УДК 004.056

В. М. Клиш
Ю. В. Баришев

АНАЛІЗ МОЖЛИВОСТЕЙ НЕКЛАСИЧНИХ МОДЕЛЕЙ РОЗМЕЖУВАННЯ ПРАВ ДОСТУПУ ДЛЯ ЗАХИСТУ МЕДИЧНИХ ДАНИХ

Вінницький національний технічний університет

Анотація

У роботі проаналізовано некласичні моделі розмежування прав доступу для медичних даних. Досліджено особливості некласичних моделей розмежування прав доступу у контексті їхнього застосування у медичних закладах. Розглянуто такі вимоги до захисту медичних даних, як рівень конфіденційності, цілісність, протидія внесенню дезінформації та гнучкість у керуванні доступом. Результати аналізу дозволяють визначити перспективність застосування кожної моделі у контексті медичних інформаційних систем.

Робота спрямована на визначення найкращого підходу до забезпечення безпеки медичних даних, що може сприяти подальшому вдосконаленню інформаційних систем у сфері охорони здоров'я.

Ключові слова: розмежування прав доступу, порівняльний аналіз, медичні дані, кібербезпека, захист даних.

Abstract

The non-classical models of access control for medical data are analyzed in this research. Special features of non-classical models access control in the context of their application in medical institutions are investigated. The requirements for the medical data protection such as the level of confidentiality, integrity, disinformation resilience and flexibility are considered for the task. Results of these analyses allow us to determine the prospects of each model application in the field of healthcare information systems.

The work is aimed to determine the best approach to ensure the medical data security, which can contribute to the further improvement of healthcare information systems.

Keywords: access control, comparative analysis, medical data, cybersecurity, data protection.

Вступ

Розмежування прав доступу в інформаційних системах виступає ключовим інструментом для забезпечення конфіденційності, надаючи доступ лише тим, хто має необхідні права.

У цьому контексті нестандартні моделі розмежування прав доступу, які можуть бути ефективними в інших галузях, недостатньо досліджені щодо застосування в галузі медицини. Відповідно актуально виконати їх аналіз та визначити межі їх потенційного застосування для захисту даних у медичній галузі.

Метою роботи є покращення рівня захисту приватності медичних даних.

Для досягнення мети було розв’язано такі завдання: проаналізовано нестандартні моделі розмежування прав доступу; визначено критерії порівняння; виконано порівняльний аналіз та обґрунтування вибору найкращого варіанту для захисту медичних даних.

Результати дослідження

В медичній галузі безпека та конфіденційність даних є критичними аспектами, які вимагають ретельного та гнучкого управління доступом. Для цього використовуються різні моделі розмежування прав доступу, які розроблені з метою ефективного контролю над доступом до медичної інформації. Однак, не всі моделі пасують медичній галузі через її особливості.

Серед моделей варто виділити такі моделі розмежування прав доступу: ABAC (Attribute-Based Access Control) [1], OrBAC (Organization-Based Access Control) [2], CBAC (Context-Based Access Control) [3] та TMAC (Team-Based Access Control) [4]. Кожна з цих моделей має свої особливості та переваги, але водночас мають обмеження, які ускладнюють їх застосування у медичних системах.

За допомогою моделі ABAC [1], доступ до об'єктів контролюється шляхом оцінки правил на основі атрибутів сутностей (суб'єкта і об'єкта), дій та оточення, що стосуються запиту. У цій моделі реалізовані два типи атрибутів: на основі дій та на основі середовища. Атрибути на основі дій регулюють доступ користувачів до ресурсів в залежності від їх дій, таких як читання, запис, видалення тощо.

Атрибути на основі середовища враховують умови, такі як час доби, місцезнаходження, стан системи тощо, для визначення можливості доступу користувача до ресурсів у певних умовах.

Модель ABAC базується на атрибутах сутностей та умовах, а не на попередньо визначених ролях чи групах користувачів. Такий підхід дозволяє більш гнучко контролювати доступ до ресурсів, враховуючи різні умови та контекст використання.

Використовуючи заздалегідь визначені атрибути, ABAC уникає потреби у безпосередньому призначенні дозволів користувачам. Крім того, суб'єкт може автентифікуватися в одній медичній установі та, за потреби, мати змогу отримати доступ до ресурсів в іншій медичній установі. Наприклад, якщо пацієнт отримав направлення на консультацію у одній медичній установі, його атрибути, такі як ім'я, медична історія та призначення, можуть бути автоматично передані до іншої медичної установи, де може знадобитися подальше обстеження чи лікування. При переході до цієї іншої установи, пацієнт може пройти автентифікацію за допомогою своїх вже наявних атрибутів, що спростить процес отримання медичних послуг та забезпечить безперешкодний перехід між медичними установами.

Модель OrBAC [2] використовує абстрактні концепції, такі як організації, ролі, дії та об'єкти, що робить її дуже гнучкою та масштабованою. Крім того, підтримує ієрархічну структуру організацій та ролей, що дозволяє легко впорядковувати та керувати правами доступу у великих та складних системах. Політика безпеки встановлюється окремо для кожної організації. Завдяки своїм особливостям OrBAC може ефективно використовуватися в різноманітних галузях, де потрібно враховувати різні фактори та умови для встановлення прав доступу.

