود و اطلاعات بیمار در دستگاه عامل بیمارستانی به نمایش گذاشته می‌شود؛ در غیر این‌صورت دسترسی رد می‌شود.



(شکل-۶): چارچوب کنترل دسترسی

(Figure-6): Access control framework

۴-۱-۳- چارچوب کنترل دسترسی

شکل (۶)، چارچوب کنترل دسترسی استفاده‌شده را در مدل $TbDAC_0$ نشان می‌دهد. در این مدل موجودیت‌هایی جهت تأمین کنترل دسترسی در سلامت الکترونیکی حضور دارند که عبارتند از:

(۱) واحد مدیریت خط‌مشی (PAP[1])، که واسطی را برای کارکنان جهت توصیف قواعد و خط‌مشی‌های امنیتی فراهم می‌کند. (۲) واحد تصمیم‌گیری (PDP[2])، که به تصمیم‌گیری تصمیم‌گیری درخصوص درخواست‌های دسترسی دریافتی از عوامل بیمارستانی براساس اطلاعات ثبت‌شده در پایگاه

[1] Policy Administrator Point
[2] Policy Decision Point

[DOI: 10.29252/jsdp.17.3.109]

دانش امنیتی می‌پردازد. (۳) واحد اعمال خط‌مشی (PEP[1])، که وظیفهٔ دریافت درخواست‌های دسترسی از عوامل بیمارستانی و انجام کنترل دسترسی را به‌کمک واحد PDP بر عهده دارد. (۴) واحد اطلاعات (PIP[2])، که وظیفهٔ نگهداری نگهداری اطلاعات عامل بیمارستانی درخواست‌دهنده و بیمار را دارد. (۵) واحد مدیریت اطلاعات زمینه‌ای، که وظیفهٔ جمع‌آوری اطلاعات زمینه‌ای مانند مکان عامل بیمارستانی و بیمار، اطلاعات مربوط به حس‌گرهای متصل به بیمار و RFID متصل به بیمار یا تخت بیمار را برعهده دارد. (۶) واحد بررسی شرایط اضطراری، که وظیفهٔ تعیین شرایط اضطراری بیمار را بر اساس پارامترهای حیاتی وی برعهده دارد. در شکل (۶)، روند کنترل دسترسی از زمان درخواست کاربر تا پذیرش یا رد درخواست به‌ترتیب اجرا شماره‌گذاری شده است.

۵-۱-۳- قواعد دسترسی در شرایط عادی

یکی از واحدهای موجود در چارچوب کنترل دسترسی، واحد قواعد کنترل دسترسی است که با توجه به خط‌مشی‌های بیمارستان و مدل‌های کنترل دسترسی توسط مدیریت قواعد تدوین می‌شود. هنگامی که درخواست دسترسی به اطلاعات بیمار توسط یک عامل بیمارستانی داده می‌شود، با استفاده از همین قواعد، پذیرش یا رد درخواست بررسی می‌شود.

قواعد کنترل دسترسی را می‌توان در دو وضعیت مختلف در نظرگرفت: **وضعیت عادی** و **وضعیت اضطراری (اورژانس)**. هر کدام از این شرایط ممکن است در قسمت اورژانس یا بخش‌های مختلف بیمارستان اتفاق بیافتد (شکل ۷) که در ادامه به بیان قواعد دسترسی در هر کدام از این موقعیت‌ها پرداخته می‌شود.

(شکل-۷): انواع قواعد دسترسی

(Figure-7): Access control rules categories

[1] Policy Enforcement Point
[2] Policy Information Point

برای بیان دقیق‌تر قواعد کنترل دسترسی باید ابتدا تعیین کرد حقایق[3] یا اطلاعات پایه‌ای که در این مدل وجود دارد کدامند و چگونه ثبت می‌شوند. حقایق درواقع اطلاعاتی هستند که توسط عوامل بیمارستانی یا حس‌گرهای متصل به بیمار ثبت می‌شوند.

- اطلاعاتی که توسط سرپرستار ثبت می‌شود:

- مکان بستری‌شدن بیمار:

AssignedLocationP (P, PL)

مکان بستری‌شدن بیمار P با استفاده از مسند AsssignedLocationP به‌صورت بالا توصیف و ثبت می‌شود. در این مسند PL با زوج $(L_p, rfid)$ نمایش داده می‌شود که $L_p \in L$ مکان بیمار را نشان می‌دهد، یعنی بخش اورژانس یا هرکدام از بخش‌های اصلی دیگر و $rfid \in rfids$، برچسب متصل به بیمار (در بخش اصلی) یا تخت بیمار (در بخش اورژانس) را نمایش می‌دهد.

L={اورژانس، پیوند مغز استخوان، پیوند کلیه، پزشکی هسته‌ای، جراحی مغز و اعصاب، جراحی قلب و پیوند قلب، اطفال و ...}

rfids = مجموعه برچسب‌های شناسایی که افراد یا تخت‌ها به آن مجهز می‌شوند.

$PL \in L \times rfids$

- مکان تحت نظر (مسئولیت) عوامل بیمارستانی:

AssignedLocationS (S, SL)

در این مسند S عامل بیمارستانی و SL با زوج (L_s, rfs) نمایش داده می‌شود که $L_s \in L$ مکان فعالیت عامل بیمارستانی را نشان می‌دهد؛ یعنی بخش اورژانس یا هرکدام از بخش‌های اصلی دیگر و $rfs \subseteq rfids$، مجموعه برچسب‌های RFID متصل‌شده به تخت بیماران (در بخش اورژانس) و خود بیماران (در بخش‌های اصلی) را که عامل بیمارستانی مسئول رسیدگی به آن‌ها است، نمایش می‌دهد:

$SL \in L \times 2^{rfids}$

- عضویت بیمار P و عامل بیمارستانی S در یک تیم:

IsMemberOfTeam (S, P)

- زمان کاری عوامل بیمارستان در بازه زمانی:

TimeTable (S, t_1, t_2)

- برچسب RFID ای که به هر بیمار مانند P نسبت داده می‌شود، دو حالت دارد؛ یا متصل به تخت است (در بخش اورژانس) که با بستری‌شدن بیمار در آن تخت به او منتسب می‌شود، یا متصل به خود بیمار است (در بخش‌های اصلی).

AssignedRFID (P, rfid)

[3] facts

[DOI: 10.29252/jsdp.17.3.109]

- اطلاعات قابل ثبت توسط حس‌گرها:

-اطلاعات حیاتی بدن بیمار:

C_i (P, V)

که در آن مسند C_i نوعی از اطلاعات مانند دمای بدن مربوط به بیمار، ضربان قلب و فشار خون او است و V مقدار آن برای بیمار P را نشان می‌دهد. به‌طور مثال Pressure(Ahmadi, 14) این اطلاع را می‌رساند که بیمار احمدی فشار خون ۱۴ را دارد.

-برچسب RFID که توسط دستگاه یک عامل بیمارستانی مانند S خوانده می‌شود:

RFID (rfid, S)

که در آن rfid، مقدار برچسب خوانده‌شده به‌وسیلهٔ RFID reader مربوط به عامل بیمارستانی S است.

علاوه‌بر حقایق و اطلاعاتی که ثبت می‌شود، اطلاعاتی نیز از طریق این حقایق استنتاج می‌شود که در ادامه به تعریف آنها می‌پردازیم:

- مسند InSubset مشخص می‌کند که آیا یک برچسب rfid مربوط به یک بیمار در یک بخش، جزو برچسب‌های تحت مسئولیت یک عامل بیمارستانی هست یا نه:

$SL=(L_s, rfs) \wedge PL=(L_p, rfid) \rightarrow$

$(InSubset(PL, SL) = True \leftrightarrow (L_p=L_s) \wedge (rfid \in rfs))$ (۹)

قواعد درشرایط عادی در دو حالت قابل بررسی است:

- در بخش اورژانس، دسترسی هر عامل بیمارستانی (پرستاران و پزشک اورژانس) به اطلاعات، از قبل تعیین شده است؛ به این شکل که هر عامل مسئول مجموعه‌ای از تخت‌ها است که بیماران با بستری‌شدن روی هرتخت، تحت مراقبت و درمان مسئول آن تخت قرار می‌گیرند.
- در بخش‌های اصلی، دسترسی با عضویت در تیم‌های پزشکی مشخص می‌شود. به این شکل که هر عامل بیمارستانی که عضو تیم پزشکی مربوط به یک بیمار شود با توجه به نقش خود در آن تیم در زمان مشخص می‌تواند به اطلاعات بیمار دسترسی داشته باشد.

به‌طور کلی در جدول (۱) تمام مسندهای استفاده‌شده در قواعد دسترسی آورده شده و در ادامه توصیف قواعد دسترسی در بخش‌های مختلف ارایه شده است.

گفتنی است که در توصیف قواعد دسترسی در این مقاله، از قاعده‌های به فرم هُرن بدون تابع[1] استفاده شده است. توجه کنید که در فرم هُرن، به‌طور ضمنی سور عمومی وجود دارد، یعنی به طور مثال قاعده $\forall x,\ p(x) \wedge q(x) \rightarrow r(x)$ در فرم هُرن درواقع معادل $\forall x,\ p(x) \wedge q(x) \rightarrow r(x)$ در منطق مرتبه نخست است. مسأله استنتاج در فرم هُرنِ بدون تابع از منطق مرتبه نخست، تصمیم‌پذیر است و لذا فرآیند استنتاج مبتنی بر این قواعد در مدل کنترل دسترسی پیشنهادی نیز تصمیم‌پذیر است.

❖ **تعریف قاعدهٔ دسترسی در بخش اورژانس:**

✓ اگر بیمار روی تختی بستری شده باشد که RFID متصل به آن تخت جزء مجموعه RFID هایی باشد که پرستار (یا عامل بیمارستانی) مسئول درمان و مراقبت از آن‌هاست، بیمار به آن پرستار (یا عامل بیمارستانی) منتسب می‌شود.

$Patient(p) \wedge Staff(s) \wedge AssignedLocationP(p, PL) \wedge AssignedLocationS(s, SL) \wedge InSubset(PL, SL) \rightarrow Assign(p, s)$ (۱۰)

✓ اگر عامل بیمارستانی مسئول یک بیمار باشد، با توجه به نقشی که عامل بیمارستانی دارد، دسترسی به بخش‌های مختلف از اطلاعات بیمار به او داده می‌شود.

$Assign(p, s) \wedge isOwnedBy(res, p) \wedge Type(res, res\text{-}Type) \wedge hasRole(s, r) \wedge CurrentTime(t) \wedge TimeTask(s, t_1, t_2) \wedge (t_1 \le t \le t_2) \wedge AssignedPermission(r, a, res\text{-}Type) \rightarrow CanAccess(s, a, res)$ (۱۱)

❖ **تعریف قاعدهٔ دسترسی در بخش‌های اصلی:**

✓ اگر عامل بیمارستانی در تیم پزشکی یک بیمار حضور داشته باشد، آنگاه عامل بیمارستانی با توجه به نقشی که در آن تیم دارد به اطلاعات بیمار دسترسی خواهد داشت.

$HasTeam(p, tm) \wedge Membership(s, tm, r) \wedge CurrentTime(t) \wedge TimeTask(s, t_1, t_2) \wedge (t_1 \le t \le t_2) \wedge IsOwnedBy(res, p) \wedge Type(res, res\text{-}Type) \wedge AssignedPermission(r, a, res\text{-}Type) \rightarrow CanAccess(s, a, res)$ (۱۲)

۶-۱-۳- قواعد دسترسی در شرایط اضطراری

مجموعه‌ای از شرایط و علایم حیاتی مربوط به بیمار وجود دارد که نیازمند رسیدگی فوری است. این شرایط با بررسی مقادیر پارامترهای حیاتی بیمار (که از طریق حس‌گرهایی که به بدن بیمار متصل است، اندازه‌گیری می‌شود) مشخص می‌شوند. در قاعدهٔ زیر نحوهٔ استنتاج شرایط اضطراری توصیف شده است:

$\bigwedge_i [Ci(P, V) \wedge V\Theta T] \rightarrow IsEmergency(P)$

$O = \{=, <, >, \le, \ge\}$

[1] Function-free Horn Clause

[DOI: 10.29252/jsdp.17.3.109]

مسند	توضیحات
AssignedLocationP(p, PL)	مکان بیمار p در قالب PL
AssignedLocationS (s, SL)	مکان انجام وظیفه‌ی عامل بیمارستانی s در قالب SL
Assign(p,s)	انتساب بیمار p به عامل بیمارستانی s
TimeTask(s,t_1,t_2)	زمان شیفت کاری عامل بیمارستانی s در بازه t_1 وt_2
CurrentTime(t)	زمان جاری را به t منتسب می‌کند و همواره True برمی‌گرداند.
CurrentDate(d)	تاریخ جاری را به d منتسب می‌کند و همواره True برمی‌گرداند.
HasRole(s,r)	انتساب نقش r به عامل بیمارستانی s
Role-Purpose(r, pu)	انتساب هدف pu به نقش r
InSubset (PL, SL)	مکان بیمار p زیرمجموعه مکان تحت مراقبت عامل بیمارستانی s
IsMemberOfTeam (s, p)	عضو بودن عامل بیمارستانی s در تیم پزشکی بیمار p در بخش اصلی
Preference(p, res-Type, pu)	ترجیحات بیمار p در قالب اختصاص هدف pu به res-Type
AssignedRFID (p, rfid)	اختصاص برچسب rfid به بیمار p
RFID (rfid, s)	شناسایی برچسب rfid توسط عامل بیمارستانی s
IsOwnedBy(res, p)	اختصاص اطلاعات res به بیمار p
Type(res, res-Type)	انتساب منبع داده res به نوع res-Type
AssignedPermission (r, a, res-Type)	انتساب فعالیت a بر روی res-Type به نقش r
CanAccess (s, a, res)	امکان دسترسی عامل بیمارستانی s به فعالیت a بر روی منبع res
HasTeam (p, tm)	انتساب تیم tm به بیمار p
Membership (s, tm, r)	انتساب نقش r در تیم پزشکی tm به عامل بیمارستانی s
Request (s, a, res)	درخواست عمل a بر روی منبع res توسط عامل بیمارستانی s
IsEmergency (p)	تعیین شرایط اضطراری بیمار p
HasPurpose (pu, res-Type)	تعریف سیاست بیمارستان در قالب انتساب هدف pu به res-Type
CanAccessP (s, a, res, pu)	امکان دسترسی عامل بیمارستانی s به عمل a بر روی منبع res با هدف دسترسی pu
PRequest(s, a, res, pu)	درخواست عمل a بر روی منبع res توسط عامل بیمارستانی s با هدف دسترسی pu
Delegate (s_1, s_2, r, tm, startTime, endTime)	واگذاری نقش r در تیم tm به عامل s_2 توسط عامل s_1 در بازه startTime تا endTime
Fetch(s, a, res, pu)	واکشی اطلاعات برای عامل s با انجام عمل a بر روی منبع res با هدف دسترسی pu

(جدول-۱): تعریف مسندها

(Table-1): Definition of predicates

در این قاعده، C_i یکی از پارامترهای حیاتی بیمار P (مانند ضربان قلب) است و VT توصیف‌کنندهٔ محدوده‌ی مقادیر این پارامتر در شرایط اضطراری است که در آن T یک مقدار ثابت و θ یکی از عملگرهای قیاسی است که به‌صورت بالا تعریف می‌شود. در این قاعده مجموعه‌ای از شرایط مرتبط با پارامترهای حیاتی مختلف در نظر گرفته شده است که در صورت برقراری هم‌زمان آن‌ها شرایط بیمار P اضطراری اعلام می‌شود. برای مثال وقتی فشار خون یک بیمار بالای ۱۷ باشد، شرایطی اورژانسی محسوب می‌شود. این قاعده را بر اساس قالب تعریف‌شده می‌توان به‌صورت زیر توصیف کرد:

$$Pressure(P,V) \wedge V > 17 \rightarrow IsEmergency(P)$$

زمانی که یک عامل بیمارستانی درخواست دسترسی به اطلاعات بیمار را داشته باشد، بررسی می‌شود که آیا وضعیت بیمار اضطراری است، یا خیر. اگر اضطراری بود، برای رسیدگی به وضعیت بیمار و درمان به‌موقع او، ممکن است، مجوزهایی برای دسترسی به اطلاعات به عامل بیمارستانی داده شود که در وضعیت عادی این مجوزها را نداشته است. پس از درمان بیمار و برگشت او به وضعیت عادی، مجوزهایی که به‌صورت پویا در شرایط اضطراری به عامل بیمارستانی داده شده بود از او پس گرفته می‌شود.

❖ تعریف قاعدهٔ دسترسی در بخش اورژانس:

✓ اگر بیمار روی تختی بستری و شرایط بیمار اضطراری باشد، نزدیک‌ترین عامل بیمارستانی درخواست

[DOI: 10.29252/jsdp.17.3.109]

دسترسی به اطلاعات بیمار را می‌دهد و با توجه به نقشی که دارد و نزدیکی او به بیمار (که با استفاده از RFID متصل به تخت بیمار بررسی می‌شود)، دسترسی به اطلاعات در این شرایط به او داده می‌شود.

$$Request(s, a, res) \wedge CurrentTime(t) \wedge TimeTask(s, t_1, t_2) \wedge (t_1 \le t \le t_2) \wedge IsOwnedBy(res, p) \wedge Type(res, res\text{-}Type) \wedge IsEmergency(p) \wedge RFID(rfid, s) \wedge AssignedRFID(p, rfid) \wedge HasRole(s, r) \wedge AssignedPermission(r, a, res\text{-}Type) \rightarrow CanAccess(s, a, res) \quad (۱۳)$$

توجه کنید که طبق این قاعده با توجه به شرایط اضطراری بیمار، هر عامل بیمارستانی (مانند پزشک) که در کنار بیمار باشد، می‌تواند برای کمک به بیمار به اطلاعات وی دسترسی پیدا کند، حتی اگر آن عامل بیمارستانی مسئول مستقیم بیمار نباشد. درواقع به‌دلیل شرایط اضطراری، برخی محدودیت‌ها نادیده گرفته و تنها بر اساس نقش عامل بیمارستانی دسترسی‌ها اعطا می‌شود.

❖ **تعریف قاعدهٔ دسترسی در بخش‌های اصلی:**

✓ اگر در بخش‌های اصلی، عامل بیمارستانی در تیم پزشکی بیمار نباشد و شرایط بیمار اضطراری باشد و عامل بیمارستانی درخواست دسترسی به اطلاعات بیمار را داشته باشد، با توجه به نزدیکی عامل بیمارستانی به بیمار و نقشی که دارد، می‌تواند به اطلاعات بیمار دسترسی داشته باشد.

$$Request(s, a, res) \wedge CurrentTime(t) \wedge TimeTask(s, t_1, t_2) \wedge (t_1 \le t \le t_2) \wedge IsOwnedBy(res, p) \wedge Type(res, res\text{-}Type) \wedge IsEmergency(p) \wedge RFID(rfid, s) \wedge AssignedRFID(p, rfid) \wedge HasRole(s, r) \wedge AssignedPermission(r, a, res\text{-}Type) \rightarrow CanAccess(s, a, res) \quad (۱۴)$$

۲-۳- مدل حافظ حریم خصوصی $TbDAC_1$

حفظ و نگهداری اطلاعات و حریم خصوصی بیماران از جمله مسائلی است که امروزه نگرانی‌هایی را به‌وجود آورده است. به همین دلیل در سال ۱۹۹۶ استاندارد HIPAA (*قانون* انتقال و پاسخ‌گویی الکترونیکی بیمه سلامت) در صنعت سلامت الکترونیکی آمریکا به‌عنوان قانون فدرال ایالات متحده تنظیم شد. در بخش مربوط به استانداردهای امنیتی این قانون آمده است که:

- سازمان باید در راه‌اندازی سامانه ثبت اطلاعات مربوط به سلامت، اقداماتی همچون تأمین هزینهٔ اقدامات امنیتی، آموزش افرادی در دسترسی به اطلاعات سلامت بیماران و سازوکارهایی جهت تضمین رعایت قوانین تصویب‌شده در سازمان‌های بالادستی برای جلوگیری از دسترسی افراد غیرمجاز به اطلاعات بیماران را در نظر داشته باشد [25].
- هر فردی که مسئول انتقال و نگهداری اطلاعات سلامت بیماران است، باید تمام حفاظت‌های فنی، فیزیکی و اجرایی را برای اطمینان از حفظ صحت و محرمانگی اطلاعات، جلوگیری از تهدیدها و خطرات محرمانگی یا امنیتی اطلاعات و جلوگیری از استفادهٔ غیرمجاز یا افشای اطلاعات، اعمال کند [25].
- عوامل بیمارستانی در شرایط اضطراری و احیای بیمار، می‌توانند به اطلاعات سلامت بیمار بدون اجازه وی دسترسی داشته باشند [26].
- بیمار نیز باید بتواند از نحوهٔ نگهداری و استفاده از اطلاعات سلامتش آگاهی داشته باشد، همچنین می‌تواند دست‌یابی به اطلاعات سلامت خود را از طریق مدیریت کلیدهای رمزگذاری کنترل کند [27].

در ادامه با ارتقای مدل هسته ارایه‌شده در بخش‌های قبلی، مدلی با قابلیت حفظ حریم خصوصی در کنترل دسترسی به اطلاعات سلامت الکترونیکی بیماران ارایه می‌شود.

۱-۲-۳- فرآیندهای درمانی با حفظ حریم خصوصی

پس از ورود بیمار به بیمارستان و هنگام تشکیل پرونده، سرپرستار وظیفه دارد ترجیحات خصوصی بیماران را ثبت و بر اساس آن تیم پزشکی و شرایط مناسب را برای بیمار فراهم کند. در این مرحله مالک داده (بیمار) تعیین می‌کند هر نوع منبعی از اطلاعاتش با چه هدفی در اختیار درخواست‌کنندگان اطلاعات قرارگیرد. این عمل درواقع همان رضایت کتبی است که بیمار زمان بستری در بیمارستان به پذیرش می‌دهد تا عوامل بیمارستانی اجازه دسترسی به اطلاعاتش را داشته باشند؛ همچنین در بیمارستان‌ها خط‌مشی‌هایی برای خدمات‌رسانی با کیفیت‌تر و سریع‌تر به بیماران با توجه به خط‌مشی‌های کلی وزارت بهداشت، درمان و علوم پزشکی تبیین شده است که در قالب مجوزهای دسترسی برای اهداف مختلف تعریف می‌شود. درواقع تعیین ترجیحات بیماران تا زمانی اعمال می‌شود که در اجرای رسالت اصلی بیمارستان خللی وارد نگردد.

به‌طورکلی بیمارستان‌ها به دو نوع تقسیم می‌شوند: بیمارستان‌های آموزشی ـ درمانی و بیمارستان‌های فقط درمانی. برای هر نوع از این بیمارستان‌ها اهدافی تعیین می‌شود که برای دست‌یابی به برخی از آنها به‌حتم مجوز

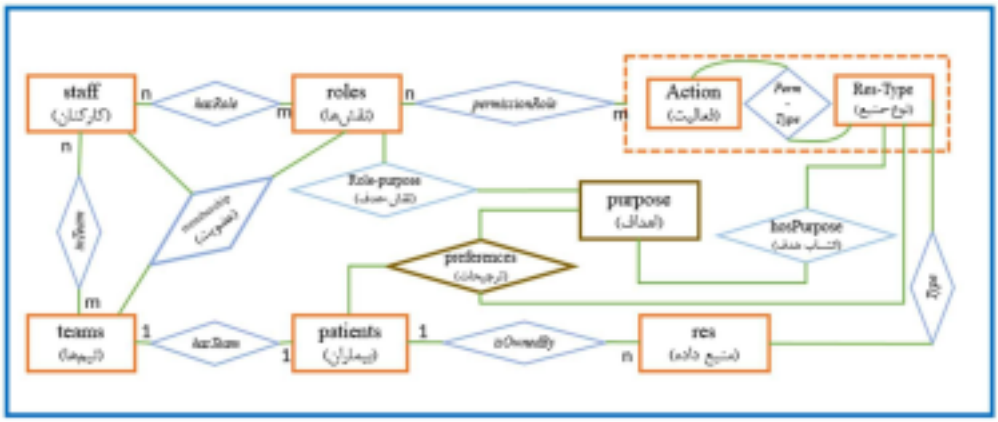
[DOI: 10.29252/jsdp.17.3.109]

دسترسی به نوع‌منبع‌های مشخصی از بیماران باید وجود داشته باشد؛ مانند هدف درمانی؛ اما برای برخی اهداف مانند هدف آموزشی، بسته به نوع بیمارستان تعیین می‌شود که مجوز دسترسی به اطلاعات بیماران لازم است یا نه. به‌عنوان مثال برای بیمارستان‌های آموزشی- درمانی اگر بیمار اجازهٔ دسترسی به برخی منابع خود را برای هدف آموزشی به بیمارستان ندهد، درحالی‌که بیمارستان برای دست‌یابی به هدف آموزشی به آن نوع‌منبع نیاز داشته باشد با توجه به نوع بیمارستان این ترجیح بیمار در نظر گرفته نمی‌شود؛ اما اگر همین شرایط در بیمارستان فقط درمانی باشد، ترجیح بیمار ثبت شده و بیمارستان اجازه ندارد از منابع بیمار برای هدف آموزشی استفاده کند.

هنگامی که بیمار زیر سن قانونی است و یا در زمانی که بیمار در شرایط اضطراری (اورژانسی) وارد بیمارستان شده و شرایط دادن رضایت کتبی و تعیین ترجیحاتش را ندارد، والدین یا فامیل درجهٔ یک او تعیین می‌کنند که هرکدام از اطلاعات موجود در پروندهٔ الکترونیکی سلامت با چه هدفی می‌تواند در دسترس درخواست‌کنندگان قرار گیرد.

۲-۲-۳- تعریف مدل داده‌ای $TbDAC_1$

برای حفظ حریم خصوصی در این مدل، دو مؤلفهٔ هدف و ترجیحات به ساختار آن اضافه شده است که در ادامه به‌تفصیل معرفی می‌شوند. شکل (۸)، مؤلفه‌های این مدل کنترل دسترسی را نشان می‌دهد.



(شکل-۸): مدل داده‌ای کنترل دسترسی حافظ حریم خصوصی

(Figure-8): privacy preserving access control data model

هدف: این مؤلفه درواقع هدف جمع‌آوری اطلاعات و استفاده از آن را با توجه به خط‌مشی‌های بیمارستان و همچنین ترجیحات مالک اطلاعات که در اینجا منظور بیمار است، تعیین می‌کند. در این مدل دو نوع هدف در نظر گرفته می‌شود. نخست همان هدفی است که اطلاعات با آن نیت جمع‌آوری می‌شوند (Purpose) و دیگری هدف دسترسی است که به معنای هدف کاربر برای دسترسی به اطلاعات است (AccessPurpose) که باید بررسی شود که این دو هدف با هم سازگار باشند و در آن صورت اجازه دسترسی به اطلاعات داده شود. همچنین اهداف در کاربرد سلامت الکترونیکی به چهار دسته تقسیم‌بندی می‌شوند: اهداف درمانی، آموزشی، پژوهشی و اداری.

اگر مجموعهٔ اهداف با purposes نمایش داده شود، اهداف بیمارستان در استفاده از انواع داده‌های بیماران به‌صورت صوری به‌شکل زیر بیان می‌شوند. مسند HospPurpose نیز توصیف‌گر همین موضوع است که در توصیف قواعد از آن استفاده می‌شود:

$$\text{hospPurpose} \subseteq \text{purposes} \times \text{res-type}$$

$$\text{HospPurpose}(pu, rt) = \text{True} \leftrightarrow (pu, rt) \in \text{hospPurpose} \quad (۱۵)$$

رابطهٔ hospPurpose درواقع با توجه به خط‌مشی‌های بیمارستان و نیازمندی‌هایی که برای دسترسی به داده‌های بیماران برای انجام بهتر رسالت خود دارد تعریف می‌شود و تعیین می‌کند برای هرکدام از اهداف تعریف‌شده در این مدل، بیمارستان نیاز به چه نوع‌منبعی دارد؛ همچنین در این مدل با اضافه‌شدن هدف، باید مشخص شود که هر نقش مجاز است برای چه اهدافی به کار گرفته شود. به همین منظور رابطهٔ role-Purpose به‌صورت زیر تعریف می‌شود:

$$\text{role-Purpose} \subseteq \text{roles} \times \text{purposes}$$

$$\text{Role-Purpose}(r, p) = \text{True} \leftrightarrow (r, p) \in \text{role-Purpose} \quad (۱۶)$$

[DOI: 10.29252/jsdp.17.3.109]

هدف دسترسی (Access Purpose) که پیش‌تر عنوان شده بود نیز هدفی است که عامل بیمارستانی هنگام درخواست دسترسی به اطلاعات بیمار آن را مشخص می‌کند و در زمان بررسی درخواست بررسی می‌شود که این هدف، با اهداف تعریف‌شده برای آن عامل (بر اساس نقش منتسب به وی) سازگار است یا خیر و با توجه به آن دسترسی داده یا رد می‌شود. درعمل هنگامی که عامل وارد سامانه می‌شود، تعیین می‌کند که با چه نقش و هدفی قصد ورود دارد؛ سپس بررسی می‌شود که با این نقش تعیین‌شده، عامل مجوز دسترسی به اطلاعات با هدف تعیین‌شده را دارد یا نه؟ که در صورت مجازبودن ادامهٔ روند درخواست برای عامل انجام می‌شود.

ترجیحات: در این مدل هر بیمار هنگام تشکیل پرونده مجموعه‌ای از ترجیحات خود را تعریف می‌کند. تابع preferences در این مدل، ترجیحات بیماران را مشخص می‌کند و به‌صورت صوری زیر تعریف می‌شود:

$$\text{preferences: patients} \rightarrow 2^{\text{res-type} \times \text{purposes}}$$

$$\text{Preference}(p, rt, pu) = \text{True} \leftrightarrow (rt, pu) \in \text{preferences}(p) \quad (۱۷)$$

باید توجه شود ترجیحاتی که بیماران برای حفظ حریم خصوصی‌شان تعیین می‌کنند، مغایر با قوانین بیمارستان، خط‌مشی‌های وزارت بهداشت، درمان و علوم پزشکی نباشد. برای بررسی سازگاربودن ترجیحات تعیین‌شده توسط بیماران با خط مشی‌های تعریفی بیمارستان، لازم است بررسی شود که برای هر نوع منبع داده‌ای که بیمارستان برای هدفی به آن نیاز دارد، بیمار نیز دسترسی به آن منبع را در ترجیحاتش برای هدف موردنظر مجاز دانسته باشد.

$$\forall p \in \text{patients}, \nexists\, pu \in \text{purposes}, (pu, rt) \in \text{hospPurpose} \wedge (rt, pu) \notin \text{preferences}(p)$$

اگر این رابطه درست نباشد یعنی منبعی وجود داشته باشد که طبق خط مشی بیمارستان دسترسی به آن منبع با هدفی خاص موردنیاز باشد، اما بیمار در ترجیحاتش دسترسی به آن منبع را برای هدف موردنظر غیرمجاز بداند با توجه به اینکه بیمارستان فقط درمانی است یا آموزشی ـ درمانی، تعیین می‌شود که ترجیحات بیمار درنظر گرفته شود یا نه.

پس از این بررسی، ترجیحات بیمار با توجه به نتیجهٔ رابطهٔ بالا بازتعریف می‌شود.

۳-۲-۳- فرآیند کنترل دسترسی حافظ حریم خصوصی

زمانی که هرکدام از عوامل بیمارستانی درخواست خود را مطرح می‌کنند، لازم است، نقش و هدف دسترسی خود را به اطلاعات درخواست‌شده مشخص کنند. اگر این هدف با هدفی که اطلاعات مورد نیاز جمع‌آوری شده و همچنین ترجیحاتی که بیمار از ابتدا تعیین کرده (با درنظرگرفتن قوانین بیمارستان و خط‌مشی‌های وزارت بهداشت، درمان و علوم پزشکی) مطابقت داشته باشد، درخواست پذیرفته و درغیراین‌صورت رد می‌شود.

۳-۲-۴- قواعد دسترسی در شرایط عادی

قواعد کنترل دسترسی حافظ حریم خصوصی نیز مانند حالت هسته در دو وضعیت عادی و اضطراری مورد ارزیابی قرار می‌گیرد. تنها تفاوتی که این مدل با قواعد کنترل دسترسی در مدل قبل دارد این است که هنگام درخواست دسترسی توسط عوامل بیمارستانی، باید هدف دسترسی آنها را در نظر داشت و با توجه به آن، خط‌مشی‌هایی که بیمارستان تعیین کرده و ترجیحاتی که بیماران مشخص کرده‌اند، مجوز دسترسی موردنیاز با حفظ حریم خصوصی بیمار به عامل بیمارستانی اختصاص یابد.

علاوه‌بر حقایق و اطلاعات پایه‌ای که در مدل کنترل دسترسی هسته به آن‌ها پرداخته شد، در مدل کنترل دسترسی حافظ حریم خصوصی، ترجیحات حفظ حریم خصوصی بیماران نیز جزو حقایقی هستند که باید در تعریف قواعد دسترسی مورد توجه قرار گیرند؛ لذا حقایقی با استفاده از مسند Preference به‌صورت زیر تعریف می‌شوند که در فرآیند کنترل دسترسی به کار گرفته می‌شوند:

Preference(P, Res-Type, Pu)

پس از تعریف این ترجیحات توسط بیمار، با توجه به خط‌مشی‌های بیمارستان، همان‌طور که در قسمت قبل گفته شد، در صورت لزوم ترجیحات بازتعریف می‌شوند.

❖ **تعریف قاعدهٔ دسترسی در بخش اورژانس:**

- ✓ اگر عامل بیمارستانی مسئول یک بیمار باشد با توجه به هدف دسترسی عامل بیمارستانی به اطلاعات بیمار، نقشی که آن عامل دارد و خط‌مشی‌های بیمارستان و ترجیحات بیمار، دسترسی به اطلاعات بیمار به او داده می‌شود:

$$\text{Assign}(p, s) \wedge \text{CurrentTime}(t) \wedge \text{TimeTask}(s, t_1, t_2) \wedge (t_1 \le t \le t_2) \wedge \text{IsOwnedBy}(res, p) \wedge \text{Type}(res, res\text{-Type}) \wedge \text{HasRole}(s, r) \wedge \text{Role-Purpose}(r, pu) \wedge \quad (۱۸)$$

[DOI: 10.29252/jsdp.17.3.109]

HospPurpose (pu, res-Type) ∧ Preference(p, res-Type, pu) ∧ AssignedPermission (r, a, res-Type) → CanAccessP (s, a, res, pu)

❖ **تعریف قاعدهٔ دسترسی در بخش‌های اصلی:**

✓ اگر عامل بیمارستانی در تیم پزشکی یک بیمار باشد، آنگاه با توجه به هدف دسترسی عامل بیمارستانی به اطلاعات بیمار، نقشی که در آن تیم دارد، خط‌مشی‌های بیمارستان و ترجیحات بیمار، دسترسی مورد تقاضا به عامل بیمارستانی داده خواهد شد:

IsOwnedBy(res, p) ∧ Type(res, res-Type) (۱۹)
∧ CurrentTime (t) ∧ TimeTask (s, t_1, t_2) ∧ ($t_1 \le t \le t_2$) ∧ HasTeam (p, tm) ∧ Membership (s, tm, r) ∧ Role-Purpose(r, pu)∧ HospPurpose (pu, res-Type) ∧ Preference(p, res-Type, pu) ∧AssignedPermission (r, a, res-Type) → CanAccessP (s, a, res, pu)

۳-۲-۵- قواعد دسترسی در شرایط اضطراری

کنترل دسترسی در شرایط اضطراری در مدل حافظ حریم خصوصی مانند مدل هستهٔ $TbDAC_0$ است؛ فقط تفاوتی که وجود دارد در این است که چون در این مدل بیماران ترجیحاتی را تعیین کرده‌اند، همچنین طبق تعریف Purpose هر نوع‌منبعی برای اهداف خاصی جمع‌آوری شده است، ممکن است درخواستی که عامل بیمارستانی دارد در شرایط اضطراری نیز قابل پذیرش نباشد و مجوز دسترسی به اطلاعات خواسته‌شده‌اش را نداشته باشد، در این شرایط درخواست او رد می‌شود.

❖ **تعریف قاعدهٔ دسترسی در بخش اورژانس:**

✓ اگر بیمار روی تختی بستری و شرایط بیمار اضطراری باشد و نزدیک‌ترین عامل بیمارستانی، مسئول آن تخت نباشد، عامل بیمارستانی درخواست دسترسی به اطلاعات بیمار را می‌دهد و با توجه به نقشی که دارد، هدف دسترسی اضطراری او به اطلاعات بیمار، نزدیکی او به بیمار (که با استفاده از RFID متصل به تخت بیمار بررسی می‌شود) و خط‌مشی‌های بیمارستان و ترجیحات بیمار، دسترسی به اطلاعات در این شرایط به او داده می‌شود:

PRequest(s, a, res, pu) ∧ CurrentTime (t) ∧ (۲۰)
TimeTask (s, t_1, t_2) ∧ ($t_1 \le t \le t_2$) ∧ IsOwnedBy(res, p) ∧ Type(res, res-Type) ∧ RFID (rfid, s) ∧ AssignedRFID (p, rfid) ∧ IsEmergency (p) ∧ HasRole (s, r) ∧ Role-Purpose (r, pu) ∧ HospPurpose (pu, res-Type) ∧ Preference(p, res-Type, pu) ∧ AssignedPermission (r, a, res-Type) → CanAccessP (s, a, res, pu)

❖ **تعریف قاعدهٔ دسترسی در بخش‌های اصلی:**

✓ اگر در بخش‌های اصلی، عامل بیمارستانی در تیم پزشکی بیمار نباشد و شرایطِ بیمار، اضطراری و عامل بیمارستانی درخواست دسترسی را با هدف اضطراری به اطلاعات بیمار داشته باشد، با توجه به نزدیکی عامل بیمارستانی به بیمار، نقشی که دارد، خط‌مشی‌های بیمارستان و ترجیحات بیمار، دسترسی به اطلاعات بیمار به او داده می‌شود.

PRequest (s, a, res, pu) ∧ CurrentTime (t) (۲۱)
∧ TimeTask (s, t_1, t_2) ∧ ($t_1 \le t \le t_2$) ∧ IsOwnedBy(res, p) ∧ Type(res, res-Type) ∧ RFID (rfid, s) ∧ AssignedRFID (p, rfid) ∧ IsEmergency (p) ∧ HasRole(s, r) ∧ Role-Purpose (r, pu) ∧ AssignedPermission (r, a, res-Type) ∧ HosPurpose (pu, res-Type) ∧ Preference(p, res-Type, pu) → CanAccessP (s, a, res, pu)

۳-۳- مدل با قابلیت وکالت دسترسی $TbDAC_2$

در زمان‌هایی ممکن است، پزشک به‌دلیل مرخصی، مدتی را در بیمارستان حضور نداشته باشد. در این موارد لازم است پزشک دیگری به‌عنوان جایگزین، نقش‌هایی را که پزشک غایب دارد، ایفا کند؛ در این موارد پزشک اصلی می‌تواند سه رویکرد را در پیش گیرد. نخست این‌که پزشک نقش خود را در یکی از تیم‌هایش به یک نفر و نقش دیگری در تیم دیگرش را به شخص دیگری وکالت دهد. دوم این‌که پزشک یکی از نقش‌هایش را به یکی از جانشینان خود وکالت دهد که در این حالت پزشک وکیل در همهٔ تیم‌هایی که پزشک اصلی آن نقش را داشته، جانشین می‌شود. در حالت آخر پزشک همهٔ نقش‌هایش را در همهٔ تیم‌هایی که در آن‌ها عضو است، به یک جایگزین وکالت می‌دهد و آن پزشک در همهٔ تیم‌هایی که پزشک اصلی در آن عضو بوده نقش‌هایش را ایفا می‌کند. در این مدل کل مجوزهای نقش پزشک اصلی به پزشک وکیل، وکالت داده می‌شود نه بخشی از مجوزها:

delegates ⊆ staff ×staff ×roles ×teams ×datetime × datetime
(s_1, s_2, r, tm, startTime, endTime) ∈ (۲۲)
delegates ↔ (s_1, tm, r) ∈ membership ∧ (s_2, r) ∈ hasRole
Delegate (s_1, s_2, r, tm, startTime, endTime) = (۲۳)
True ↔ CurrentDate(d) ∧ (s_1, s_2, r, t, startTime, endTime) ∈ delegates ∧ (startTime ≤ d≤ endTime)

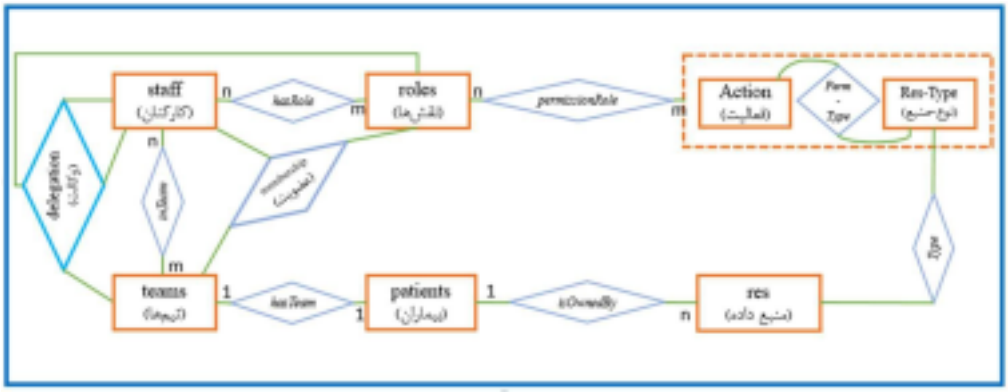
طبق توصیف بالا پزشک s_1 می‌تواند نقش r خود را در تیم tm به پزشک s_2 در طول بازهٔ زمانی startTime تا endTime وکالت دهد.

[DOI: 10.29252/jsdp.17.3.109]

در توصیف بالا مسند CurrentDate(d) تاریخ فعلی را به متغیر d منتسب می‌کند و همواره True برمی‌گرداند.

شکل (۹)، این مدل را نشان می‌دهد.

برای حالتی که پزشک بخواهد یک جانشین انتخاب کند و همهٔ نقش‌هایش در همه‌ی تیم‌ها را به او بسپارد، کافی است به جای مقادیر r و t علامت * جایگزین شود. در حالتی که پزشک یک نقش خود را به یک نفر وکالت می‌دهد تا آن شخص در همهٔ تیم‌هایی که پزشک اصلی آن نقش را داشته جایگزین وی شود، به جای مقدار t، علامت * گذاشته می‌شود.



(شکل-۹): مدل داده‌ای کنترل دسترسی با قابلیت وکالت دسترسی

(Figure-9): access control data model with access delegation

۱-۳-۳- فرآیند مدیریت وکالت

زمانی که هر کدام از عوامل بیمارستانی به‌خصوص پزشکان قصد دارند برای مدتی در بیمارستان حضور نداشته باشند، باید مانند هر نهاد دیگری برای مدتی‌که حضور ندارند، مرخصی بگیرند. در این موارد فرد (پزشک) باید هنگام ارایه درخواست مرخصی به بیمارستان، فرد (پزشک) دیگری را به‌عنوان جانشین خود در بازهٔ زمانی مشخصی تعیین کند. پس از ارائهٔ این درخواست فرد (پزشک) وکیل باید پذیرش این مسئولیت را تأیید و در آخرین مرحله رییس بیمارستان نیز آن را تأیید کند؛ در این صورت اجازه مرخصی به فرد (پزشک) داده می‌شود و نقش‌های او به پزشک وکیل در بازهٔ زمانی مطرح شده واگذار می‌شود. درواقع یک گواهی برای درخواست مرخصی صادر می‌شود که تا زمانی که باطل نشود پزشک وکیل عهده‌دار نقش‌های پزشک اصلی خواهد بود.

نقش‌هایی را که به یک عامل بیمارستانی وکالت داده شده است، می‌توان از رابطه زیر به‌دست آورد. در این رابطه t_c زمان فعلی در نظر گرفته شده است:

$$\text{DassignedRole}(s, t_c) = \{r \in roles \mid \exists\, s' \in staff,\ \exists\, r \in roles, \exists\, tm \in teams, (s', s, r, tm, startTime, endTime) \in delegates \wedge (startTime \le t_c \le endTime)\}$$

همچنین تیم‌هایی که یک عامل بیمارستانی در زمان t_c به واسطه وکالت در آن‌ها عضو می‌شود از رابطهٔ زیر به‌دست می‌آید:

$$\text{DassignedTeam}(s, t_c) = \{tm \in teams \mid \exists\, s' \in staff, \exists\, r \in roles, \exists\, tm \in teams, (s', s, r, tm, startTime, endTime) \in delegates \wedge (startTime \le t_c \le endTime)\}$$

و کل تیم‌های یک کاربر در زمان t_c از رابطهٔ زیر به‌دست می‌آید:

$$\text{AssignedTeams}(s, t_c) = \text{assignedTeam}(s) \cup \text{DassignedTeam}(s, t_c)$$

زمانی که پزشک اصلی (s) از مرخصی بازگردد (یا اتمام زمان وکالت) نقش وکالت داده شده به هر وکیل او در هر تیم باید از وکیل بازپس گرفته شود. برای این منظور کافی است تمام چندتایی‌های مربوط به وکالت s یعنی (s, *, *, *) را از delegates حذف کنیم.

ممکن است، در بازه‌ای که پزشک اصلی حضور ندارد، پزشک جایگزین نیز مرخصی بگیرد. در این موارد او نیز به جای خود، پزشک دیگری را جایگزین می‌کند که همهٔ نقش‌هایش به او واگذار می‌شود، حتی نقش‌هایی که به‌صورت وکالتی از پزشکی دیگر به او سپرده شده بود.

پس از منقضی‌شدن زمان مرخصی (گواهی) یا بازگشت پزشک اصلی، گواهی مرخصی باطل می‌شود و تمام نقش‌هایی که به پزشک وکیل و حتی پزشکِ وکیلِ پزشکِ وکیل واگذار شده بود، بازپس‌گرفته می‌شود.

[DOI: 10.29252/jsdp.17.3.109]

۲-۳-۳- فرآیند کنترل دسترسی با قابلیت وکالت

هنگامی که هر یک از عوامل بیمارستانی درخواست دسترسی به اطلاعات بیماری را داشته باشند، مانند مدل‌های قبلی اگر از اعضای تیم بیمار یا مسئول تخت بیمار باشند می‌توانند به اطلاعاتش دسترسی داشته باشند. تنها تفاوتی که در این مدل وجود دارد، این است که ممکن است، پزشکی برای مدتی که پزشک دیگر نقش‌های خود را به او واگذار کرده اجازهٔ دسترسی به اطلاعات بعضی بیماران را داشته باشد که در این مدل در زمان کنترل دسترسی این تغییرات در پایگاه دانش امنیتی با توجه به پایگاه قواعد کنترل دسترسی و اطلاعات بیمار و عامل بیمارستانی بررسی می‌شود.

۳-۳-۳- قواعد دسترسی در شرایط عادی

قواعد کنترل دسترسی با قابلیت وکالت دسترسی مانند حالت هسته است، تنها تفاوتی که وجود دارد، این است که هنگامی که عامل بیمارستانی درخواست دسترسی به اطلاعات بیماری را دارد، درصورتی‌که جزو تیم پزشکی آن بیمار نیست، با توجه به نقش وی و این‌که ممکن است، یکی از اعضای تیم پزشکی بیمار نقش خود را به این عامل بیمارستانی برای مدتی واگذار کرده باشد، دسترسی به عامل بیمارستانی داده می‌شود.

❖ **قاعدهٔ دسترسی در بخش اورژانس:**

در بخش اورژانس از آن‌جایی‌که دسترسی‌های عوامل بیمارستانی براساس نوبت کاری و مجموعه تخت‌هایی است که مسئول مراقبت و درمان از آنها هستند و پس از تمام‌شدن شیفت کاری افراد جدید جایگزین می‌شوند مفهومی با عنوان وکالت را نمی‌توان درنظر گرفت و قواعد دسترسی به‌طوردقیق مانند همین حالت در مدل هسته است.

❖ **تعریف قاعدهٔ دسترسی در بخش‌های اصلی:**

✓ اگر عامل بیمارستانی به واسطهٔ وکالت‌دادن نقشی توسط یکی از اعضای تیم بیمار به وی، برای مدت مشخصی عضو تیم شده باشد، آنگاه عامل بیمارستانی با توجه به نقشی که در تیم به او واگذار شده به اطلاعات بیمار دسترسی خواهد داشت:

$$\text{Delegate}(s', s, r, tm, startTime, endTime) \wedge \text{Membership}(s', tm, r) \wedge \text{CurrentTime}(t) \wedge \text{TimeTask}(s, t_1, t_2) \wedge (t_1 \le t \le t_2) \wedge \text{HasTeam}(p, tm) \wedge \text{IsOwnedBy}(res, p) \wedge \text{Type}(res, res\text{-}Type) \wedge \text{AssignedPermission}(r, a, res\text{-}Type) \rightarrow \text{CanAccess}(s, a, res) \quad (۲۴)$$

۴-۳-۳- قواعد دسترسی در شرایط اضطراری

زمانی که هر یک از عوامل بیمارستانی درخواست دسترسی به اطلاعات بیماری را داشته باشند و پس از بررسی وضعیت بیمار مشخص شود که شرایط اضطراری است، با توجه به نقش عامل بیمارستانی ممکن است، برای درمان سریع‌تر بیمار تا زمانی که پزشک یا اعضای تیم پزشکی او در کنار بیمار حاضر شوند، مجوزهایی به عامل بیمارستانی واگذار شود که در وضعیت عادی آن‌ها را نداشته است.

در مواردی هم که درخواست‌کننده‌ای وجود ندارد، اما با تغییرات حس‌گرهای متصل به بیمار وضعیت اضطراری تشخیص داده می‌شود، به نزدیک‌ترین پزشک به بیمار که درکنار او حاضر می‌شود و درخواست دسترسی می‌کند، مجوز دسترسی به اطلاعاتی که لازم است داده می‌شود تا زمانی که پزشک تیم بیمار حاضر شود. پس از اتمام درمان و بازگشت بیمار به وضعیت عادی، تمام مجوزهایی که در این زمان به عوامل بیمارستانی واگذار شده بود، بازپس‌گرفته می‌شود.

در هر حال چون در شرایط اضطراری موضوع واگذاری موقت دسترسی به عوامل بیمارستانی حاضر بر بالین بیمار (که لزوماً عضو تیم پزشکی نیستند) مطرح است؛ لذا وکالت تأثیری بر قواعد دسترسی در شرایط اضطراری ندارد و همان قواعد مطرح در مدل هسته، در این حالت نیز برقرار است.

۴-۳- مدل $TbDAC_3$

این مدل ترکیبی از دو مدل کنترل دسترسی حافظ حریم خصوصی و مدل با قابلیت وکالت دسترسی است که تمام مؤلفه‌ها و روابط را برای اعمال کنترل دسترسی در نظر می‌گیرد. شکل (۱۰)، این مدل را نشان می‌دهد.

۱-۴-۳- فرآیند کنترل دسترسی

فرآیند مدیریتی در این مدل درواقع ترکیب همهٔ مدل‌های قبلی است. هنگامی که یکی از عوامل بیمارستانی درخواست دسترسی به اطلاعات بیماری را دارد، مراحلی برای بررسی این درخواست توسط واحد تصمیم‌گیرندهٔ دسترسی (PDP) طی می‌شود که در شکل (۱۱) نشان داده شده است. در این فرآیند شرایط اضطراری هم در نظر گرفته شده است.

همان‌طور که در شکل قابل مشاهده است، درخواست دسترسی درواقع به این شکل است که یک عامل بیمارستانی با نقش خود درخواست فعالیت بر روی نوع‌منبع مربوط به یک بیمار را با هدف دسترسی خاصی دارد.

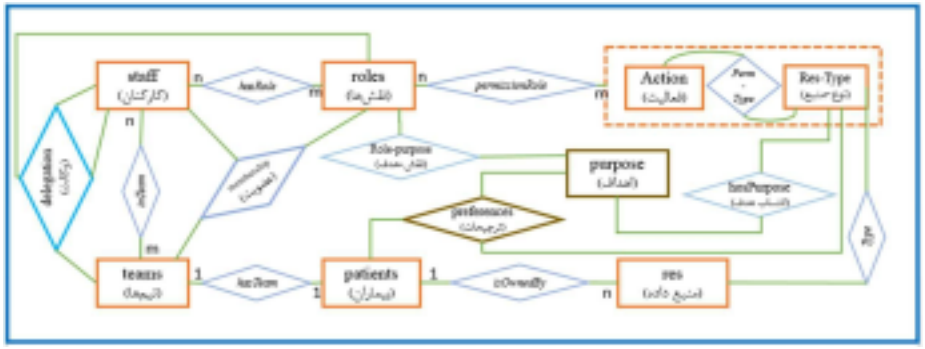
[DOI: 10.29252/jsdp.17.3.109]

۱. در نخستین مرحله باید بررسی شود که اینک زمان کاری و مجاز برای دسترسی عامل بیماستانی هست یا نه؟ اگر زمان مجاز باشد که روند ادامه می‌یابد در غیر این‌صورت درخواست رد می‌شود.

۲. در این مرحله با استفاده از مؤلفهٔ نخست مکان عامل بیمارستانی و بیمار بررسی می‌شود که آنها در مکان یکسان قرار دارند یا خیر؟ (برای مثال هر دو در اورژانس یا هر دو در بخش یکسان) اگر یکسان نباشد که دسترسی داده نمی‌شود؛ اما اگر یکسان باشد، وارد مرحلهٔ بعد می‌شود.

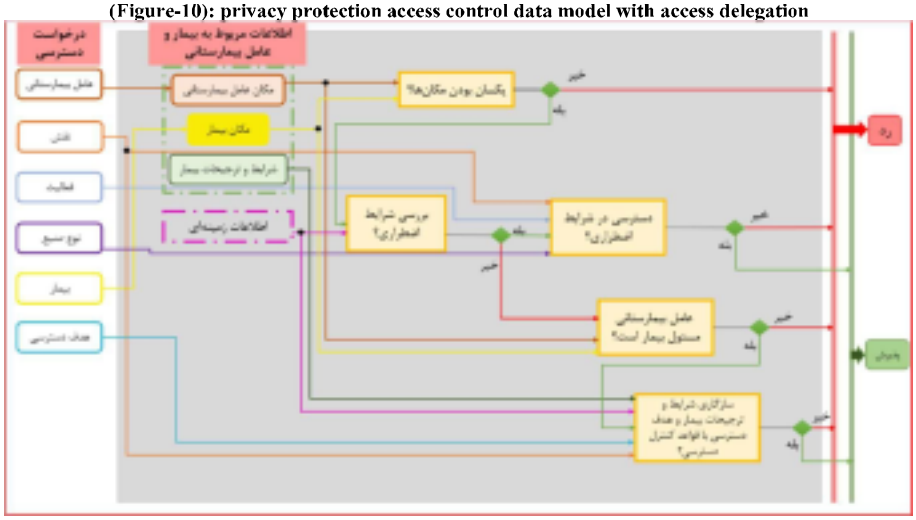
۳. در این مرحله با استفاده از اطلاعاتی که توسط حس‌گرهای مرتبط به روزرسانی می‌شود، بررسی می‌شود که آیا شرایط اضطراری است یا نه؟ اگر شرایط اضطراری باشد، باید بررسی شود این درخواست، امکان پذیرش در شرایط اضطراری را دارد یا خیر. برای بررسی این درخواست ابتدا بررسی می‌کنیم که فعالیت روی نوع‌منبع درخواست‌شده در شرایط اضطراری قابل دسترسی است یا نه اگر نباشد که دسترسی رد می‌شود درغیراین‌صورت بررسی می‌شود عامل بیمارستانی با این نقش، مجوز فعالیت روی این نوع‌منبع را دارد یا نه. اگر مجوز نداشته باشد که دسترسی رد در غیر این‌صورت درخواست دسترسی پذیرفته می‌شود. حال اگر شرایط اضطراری نباشد وارد مرحله بعد می‌شود.

۴. در این مرحله با استفاده از آرگومان دوم مکان عامل و بیمار بررسی می‌شود که آیا بیمار تحت مسئولیت عامل بیمارستانی است یا خیر اگر عامل بیمارستانی مسئول بیمار نباشد که درخواست او رد می‌شود؛ اما اگر عامل بیمارستانی مسئول رسیدگی به بیمار باشد، بررسی می‌شود هدف دسترسی با هدف جمع‌آوری آن داده (فعالیت روی نوع-منبع) سازگار است یا نه؟ همچنین شرایط و ترجیحات بیمار، شرایط زمانی و سایر قوانین بیمارستانی که در قواعد کنترل دسترسی آمده است بررسی می‌شود. اگر این شرایط با درخواست دسترسی سازگار بود که دسترسی داده می‌شود، در غیر این‌صورت دسترسی رد خواهد شد.



(شکل-۱۰): مدل داده‌ای کنترل دسترسی حافظ حریم خصوصی با قابلیت وکالت دسترسی

(Figure-10): privacy protection access control data model with access delegation



(شکل-۱۱): فرآیند رسیدگی به درخواست کنترل دسترسی توسط PDP

(Figure-11): the process of handling an access control request by PDP

[DOI: 10.29252/jsdp.17.3.109]

۲-۴-۳- قواعد دسترسی در شرایط عادی

قواعد کنترل دسترسی حافظ حریم خصوصی با قابلیت وکالت دسترسی از ترکیب دو قاعدهٔ قبلی حاصل شده است. درواقع دسترسی به اطلاعات بیمار با توجه به هدف دسترسی عامل بیمارستانی به اطلاعات، خط‌مشی‌های بیمارستان، ترجیحات بیمار و نقشی که عامل بیمارستانی دارد یا به او وکالت داده شده (در یک دورهٔ زمانی مشخص)، به عامل بیمارستانی داده می‌شود.

❖ **قاعدهٔ دسترسی در بخش اورژانس:**

✓ اگر عامل بیمارستانی مسئول یک بیمار باشد با توجه به هدف دسترسی عامل بیمارستانی به اطلاعات بیمار و نقشی که عامل بیمارستانی دارد و خط‌مشی‌های بیمارستان و ترجیحات بیمار، دسترسی به اطلاعات بیمار به او داده می‌شود. در این حالت چون وکالت به شکلی که ما تعریف کردیم، قابل تعریف نیست، قاعده به‌طوردقیق مانند حالت حافظ حریم خصوصی است.

❖ **تعریف قاعدهٔ دسترسی در بخش‌های اصلی:**

✓ اگر عامل بیمارستانی در تیم پزشکی بیمار حضور داشته باشند (بدون وکالت یا با وکالت)، آن‌گاه با توجه به هدف دسترسی عامل بیمارستانی به اطلاعات بیمار، نقشی که در آن تیم دارد (یا به او وکالت داده شده)، خط‌مشی‌های بیمارستان و ترجیحات بیمار، امکان دسترسی وی به اطلاعات بیمار مشخص خواهد شد.

$$\text{IsMemberOfTeam}(s, p) \wedge \text{IsOwnedBy}(res, p) \wedge \text{Type}(res, res\text{-}Type) \wedge \text{HasTeam}(p, tm) \wedge \text{Membership}(s, tm, r) \wedge \text{Role-Purpose}(r, pu) \wedge \text{HospPurpose}(pu, res\text{-}Type) \wedge \text{Preference}(p, res\text{-}Type, pu) \wedge \text{CurrentTime}(t) \wedge \text{TimeTask}(s, t_1, t_2) \wedge (t_1 \le t \le t_2) \wedge \text{AssignedPermission}(r, a, res\text{-}Type) \rightarrow \text{CanAccessP}(s, a, res, pu) \quad (۲۵)$$

✓ به‌صورت کلی اگر عامل بیمارستانی نزدیک به بیماری شود و با برچسب‌خوان (RFID reader)، برچسب RFID منتسب به بیمار را شناسایی کند؛ در حالتی که بیمار و عامل بیمارستانی در یک تیم باشند یا بیمار به عامل موردنظر منتسب شده باشد با توجه به نقش عامل در تیم بیمار، خط‌مشی‌های بیمارستانی و ترجیحات بیمار، اطلاعات بیمار می‌تواند به‌طور خودکار واکشی شده و در اختیار عامل بیمارستانی قرار می‌گیرد.

❖ **قاعده واکشی خودکار در بخش‌های اصلی:**

$$\text{RFID}(rfid, s) \wedge \text{AssignedRFID}(p, rfid) \wedge \text{IsMemberOfTeam}(s, p) \wedge \text{CurrentTime}(t) \wedge \text{TimeTask}(s, t_1, t_2) \wedge (t_1 \le t \le t_2) \wedge \text{IsOwnedBy}(res, p) \wedge \text{Type}(res, res\text{-}Type) \wedge \text{HasTeam}(p, tm) \wedge \text{Membership}(s, tm, r) \wedge \text{Role-Purpose}(r, pu) \wedge \text{HospPurpose}(pu, res\text{-}Type) \wedge \text{Preference}(p, res\text{-}Type, pu) \wedge \text{AssignedPermission}(r, a, res\text{-}Type) \rightarrow \text{Fetch}(s, a, res, pu) \quad (۲۶)$$

❖ **قاعده واکشی خودکار در بخش اورژانس:**

$$\text{RFID}(rfid, s) \wedge \text{AssignedRFID}(p, rfid) \wedge \text{Assign}(p, s) \wedge \text{IsOwnedBy}(res, p) \wedge \text{Type}(res, res\text{-}Type) \wedge \text{HasRole}(s, r) \wedge \text{Role-Purpose}(r, pu) \wedge \text{HospPurpose}(pu, res\text{-}Type) \wedge \text{Preference}(p, res\text{-}Type, pu) \wedge \text{CurrentTime}(t) \wedge \text{TimeTask}(s, t_1, t_2) \wedge (t_1 \le t \le t_2) \wedge \text{AssignedPermission}(r, a, res\text{-}Type) \rightarrow \text{Fetch}(s, a, res, pu) \quad (۲۷)$$

گفتنی است که استنتاج امکان واکشی به معنای استنتاج امکان دسترسی نیز هست و لذا به‌صورت کلی قاعدهٔ زیر نیز برقرار است:

$$\text{Fetch}(s, a, res, pu) \rightarrow \text{CanAccessP}(s, a, res, pu)$$

۳-۴-۳- قواعد دسترسی در شرایط اضطراری

شرایط اضطراری در این مدل کنترل دسترسی ترکیبی از دو مدل قبلی است. در قواعد کنترل دسترسی همانند مدل کنترل دسترسی با قابلیت وکالت دسترسی، وکالت در فرآیند کنترل دسترسی در بخش اورژانس مطرح نیست و فقط قسمت حافظ حریم خصوصی‌بودن در بخش اورژانس اعمال می‌شود؛ اما در بخش‌های اصلی باید در نظر داشت که عامل بیمارستانی ممکن است از طریق وکالت یک نقش، عضو تیم بیمار شده باشد که در این شرایط با توجه به نقش وکالتی‌اش، خط‌مشی‌های بیمارستان و ترجیحات بیمار دسترسی به او داده می‌شود؛ در غیر این‌صورت با نزدیک‌بودن عامل بیمارستانی به بیمار و نقش عامل، دسترسی وی تعیین می‌شود.

❖ **تعریف قاعدهٔ دسترسی بخش در اورژانس:**

✓ اگر بیمار روی تختی بستری و شرایط بیمار اضطراری باشد و نزدیک‌ترین عامل بیمارستانی، مسئول آن تخت نباشد، عامل بیمارستانی درخواست دسترسی به اطلاعات بیمار را می‌دهد و با توجه به نقشی که دارد، هدف دسترسی اضطراری او به اطلاعات بیمار، نزدیکی او به بیمار (که با استفاده از RFID متصل به تخت بیمار بررسی می‌شود) و خط‌مشی‌های بیمارستان و ترجیحات بیمار، دسترسی به اطلاعات در این شرایط به او داده می‌شود.

[DOI: 10.29252/jsdp.17.3.109]

PRequest(s, a, res, pu) ∧ CurrentTime (t) ∧ (۲۸)
TimeTask (s, t_1, t_2) ∧ ($t_1 \leq t \leq t_2$) ∧ IsOwnedBy(res, p) ∧ Type(res, res-Type) ∧ RFID (rfid, s) ∧ AssignedRFID (p, rfid) ∧ IsEmergency (p) ∧ HasRole (s, r) ∧ Role-Purpose(r, pu) ∧ HospPurpose (pu, res-Type) ∧ Preference(p, res-Type, pu) ∧ AssignedPermission (r, a, res-Type) → CanAccessP(s, a, res, pu)

❖ **تعریف قاعدهٔ دسترسی در بخش‌های اصلی:**

✓ اگر عامل بیمارستانی و بیمار در یک تیم پزشکی نباشند و نقشی از آن تیم هم به عامل وکالت داده نشده باشد، با توجه به نزدیکی عامل بیمارستانی به بیمار، نقش بیمار، هدف اضطراری دسترسی به اطلاعات بیمار، خط‌مشی‌های بیمارستان و ترجیحات کاربر، دسترسی به عامل بیمارستانی داده می‌شود:

PRequest(s, a, res, pu) ∧ CurrentTime(t) ∧ (۲۹)
TimeTask (s, t_1, t_2) ∧ ($t_1 \leq t \leq t_2$) ∧ IsOwnedBy(res, p) ∧ Type(res, res-Type) ∧ RFID (rfid, s) ∧ AssignedRFID(p, rfid) ∧ IsEmergency(p) ∧ HasRole(s, r) ∧ Role-Purpose(r, pu) ∧ HospPurpose(pu, res-Type) ∧ Preference(p, res-Type, pu) ∧ AssignedPermission(r, a, res-Type) → CanAccessP(s, a, res, pu)

۵-۳- مدیریت کنترل دسترسی

در توصیف خانواده مدل کنترل دسترسی TbDAC، با تشریح کامل فرآیندهای بیمارستانی و کنترل دسترسی، به‌طور ضمنی به نحوه مدیریت کنترل دسترسی نیز تا حد زیادی اشاره شد. در ادامه به‌طور مشخص نحوه مدیریت کنترل دسترسی و نحوه درج اطلاعات موردنیاز در کنترل دسترسی مورد تشریح قرار می‌گیرد.

در مدل پیشنهادی دو نقش مدیریتی برای مدیریت کنترل دسترسی در نظر گرفته شده است؛ مدیر ارشد امنیتی (که در کل سیستم یک نفر است) و مدیر امنیتی بخش (که در سیستم بیمارستانی به‌طورمعمول همان سرپرستار بخش در نظر گرفته می‌شود). وظایف هر یک از این نقش‌ها در مدیریت کنترل دسترسی به شرح زیر است.

مدیر ارشد امنیتی (SU): مدیر ارشد امنیتی در نصب و راه‌اندازی اولیه سامانه کنترل دسترسی مشخص می‌شود و بیشترین اختیارات مدیریت امنیت را دارد. ضمن آن‌که حیطه مدیریتی مدیران امنیتی بخش‌ها نیز توسط مدیر ارشد تعین و تبیین می‌شود. به‌طور خلاصه اختیارات و وظایف مدیر ارشد امنیتی عبارتند از:

- تعریف نوع‌منبع‌ها (Res-Type)، اَعمال (Action) و نوع‌مجوزها (Perm-Type).
- تعریف نقش‌ها (roles) و انتساب نوع‌مجوزها به نقش‌ها (permissionRole).
- تعریف کارکنان (staff) و انتساب نقش‌های مجاز به آنها (hasRole). اعطای نقش مدیریت امنیتی بخش‌ها نیز در همین قالب صورت می‌پذیرد.
- تعریف مجموعه اهداف دسترسی ممکن (purpose).
- تعیین حیطه مدیریتی مدیران امنیتی بخش‌ها با استفاده از تابع canAssign که به‌صورت زیر تعریف می‌شود:

$$canAssign : staff \rightarrow 2^{staff}$$

این تابع مشخص می‌کند که یک فرد (که دارای نقش مدیر امنیتی بخش است)، حق مدیریت بر روی چه کارکنانی را دارد. این حق مدیریت، امکان انتساب نقش را به کارکنان تحت مدیریت فرد در تیم یک بیمار برای مدیر امنیتی بخش فراهم می‌کند. گفتنی است که در تعریف بالا این محدودیت برقرار است که اگر canAssign(s)=x (برای $x \subseteq staff$) برقرار باشد، آن‌گاه $DSO \in assignedRole(s)$.

- تعریف قواعد توصیف‌کنندهٔ شرایط اضطراری و قواعد دسترسی بر اساس قوانین و مقررات بیمارستانی. البته این قواعد در بیمارستان‌ها تاحد زیادی به یکدیگر شباهت دارند و لذا درعمل این قواعد، ازپیش‌تعریف‌شده و ثابت هستند؛ امّا جهت افزایش انعطاف‌پذیری مدل، اختیار تغییر در این قواعد برای مدیر ارشد امنیتی در نظر گرفته شده است.

مدیر امنیتی بخش (DSO): با ورود هر بیمار لازم است اطلاعات مرتبط با بیمار در این مدل، توسط مدیر امنیتی بخش تعریف شود. همان‌طور که در تشریح فرآیندهای بیمارستانی در این مقاله آمده است، نقش مدیر امنیتی هر بخش در بیمارستان‌ها عموما به سرپرستار آن بخش واگذار می‌شود. به‌طور خلاصه اختیارات و وظایف مدیر ارشد امنیتی عبارتند از:

- ثبت اطلاعات بیمار (Patient) و ترجیحات حریم خصوصی وی (preferences).
- تعریف تیم پزشکی بیمار (hasTeam) و تعریف اعضای تیم پزشکی (inTeam).
- تعیین نقش عوامل بیمارستانی در تیم پزشکی بیمار (membership). البته عوامل بیمارستانی که طبق رابطه canAssign امکان مدیریت نقش آنها را دارد.

[DOI: 10.29252/jsdp.17.3.109]

- تعریف و حذف وکالت دسترسی (delegation) پس از طی فرآیند توصیف‌شده جهت اعطای وکالت و تأیید رییس بیمارستان.

۴- ارزیابی و مطالعه موردی

مدل ارایه‌شده از چند دیدگاه مورد ارزیابی قرار گرفته شده است. در ارزیابی یک مدل کنترل دسترسی در درجه نخست باید قدرت مدل در رفع نیازمندی‌های احصاشده برای محیط موردنظر و میزان پوشش انواع خط‌مشی‌های امنیتی در محیط مورد نظر را مورد ارزیابی قرار داد. آزمون توانمندی مدل در پشتیبانی از انواع سناریوهای دسترسی واقعی، رویکرد دوم در ارزیابی مدل‌های کنترل دسترسی است و درنهایت بررسی کاربردپذیری مدل درعمل با پیاده‌سازی یک سامانهٔ کنترل دسترسی بر اساس مدل پیشنهادی و ارزیابی زمان پاسخ در فرآیند کنترل دسترسی در سناریوهای واقعی، رویکرد سوم در ارزیابی مدل پیشنهادی است. در ادامه این بخش، نتایج حاصل از ارزیابی مدل بر اساس این سه رویکرد ارایه شده است.

(جدول-۲): ارزیابی کیفی مدل کنترل دسترسی پیشنهادی در قیاس با مدل‌های مشابه در سلامت الکترونیکی

(Table-2): Evaluation of the proposed access control model in comparison with related models in e-health

قابلیت‌های مدل / مدل کنترل دسترسی	مدل استفاده شده	آگاه از محیط	وکالت دسترسی	دسترسی اضطراری	انعطاف‌پذیری	حافظ حریم خصوصی
جرجیدیس و همکاران [16]	ترکیب RBAC و TMAC	✓	×	×	×	×
نرایانان [23]	TBAC	✓	✓	×	✓	×
جورجیکاکیس [18]	STEM-RBAC	✓	×	✓	×	✓
نی و همکاران [19]	P-RBAC	×	×	×	×	✓
یانگ و همکاران [20]	PBAC	×	×	×	×	✓
سیکورانزا و همکارش [8]	MPP-ABAC	×	×	×	✓	✓
گوپه و همکارش [22]	ترکیب MAC وRBAC	✓	×	✓	✓	×
خن و همکارش [13]	ترکیب DAC و RBAC	✓	✓	✓	✓	×
مدل پیشنهادی TbDAC	ترکیب RBAC، TBAC و PBAC	✓	✓	✓	✓	✓

۴-۱- ارزیابی کیفی مدل

ارزیابی کیفی مدل در قیاس با مدل‌های مشابه ارایه‌شده در جدول (۲) ارایه شده است. همان‌طورکه در این جدول آمده، مدل ارایه‌شده به‌گونه‌ای طراحی شده است که نیازمندهای مهم کنترل دسترسی در سلامت الکترونیکی را که در مدل‌های مشابه دیگر پوشش داده نشده بود، ارضا کند.

یکی از نکاتی که در نگاه نخست درخصوص این مدل قابل طرح است، رابطه آن با مدل‌های کلاسیک نقش‌مبنا است. گفتنی است که تعریف نقش در مدل مبتنی بر نقش (RBAC) با تعریف آن این مدل متفاوت است. درواقع در مدل $RBAC_0$، نقش شامل مجموعه از مجوزها (هر مجوز نمایان‌گر انجام عملیات بر روی منابع) است، درحالی‌که در مدل ارایه‌شده در این مقاله، نقش شامل مجموعه‌ای نوع‌مجوز (نمایان‌گر امکان انجام عملیات نوعی بر روی نوع‌منابع) است و فقط پس از عضویت یک عامل در تیم پزشکی یک بیمار، نوع‌مجوزهای مربوط به نقش‌های منتسب به عامل، بر اساس منابع اطلاعاتی مرتبط با بیمار موردنظر، به‌صورت مجموعه‌ای از مجوزها عینیت می‌یابد.

نکته قابل توجه دیگر آن است که از آنجایی که در کاربردهای واقعی به‌خصوص در محیط بیمارستانی به سلسله‌مراتب نقش‌ها توجه نمی‌شود؛ این مدل نیز بدون درنظرگرفتن سلسله‌مراتب نقش‌ها ارائه شده است. ضمن آن‌که وجود سلسله‌مراتب نقش‌ها با وجود قیدهای مختلف ناشی از لحاظ‌کردن شرایط زمینه‌ای و محدودیت‌های حریم خصوصی (به‌دلیل لزوم ارث‌بری محدودیت‌ها علاوه‌بر مجوزها در سلسله‌مراتب نقش‌ها)، پیچیدگی قابل توجهی را ایجاد می‌کند که درعمل کاربردی نیست؛ تأکید می‌شود که رعایت سادگی، در عین برخورداری از قدرت بیان مناسب از راه‌بردهای اصلی این پژوهشی به‌منظور کاربردی‌کردن عملی این مدل در کاربرد اینترنت اشیا در سلامت الکترونیکی بوده و لذا ارایه یک مدل قدرتمند ولی پیچیده مدنظر نبوده است.

گفتنی است که با درنظرگرفتن زمان و مکان بیمار و عامل بیمارستانی و همچنین اطلاعات حیاتی بدن بیمار برای

[DOI: 10.29252/jsdp.17.3.109]

تشخیص شرایط اضطراری در کنار لحاظ‌کردن محدودیت‌های مرتبط با حفظ حریم خصوصی بیمار در فرآیند کنترل دسترسی، می‌توان گفت که این مدل به‌لحاظ مفهومی اشتراکاتی با مدل $RBAC_2$ استاندارد دارد ولی به‌دلیل تفاوت مدل پیشنهادی با مدل $RBAC_2$ در مفهوم نقش و نوع محدودیت‌ها (که در مدل استاندارد محدود به محدودیت تفکیک وظایف است)، نمی‌توان مدل پیشنهادی را فقط توسعه‌ای ساده بر مدل $RBAC_2$ استاندارد در نظر گرفت. توجه کنید که ترکیب مفهوم نقش با مفهوم تیم در کنار محدودیت‌های ناشی از حفظ حریم خصوصی مبتنی بر هدفِ استفاده، نوآوری اصلی مدل پیشنهادی است که قابلیت‌های مناسبی را برای به‌کارگیری عملی آن در سلامت الکترونیکی به همراه داشته است.

۲-۴- آزمون مدل بر اساس سناریوهای دسترسی

برای این‌که کاربرد مدل کنترل دسترسی ارائه‌شده در محیط سلامت الکترونیکی سنجیده شود، لازم است، قواعد کنترل دسترسی در سناریوهای مختلف مورد آزمون قرار گیرد که بتوان مطمئن شد که مدل، همهٔ حالات مورد نظر را به‌صورت دقیق پشتیبانی می‌کند و می‌تواند نیازمندی درخواست‌دهندگان برای دسترسی به اطلاعات بیماران را برطرف کند. به‌همین منظور در این بخش به بررسی این سناریوها و کاربرد مدل ارائه‌شده در این موارد پرداخته شده است. گفتنی است که این سناریوها بر اساس قواعد کنترل دسترسی مدل $TbDAC_3$ بررسی شده‌اند و اثبات استنتاج این سناریوها در زبان پرولوگ با استفاده از ابزار مربوطه مورد بررسی قرار گرفته است.

این سناریوها بر اساس اطلاعات مربوط به یک بیمارستان است که مؤلفه‌های آن در زیر فهرست شده است:

- staff={ahmadi, salami, tahami, amiri, javadi}
- roles={Nurse, Doctor, heart specialist Doctor, General practitioner }
- patients={alavi, fathi, vahidi}
- locations={emergencyRoom, heartSection}
- teams={team3}
- res-Type={Test, I/O Sensor }
- res={Test alavi's Recored, Sensor fathi's Recored, Test vahidi's Recored }
- actions={read}
- assignedLocationP={(alavi, (emergencyRoom, rfid2)), (fathi, (emergencyRoom, rfid12)) }
- assignedLocationS={(ahmadi,(emergencyRoom, {rfid1,…, rfid9})), (salami, (emergencyRoom, {rfid1, rfid2, … , rfid10}))}
- hasRole={(ahmadi, Nurse), (salami, Doctor), (salami, General practitioner), (tahami, heart specialist Doctor)}
- role-Purpose={(Nurse, treatment), (Doctor, Emergency), (General practitioner, Emergency), (heart specialist Doctor, treatment)}
- hasTeam={(vahidi, Team3) }
- assignedPermission={(Nurse, Read, Test), (Doctor, Read, I/O Sensor), (heart specialist Doctor, Read, Test), (General practitioner, Read, Test)}
- hospPurpose={(Treatment, Test), (Emergency , I/O Sensor), (Emergency , Test)}
- preferences={(alavi, Test, Treatment), (fathi, I/O Sensor, Emergency), (vahidi, Test, Treatment), (vahidi, Test, Emergency)}

سناریوی نخست:

عامل بیمارستانی، احمدی یک پرستار است و در بخش اورژانس بیمارستان خدمت می‌کند؛ مجموعه تخت‌هایی که این عامل مسئول آنهاست به $rfid_1$ تا $rfid_9$ تجهیز شده‌اند. ساعت کاری احمدی از ساعت ۷ تا ۱۵ است. بیماری به نام علوی در بخش اورژانس و روی تختی با $rfid_2$ بستری است. احمدی درخواست دسترسی به نتایج آزمایش علوی را با هدف درمانی دارد. با توجه به اینکه ساعت فعلی ۹ است، با استفاده از اطلاعات اولیه آیا این درخواست دسترسی پذیرفته می‌شود یا خیر؟

- حقایق در زبان پرولوگ:

```
staff(ahmadi).
patient(alavi).
hasRole(ahmadi,nurse).
role_Purpose(nurse,treatment).
assignedLocationS(ahmadi,sl(emergencyRoom,[rfid
1,rfid2,rfid3,rfid4,rfid5,rfid6,rfid7,rfid8,rfi
d9])).
assignedLocationP(alavi,pl(emergencyRoom,rfid2)
).
isOwnedBy(test_alavi_Record,alavi).
type(test_alavi_Record,test).
hospPurpose(treatment,test).
preference(alavi,test,treatment).
assignedPermission(nurse,read,test).
timeTask(ahmadi,7,15).
currentTime(9).
```

- قواعد کنترل دسترسی مورد نیاز:

```
insubset(pl(Ls,Y),sl(Lp,L)):-
    Ls=Lp,
    member(Y,L).
assign(P,S):-
    patient(P),
    staff(S),
    assignedLocationP(P,PL),
    assignedLocationS(S,SL),
    insubset(PL,SL).
canAccessP(S,A,Res,Pu):-
    assign(P,S),
    currentTime(T),
    timeTask(S,T1,T2),
    T1=<T,
    T=<T2,
    isOwnedBy(Res,P),
    type(Res,Res_type),
    hasRole(S,R),
    role_Purpose(R,Pu),
    hospPurpose(Pu,Res_type),
    preference(P,Res_type,Pu),
    assignedPermission(R,A,Res_type).
```


[DOI: 10.29252/jsdp.17.3.109]

با استفاده از حقایق بالا و قواعد کنترل دسترسی در بخش اورژانس و در شرایط عادی، نتایج زیر استنتاج می‌شود:

طبق مسند InSubset رابطه (۱) از آنجایی‌که مکان علوی و احمدی یکسان است و rfid منتسب به علوی عضو مجموعهٔ rfidهای تحت مسئولیت احمدی است، علوی تحت نظر احمدی قرار می‌گیرد (رابطه ۲).

$$\text{InSubset}((\text{emergencyRoom}, \text{rfid}_2), (\text{emergencyRoom}, \{\text{rfid}_1, \text{rfid}_2, \dots, \text{rfid}_9\}))$$
$$\text{Assign}(\text{alavi}, \text{ahmadi})$$

با توجه به اطلاعات موجود و قاعدهٔ دسترسی رابطه (۳) استنتاج می‌شود که نتایج آزمایش علوی با هدف درمانی در اختیار احمدی قرار می‌گیرد.

```
?- canAccessP(ahmadi,read,test_alavi_Record,treatment).
true .
```

سناریوی دوم:

عامل بیمارستانی سلامی با نقش پزشک در بخش اورژانس حضور دارد. مجموعه تخت‌هایی که این عامل مسئول آنها است به $rfid_1$ تا $rfid_{10}$ تجهیز شده‌اند. ساعت کاری سلامی از ساعت ۷ تا ۱۵ اما این پزشک ۲۴ ساعته اجازهٔ دسترسی به اطلاعات مجازش را دارد. بیماری به نام فتحی در بخش اورژانس و روی تختی با $rfid_{12}$ بستری است. شرایط فتحی اضطراری است. سلامی درخواست دسترسی به اطلاعات حس‌گرهای متصل به فتحی را با هدف درمانی (در شرایط اضطراری) دارد. با توجه به اینکه ساعت فعلی ۱۱ است، با استفاده از اطلاعات اولیه آیا این درخواست دسترسی پذیرفته می‌شود یا خیر؟

فرض کنید که با توجه به اطلاعات دریافتی از حسگرهای متصل به بیمار شامل فشار خون (زیر ۷) و ضربان قلب (زیر ۳۵) و قواعد شرایط اضطراری استنتاج می‌شود که بیمار در شرایط اضطراری است و لذا IsEmergency(fathi) برقرار است.

با این اوصاف بر اساس اطلاعات موجود، حقایق زیر در پایگاه دانش امنیتی برقرار است:

■ حقایق در زبان پرولوگ:

```
staff(salami).
patient(fathi).
rfid(rfid12,salami).
assignedRFID(fathi,rfid12).
hasRole(salami,doctor).
role_Purpose(doctor,emergency).
assignedLocationS(salami,sl(emergencyRoom,[rfid1
,rfid2,rfid3,rfid4,rfid5,rfid6,rfid7,rfid8,rfid9
,rfid10])).
assignedLocationP(fathi,pl(emergencyRoom,rfid12)
).
isOwnedBy(sensor_fathi_Record,fathi).
isEmergency(fathi).
type(sensor_fathi_Record,i/o_Sensor).
hospPurpose(emergency,i/o_Sensor).
preference(fathi,i/o_Sensor,emergency).
assignedPermission(doctor,read,i/o_Sensor).
timeTask(salami,0,24).
pRequest(salami,read,sensor_fathi_Record,emergen
cy).
currentTime(11).
```

■ قواعد کنترل دسترسی مورد نیاز:

```
canAccessP(S,A,Res,Pu):-
    pRequest(S,A,Res,Pu),
    currentTime(T),
    timeTask(S,T1,T2),
    T1=<T,
    T=<T2,
    isOwnedBy(Res,P),
    type(Res,Res_type),
    rfid(RFID,S),
    assignedRFID(P,RFID),
    isEmergency(P),
    hasRole(S,R),
    role_Purpose(R,Pu),
    hospPurpose(Pu,Res_type),
    preference(P,Res_type,Pu),
    assignedPermission(R,A,Res_type).
```

با استفاده از حقایق بالا و قواعد کنترل دسترسی در اورژانس در شرایط اضطراری رابطه (۴)، استنتاج می‌شود که اطلاعات دریافتی از حس‌گرهای متصل به فتحی می‌تواند با هدف اضطراری در اختیار سلامی قرار گیرد.

```
?- canAccessP(salami,read,sensor_fathi_Record,emergency).
true.
```

سناریوی سوم:

عامل بیمارستانی تهامی با نقش پزشک متخصص قلب در یکی از بخش‌های اصلی بیمارستان حضور دارد. تیم پزشکی مربوط به بیمار وحیدی team3 است. دکتر تهامی در team3 عضو بوده و نقش پزشک متخصص را در این تیم دارد. دکتر تهامی اجازه دسترسی به اطلاعات مجازش را به‌صورت ۲۴ ساعته دارد. اگر دکتر تهامی درخواست دسترسی به نتایج آزمایش‌های وحیدی را با هدف درمانی داشته باشد، با توجه به اینکه ساعت فعلی ۱۱ است، با استفاده از اطلاعات اولیه آیا این درخواست دسترسی پذیرفته می‌شود یا خیر؟

■ حقایق در زبان پرولوگ:

```
staff(tahami).
patient(vahidi).
hasTeam(vahidi,team3).
membership(tahami,team3,heart_specialist_
Doctor).
role_Purpose(heart_specialist_Doctor,trea
tment).
isOwnedBy(test_vahidi_Record,vahidi).
type(test_vahidi_Record,test).
hospPurpose(treatment,test).
preference(vahidi,test,treatment).
assignedPermission(heart_specialist_Docto
r,read,test).
timeTask(tahami,0,24).
currentTime(11).
```


[DOI: 10.29252/jsdp.17.3.109]

```
staff(tahami).
staff(amiri).
patient(vahidi).
delegate(tahami,amiri,heart_specialist_Do
ctor,team3,date(97,5,30),date(97,6,6)).
hasTeam(vahidi,team3).
hasRole(tahami,heart_specialist_Doctor).
isOwnedBy(test_vahidi_Record,vahidi).
type(test_vahidi_Record,test).
rolePurpose(heart_specialist_Doctor,treat
ment).
hospPurpose(treatment,test).
preference(vahidi,test,treatment).
assignedPermission(heart_specialist_Docto
r,read,test).
currentDate(date(97,6,4)).
currentTime(12).
timeTask(amiri,0,24).
```

- قواعد کنترل دسترسی مورد نیاز:

```
membership(S,Tm,R):-
    delegate(S2,S,R,Tm,D1,D2).

isMemberOfTeam(S,P):-
    patient(P),
    hasTeam(P,Tm),
    membership(S,Tm,R).


canAccessP(S,A,Res,Pu):-
    isMemberOfTeam(S,P),
    currentTime(T),
    timeTask(S,T1,T2),
    T1=<T,
    T=<T2,
    isOwnedBy(Res,P),
    type(Res,Res_type),
    hasTeam(P,Tm),
    membership(S,Tm,R),
    rolePurpose(R,Pu),
    hospPurpose(Pu,Res_type),
    preference(P,Res_type,Pu),
    assignedPermission(R,A,Res_type).
```

با استفاده از حقایق بالا و قواعد کنترل دسترسی در بخش اصلی در شرایط عادی و درحالتی‌که یک عامل بیمارستانی به عامل بیمارستانی دیگر نقش خود را واگذار کرده، نتایج زیر استنتاج می‌شود.

طبق مسند Delegate رابطه (۷)، از آنجایی‌که دکتر تهامی نقش پزشک متخصص قلب را در تیم سه به دکتر امیری واگذار کرده و تاریخ کنونی بین تاریخ شروع و پایان این وکالت است؛ پس دکتر امیری این نقش را در تیم سه عهده‌دار می‌شود. همچنین از آنجایی‌که این عضویت استنتاج شد و وحیدی نیز عضو تیم سه است، پس طبق رابطه (۸) نتیجه می‌شود امیری در تیم پزشکی وحیدی است.

Membership (amiri, $Team_3$, heart specialist Doctor)

IsMemberOfTeam (amiri, vahidi)

حال با توجه به اطلاعات موجود و قاعدهٔ دسترسی رابطه (۹) استنتاج می‌شود که نتایج آزمایش وحیدی با هدف درمانی در اختیار امیری می‌تواند قرار بگیرد.

- قواعد کنترل دسترسی مورد نیاز:

```
isMemberOfTeam(S,P):-
    patient(P),
    hasTeam(P,Tm),
    membership(S,Tm,R).


canAccessP(S,A,Res,Pu):-
    isMemberOfTeam(S,P),
    isOwnedBy(Res,P),
    type(Res,Res_type),
    hasTeam(P,Tm),
    membership(S,Tm,R),
    role_Purpose(R,Pu),
    hospPurpose(Pu,Res_type),
    preference(P,Res_type,Pu),
    currentTime(T),
    timeTask(S,T1,T2),
    T1=<T,
    T=<T2,
    assignedPermission(R,A,Res_type).
```

با استفاده از حقایق بالا و قواعد کنترل دسترسی در بخش اصلی در شرایط عادی، نتایج زیر استنتاج می‌شود.

طبق مسند IsMemberOfTeam رابطه (۵)، از آنجایی که تیم مربوط به وحیدی team3 است و دکتر تهامی نیز در این تیم سه نقش پزشک متخصص را دارد، پس دکتر تهامی در تیم پزشکی وحیدی است.

IsMemberOfTeam (tahami, vahidi)

با توجه به اطلاعات موجود و قاعدهٔ دسترسی رابطه (۶) استنتاج می‌شود که نتایج آزمایش وحیدی با هدف درمانی در اختیار تهامی قرار می‌گیرد.

```
?- canAccessP(tahami,read,test_vahidi_Record,treatment).
true.
```

سناریوی چهارم:

عامل‌های بیمارستانی تهامی و امیری در یکی از بخش‌های اصلی بیمارستان حضور دارند. اطلاعات مانند سناریوی قبل است. دکتر تهامی از تاریخ ۱۳۹۷/۵/۳۰ تا تاریخ ۱۳۹۷/۶/۶ مرخصی گرفته و در بیمارستان حضور ندارد. این پزشک نقش خود را در team3 به دکتر امیری وکالت داده است. با توجه به این‌که دکتر تهامی اجازهٔ دسترسی به اطلاعات مجازش را به‌صورت ۲۴ ساعته داشت، دکتر امیری نیز این اجازه را دارد. اگر دکتر امیری درخواست دسترسی به نتایج آزمایش‌های وحیدی را با هدف درمانی داشته باشد، با توجه به این‌که ساعت فعلی ۱۲ مورخ ۱۳۹۷/۶/۴ است، با استفاده از اطلاعات اولیه آیا این درخواست دسترسی پذیرفته می‌شود؟

- حقایق در زبان پرولوگ:

[DOI: 10.29252/jsdp.17.3.109]

[DOI: 10.29252/jsdp.17.3.109]

```
?- canAccessP(amiri,read,test_vahidi_Record,treatment).
true.
```

سناریوی پنجم:

عامل بیمارستانی جوادی با نقش پزشک عمومی در یکی از بخش‌های اصلی بیمارستان حضور دارد. ساعت کاری دکتر جوادی از ۱۵:۳۰ تا ۰۰:۳۰ است. وضعیت بیمار وحیدی اضطراری است. دکتر جوادی در نزدیکی بیمار است و از طریق RFID reader برچسب RFID منتسب به بیمار وحیدی را می‌خواند. با توجه به اینکه ساعت فعلی هجده است، اگر دکتر جوادی درخواست دسترسی به نتایج آزمایش وحیدی را داشته باشد، با استفاده از اطلاعات اولیه آیا این درخواست دسترسی پذیرفته می‌شود؟

- حقایق در زبان پرولوگ:

```
staff(javadi).
patient(vahidi).
rfid(rfid45,javadi).
assignedRFID(vahidi,rfid45).
isOwnedBy(test_vahidi_Record,vahidi).
type(test_vahidi_Record,test).
isEmergency(vahidi).
hasRole(javadi,general_practitioner).
rolePurpose(general_practitioner,emergenc
y).
hospPurpose(emergency,test).
preference(vahidi,test,emergency).
assignedPermission(general_practitioner,r
ead,test).
pRequest(javadi,read,test_vahidi_Record,e
mergency).
timeTask(javadi,15,24).
currentTime(18).
```

- قواعد کنترل دسترسی مورد نیاز:

```
canAccessP(S,A,Res,Pu):-
    pRequest(S,A,Res,Pu),
    isOwnedBy(Res,P),
    type(Res,Res_type),
    rfid(RFID,S),
    assignedRFID(P,RFID),
    isEmergency(P),
    hasRole(S,R),
    rolePurpose(R,Pu),
    hospPurpose(Pu,Res_type),
    preference(P,Res_type,Pu),
    currentTime(T),
    timeTask(S,T1,T2),
    T1=<T,
    T=<T2,
    assignedPermission(R,A,Res_type).
```

با استفاده از حقایق بالا و قواعد کنترل دسترسی در بخش اصلی در شرایط اضطراری رابطه (۱۰)، نتایج آزمایش وحیدی در شرایط اضطرری در اختیار جوادی قرار می‌گیرد.

```
?- canAccessP(javadi,read,test_vahidi_Record,emergency).
true.
```

سناریوی ششم:

عامل بیمارستانی تهامی در بخش اصلی قرار دارد. اگر تهامی برچسب RFID منتسب به وحیدی را بخواند به این معنا است که تهامی در نزدیکی وحیدی قرار دارد. حال اگر تهامی در تیم پزشکی وحیدی باشد، اطلاعات مورد نیاز با توجه به نقش تهامی در تیم پزشکی، خط‌مشی‌های بیمارستان و ترجیحات بیمار وحیدی، در دسترس تهامی می‌تواند قرار گیرد.

- حقایق در زبان پرولوگ:

```
staff(tahami).
patient(vahidi).
rfid(rfid45,tahami).
assignedRFID(vahidi,rfid45).
isMemberOfTeam(tahami,vahidi).
hasTeam(vahidi,team3).
membership(tahami,team3,heart_specialist_
Doctor).
isOwnedBy(test_vahidi_Record,vahidi).
type(test_vahidi_Record,test).
rolePurpose(heart_specialist_Doctor,treat
ment).
hospPurpose(treatment,test).
preference(vahidi,test,treatment).
assignedPermission(heart_specialist_Docto
r,read,test).
timeTask(tahami,0,24).
currentTime(13).
```

- قواعد کنترل دسترسی مورد نیاز:

```
fetch(S,A,Res,Pu):-
    rfid(RFID,S),
    assignedRFID(P,RFID),
    isMemberOfTeam(S,P),
    currentTime(T),
    timeTask(S,T1,T2),
    T1=<T,
    T=<T2,
    isOwnedBy(Res,P),
    type(Res,Res_type),
    hasTeam(P,Tm),
    membership(S,Tm,R),
    rolePurpose(R,Pu),
    hospPurpose(Pu,Res_type),
    preference(P,Res_type,Pu),
    assignedPermission(R,A,Res_type).
```

با استفاده از حقایق بالا و قواعد کنترل دسترسی در بخش اصلی در شرایط عادی رابطه (۱۱)، نتیجهٔ زیر استنتاج می‌شود.

```
?- fetch(tahami,read,test_vahidi_Record,treatment).
true.
```

۳-۴- پیاده‌سازی سامانه کنترل دسترسی و ارزیابی تجربی

پیاده‌سازی سامانه کنترل دسترسی بر اساس مدل پیشنهادی به زبان اندروید در محیط اندرویداستودیو (Android Studio) و با استفاده از ابزار جنی‌موشن (Genymotion) انجام شده و درنهایت یک برنامه‌کاربردی به نام سیستم پروندهٔ الکترونیکی سلامت بیمارستان ایجاد شده است.

استفاده از این سامانه در مطالعه موردی و سناریوهای اشاره‌شده در بخش قبل نشان می‌دهد که مدل پیشنهادی TbDAC قادر است در محیط واقعی بیمارستانی، نسبت به مدل‌های پیشین([28]) ارائه‌شده، نیازمندی‌های بیشتری را پوشش دهد. در این مدل زمانی که بیمار در شرایط اضطراری قرار می‌گیرد، عامل بیمارستانی نزدیک بیمار با توجه به نقش خود حتی اگر عضو تیم پزشکی بیمار نباشد، با حفظ حریم خصوصی بیمار به اطلاعات مورد نیاز برای درمان فوری و بازگرداندن بیمار به شرایط عادی دست می‌یابد. درواقع وکالتی پویا به عامل بیمارستانی داده می‌شود. همچنین پزشکانی که مسئول بیمار هستند به‌صورت شبانه‌روزی اجازهٔ دسترسی به اطلاعات بیماران را دارند و اگر نزدیک بیمار باشند با استفاده از برچسب RFID متصل به بیمار، زمان شناسایی او را به کمینه رسانده و سریع‌تر به درمان بیمار می‌پردازند که این مورد در مدل‌های پیشین درنظر گرفته نشده بود.

زمان پاسخ به درخواست عامل بیمارستانی در اجرای هرکدام از این سناریوها در سامانه پیاده‌سازی‌شده در نمودار شکل (۱۲) قابل مشاهده است. در این نمودار با افزایش تعداد درخواست‌ها، زمان پاسخ نیز افزایش می‌یابد.

(شکل-۱۲): نتیجه ارزیابی زمان پاسخ به درخواست‌ها
(Figure-12): Evaluation of response times of requests

۵- نتیجه‌گیری

گسترش استفاده از فناوری‌های نوین و به‌طور خاص اینترنت اشیا در حوزه سلامت الکترونیکی با مسائل مختلفی روبه‌رو است که از مهم‌ترین آنها مسأله امنیت و کنترل دسترسی است.

نیازمندی‌های امنیتی مختلفی در سلامت الکترونیکی مطرح است که از مهم‌ترین آنها حفظ حریم خصوصی بیماران و دسترسی کنترل‌شده و در عین حال پویا به اطلاعات سلامت آنها طبق شرایط بیمار است؛ به‌طوری‌که دسترسی افراد بسته به اینکه بیمار در شرایط اضطراری باشد یا نباشد و بسته به اینکه فرد متقاضی دسترسی دارای چه نقشی در ارتباط با بیمار باشد و چه هدفی را در دسترسی به اطلاعات بیمار داشته باشد، باید به‌صورت انعطاف‌پذیر و پویا تعیین شود.

در این پژوهش با تحلیل نیازمندی‌های مختلف موردنیاز در حوزه سلامت الکترونیکی (بر اساس اطلاعات جمع‌آوری‌شده از چند بیمارستان بزرگ کشور) مشخص شد که مدل‌های ارایه‌شده تاکنون در حوزه سلامت الکترونیکی و زمینه‌های مشابه، توانایی ارضای تمام نیازمندی‌های مطرح‌شده در کنترل دسترسی به اطلاعات بیماران را ندارند. به‌همین دلیل در این مقاله یک مدل کنترل دسترسی با قابلیت‌های مهمی همچون حفظ حریم خصوصی، اعطای وکالت دسترسی و دسترسی در شرایط اضطراری پیشنهاد شد. در این مدل به هر نقش بیمارستانی مجموعه‌ای از نوع‌مجوزها اعطا می‌شود و سپس بسته به اینکه عامل بیمارستانی در تیم پزشکی یا مسئول مستقیم چه بیماری باشد، مجوز دسترسی به اطلاعات سلامت الکترونیکی آن بیمار (از جمله اطلاعات انواع حس‌گرهای متصل به بیمار، آزمایش‌ها، سوابق پزشکی و فرآیند درمانی به‌عمل آمده) بر اساس نوع‌مجوزهای نقش منتسب به وی، اعطا می‌شود. حفظ حریم خصوصی بیمار در این مدل بر اساس ترجیحات بیمار (که در زمان پذیرش بیمار از وی اخذ شده است) و اهداف دسترسی عوامل بیمارستانی و همچنین سیاست‌های کلان بیمارستان درخصوص حریم خصوصی بیماران کنترل می‌شود. دسترسی وکالتی به اطلاعات بیماران (به‌طور مثال درصورت عدم حضور پزشک اصلی) و دسترسی بی قید و شرط موقت در شرایط اضطراری نیز از خصوصیات دیگر مدل پیشنهادی است که با ایجاد پویایی در مدل، عدم توقف فرآیندهای درمانی را در شرایط مختلف با حفظ بیشینه‌ای سیاست‌های دسترسی و حریم خصوصی ممکن می‌سازد.

ارزیابی کیفی به‌عمل‌آمده از مدل و بررسی سناریوهای واقعی در یک مطالعه موردی نشان از کارایی مناسب مدل در برآورده‌سازی نیازهای امنیتی و کنترل دسترسی در کاربردهای واقعی دارد. در این پژوهش یک پیش‌نمونه از سامانه کنترل دسترسی مبتنی بر مدل پیشنهادی در دستگاه‌های همراه اندرویدی نیز طراحی و پیاده‌سازی شد و زمان‌های پاسخ سامانه بر اساس سناریوهای مطرح در مطالعه موردی، مورد اندازه‌گیری قرار گرفت. زمان پاسخ اندازه‌گیری‌شده در حدود یک ثانیه و یا کمتر بوده که با توجه به توان پردازشی پایین دستگاه‌های همراه، زمان

[DOI: 10.29252/jsdp.17.3.109]

بسیار مناسبی محسوب می‌شود. البته باید توجه داشت که پیاده‌سازی کامل یک سامانه کنترل دسترسی در محیط واقعی نیازمند بهره‌گیری از زیرساخت کلید عمومی (PKI) و زیرساخت مدیریت مجوزها (PMI) برای صدور و وارسی گواهی‌های نقش‌ها (به‌طور مثال گواهی دیجیتالی طبابت یا پرستاری از سوی وزارت بهداشت) و وکالت‌های الکترونیکی (رسمی و حقوقی) قابل اعطا در این مدل است. ارایه یک طرح عملیاتی مناسب بر اساس این دو زیرساخت با توجه به ساختار نظام بهداشت، درمان و آموزش پزشکی در کشور می‌تواند در ادامه این پژوهش در آینده مدنظر قرار گیرد.

6- References ۶- مراجع

[1] I. B. Ida, A. Jemai, and A. Loukil, "A survey on security of IoT in the context of ehealth and clouds," *in Proceedings of 11th International Design Test Symposium (IDT)*, pp.25–30, Dec2016.

[2] A. J. Jara, A. F. Alcolea, M. A. Zamora, A. F. G. Skarmeta, and M. Alsaedy, "Drugs interaction checker based on iot," *in Proceedings of 2010 Internet of Things (IOT)*, pp.1–8, Nov2010.

[3] A, Kevin, "That 'internet of things' thing," *RFID journal*, vol. 22, pp.97-114, Jul2009.

[4] D.Lu and T.Liu, "The application of iot in medical system," *in Proceedings of 2011 IEEE International Symposium on IT in Medicine and Education*, vol.1, pp.272–275, Dec2011.

[5] R. Marti, J. Delgado, and X. Perramon, "Security specification and implementation for mobile e-health services," *in Proceedings of 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service*, March.2004, pp.241–248.

[6] F. Rezaeibagha and Y. Mu, "Distributed clinical data sharing via dynamic access-control policy transformation," *International Journal of Medical Informatics*, vol.89, no.Supplement C, pp.25–31, 2016.

[7] I. Iakovidis, "Towards Personal Health Record: Current Situation, Obstacles and Trends in Implementation of Electronic Healthcare Record in Europe," *International Journal of Medical Informatics*, vol.52, pp.105-115, 1998.

[8] M.Sicuranza, A.Esposito, and M.Ciampi, "A view-based access control model for her systems," *in Proceedings of Intelligent Distributed Computing VIII*, pp.443 452, Springer, 2015.

[9] M. Abomhara, H. Yang, G. M. Køien, and M. B. Lazreg, "Work-based access control model for cooperative healthcare environments: Formal specification and verification," *Journal of Healthcare Informatics Research*, vol.1, pp.19–51, Jun2017.

[10] H. S. G. Pussewalage and V. A. Oleshchuk, "An attribute based access control scheme for secure sharing of electronic health records," *in Proceedings of 18th IEEE International Conference on e-Health Networking*, Applications and Services (Healthcom), Sept.2016, pp.1–6.

[11] M.Sicuranza and A.Esposito, "An access control model for easy management of patient privacy in her systems," *in Proceedings of 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, Dec.2013, pp.463–470.

[12] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, "Access control in the internet of things: Big challenges and new opportunities," *Computer Networks*, vol.112, no.Supplement C, pp.237–262, 2017.

[13] M.F.F.Khan and K.Sakamura, "A secure and flexible e-health access control system with provisions for emergency access overrides and delegation of access privileges," *in Proceedings of 18th International Conference on Advanced Communication Technology (ICACT)*, pp.541–546, Jan2016.

[14] M. Jayabalan and T. O'Daniel, "Access control and privilege management in electronic health record: a systematic literature review," *Journal of Medical Systems*, vol.40, p.261, Oct2016.

[15] M.F.F.Khan and K.Sakamura, "Context-aware access control for clinical information systems," *in Proceedings of 2012 International Conference on Innovations in Information Technology (IIT)*, March.2012, pp.123–128.

[16] C. K. Georgiadis, I. Mavridis, G. Pangalos, and R. K. Thomas, "Flexible team-based access control using contexts," *in Proceedings of the Sixth ACM Symposium on Access Control Models and Technologies, SACMAT'01*, (NewYork, NY, USA), pp.21–27, 2001.

[17] M. Yarmand, K. Sartipi, and D. Down, "Behavior-based access control for distributed healthcare environment," *in Computer-Based Medical Systems, 2008. CBMS'08. 21st IEEE International Symposium on*, pp.126–131, June2008.

[18] E. Georgakakis, S. Nikolidakis, D. Vergados, and C. Douligeris, "Spatio temporal emergency role based access control (stem-rbac): A time and location aware role based access control model with a break the glass mechanism," *in Computers and Communications (ISCC): 2011 IEEE Symposium on*, pp. 764–770, June2011.

[19] Q.Ni, A.Trombetta, E.Bertino, andJ.Lobo, "Privacy-aware role based access control, " *in*

[DOI: 10.29252/jsdp.17.3.109]

Proceedings of 12th ACM Symposium on Access Control Models and Technologies, SACMAT '07, pp.41–50, ACM, 2007.

[20] N. Yang, H. Barringer, and N. Zhang, "A purpose-based access control model," *in Proceedings of Third International Symposium on Information Assurance and Security,* pp.143–148, Aug2007.

[21] K. Seol, Y.-G. Kim, E. Lee, Y.-D. Seo, and D.-K. Baik, ''Privacy preserving attribute-based access control model for XML-based electronic health record system,'' *IEEE Access*, vol. 6, pp. 9114–9128, 2018.

[22] Majeed, Abdul, "Attribute-centric anonymization scheme for improving user privacy and utility of publishing e-health data," *Journal of King Saud University-Computer and Information Sciences*, March 2018.

[23] P.Gope and R.Amin, "A novel reference security model with the situation based access policy for accessing ephr data," *Journal of Medical Systems*, vol.40, p.242, Sep2016.

[24] H. Narayanan and M. Giine, "Ensuring access control in cloud provisioned healthcare systems," *in Consumer Communications and Networking Conference (CCNC): 2011 IEEE*, Jan.2011, pp.247–251.

[25] US Department of Health and Human Services, "Public Law 104-191: Health Insurance Portability and Accountability Act of 1996," Retrieved November 24 (2003): 2003.

[26] J. Jing, A. Gail-Joon, H. Hongxin, J. Michael, and Z.Xinwen, "Patient-centric authorization framework for electronic healthcare services," *computers & security*, vol.30, no.2-3, pp.116-127, 2011.

[27] M.A. Doostari, M. Miabi, and M. Momeni, "Proposing a privacy and anonymity protocol in ehealth using public key infrastructure", *in Proceedings of the 4th International Conference on Applied Research in Computer Engineering and Signal Processing,* Tehran, Iran, 2016.

[۲۷] دوستاری، محمدعلی؛ مریم میابی جغال و مسعود مومنی تزنگی، ۱۳۹۵، ارایه پروتکل حفظ حریم خصوصی و گمنامی در سلامت الکترونیک با استفاده از زیرساخت کلید عمومی، چهارمین کنفرانس بین المللی پژوهش های کاربردی درمهندسی کامپیوتر و پردازش سیگنال، تهران، دانشگاه صنعتی مالک اشتر - دانشگاه شهید بهشتی.

[28] F. hashemibeni, "Privacy preserving access control in iot for ehealth," Master's thesis, Sharif University of Technology, September 2015.

فائقه غفرانی مدرک کارشناسی خود را در سال ۱۳۹۳ در رشته علوم رایانه از دانشگاه خوارزمی تهران و مدرک کارشناسی ارشد خود را در سال ۱۳۹۷ در رشته مهندسی فناوری اطلاعات گرایش شبکه‌های رایانه‌ای از دانشگاه صنعتی شریف دریافت کرد. حوزه‌های تخصصی ایشان کنترل دسترسی و اینترنت اشیا است.

نشانی رایانامه ایشان عبارت است از:
ghofrani@ce.sharif.edu

مرتضی امینی دکترای تخصصی خود را در رشته مهندسی رایانه گرایش نرم‌افزار از دانشگاه صنعتی شریف در سال ۱۳۸۹ دریافت کرد. ایشان در حال حاضر دانشیار دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف و زمینه‌های پژوهشی ایشان امنیت پایگاه داده و کنترل دسترسی، روش‌های صوری و منطق در امنیت اطلاعات، تشخیص نفوذ و همبسته‌سازی هشدار و کنترل جریان اطلاعات در اندروید است. از جمله افتخارات ایشان می‌توان به انتخاب ایشان به‌عنوان استاد برتر آموزشی دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف در سال ۱۳۹۵ و استاد برتر پژوهشی این دانشکده در سال ۱۳۹۶ و اجرای چندین طرح کلان ملی پژوهشی اشاره کرد.

نشانی رایانامه ایشان عبارت است از:
amini@sharif.edu

[DOI: 10.29252/jsdp.17.3.109]