Підтримка ієрархічної структури організацій та ролей спростить управління доступом до медичних даних та ресурсів. Крім того, можливість встановлення політик безпеки для кожної організації дозволить враховувати специфічні потреби кожної лікарні і забезпечити високий рівень конфіденційності та безпеки медичної інформації. Проте, OrBAC зазвичай не має можливості динамічно змінювати права доступу в залежності від часу або місцезнаходження. У цій моделі доступ до інформації зазвичай визначається на основі ролі, яку виконує користувач, і його привілеїв, а не на основі часу. Таким чином, якщо лікар має відповідні права доступу, він зможе будь-коли редагувати інформацію.

Context-Based Access Control (CBAC) [3] – це розширення традиційних методів контролю доступу, таких як контроль доступу на основі ролей (RBAC) і контроль доступу на основі атрибутів (ABAC), які в основному покладаються на статичні правила та політики. Ця модель має підхід до управління доступом, який базується на контексті. Адміністратор визначає для кожного контексту набір дозволів, тому коли суб'єкт працює в певному контексті, він миттєво отримує набір дозволів, активних для відповідного контексту.

CBAC дозволяє організаціям точно налаштовувати рішення щодо контролю доступу, враховуючи ці контекстуальні фактори, наприклад, може обмежити доступ до конфіденційних даних у неробочий час, може надати доступ до ресурсів лише тоді, коли користувач перебуває в конкретному фізичному місці. Однак, неправильна конфігурація або недостатня обробка контексту може призвести до помилок у наданні доступу, що може призвести до порушень безпеки. Також керування політиками доступу, які базуються на контексті, може бути складним завданням, особливо у великих медичних установах з великою кількістю користувачів і ресурсів.

Модель TeaM-based Access Control (TMAC) [4] спрямована на забезпечення контролю доступу у спільних середовищах, використовуючи підхід на основі ролей. Головним поняттям в підході TMAC є «команда», що слугує абстракцією для інкапсуляції користувачів та їхніх ролей. При розробці цієї моделі, враховували дві основні вимоги: використати переваги рольових моделей для ефективного керування доступом, але забезпечити більший контроль над окремими користувачами, а також врахування контексту в процесі виконання завдань. У цій моделі дозвіл може бути активований або деактивований, від цього залежить чи буде операція успішною. Також використання контекстів дозволяє налаштувати доступи більш гнучко з урахуванням обставин.

У моделі TMAC користувачі призначаються до команд, і через належність до команди отримують доступ до ресурсів команди. Однак, конкретні дозволи надаються згідно з його поточною діяльністю та належністю до команди. Це корисно тим, що лікар не буде мати доступ до чужих пацієнтів. Лише коли лікар приєднується до команди, він отримає доступ до медичних записів пацієнта. Який рівень доступу він матиме до чутливих даних буде визначено його роллю в команді.

Дозвіл доступу лікаря до пацієнта залишається активним виключно у випадку стеження за ним. Крім того, ця модель враховує різноманітні контекстуальні параметри, такі як час доступу, місцезнаходження тощо.

Проте, модель TMAC також має свої недоліки. Наприклад, використання контекстуальних параметрів може потребувати додаткового адміністративного та обчислювального ресурсів для їх відстеження та обробки.

Для медичних даних важливо забезпечити конфіденційність, щоб гарантувати захист особистої інформації пацієнтів, збереження цілісності для уникнення випадків втручання чи зміни даних, протидія внесенню дезінформації для забезпечення достовірності інформації, а також гнучкість, щоб забезпечити можливість адаптації до змін у вимогах та умовах обробки даних. Розглянуті вимоги до захисту медичних даних представлені нижче у вигляді таблиці 1.

Таблиця 1. Результати порівняльного аналізу моделей розмежування прав доступу

Модель	**Конфіденційність**	**Цілісність**	**Протидія внесенню дезінформації**	**Гнучкість**
ABAC	Висока	Висока	Висока	Висока
OrBAC	Висока	Середня	Середня	Середня
CBAC	Висока	Висока	Висока	Середня
TMAC	Висока	Висока	Висока	Середня

Таким чином для медичних даних найдоцільніше обрати модель ABAC, оскільки вона забезпечує високий рівень конфіденційності, гнучкість у керуванні доступом та врахування контексту, що важливо для гнучкого та ефективного керування доступом до медичної інформації.

Висновки

Кожна з розглянутих моделей розмежування прав доступу має свої переваги та обмеження у контексті захисту медичних даних. Модель ABAC відзначається високим рівнем конфіденційності та гнучкістю у керуванні доступом, дозволяючи враховувати різні умови та контекст використання, що сприяє ефективній протидії внесенню дезінформації. Модель OrBAC пропонує масштабованість та точне визначення ролей, проте має обмежену гнучкість у керуванні доступом у залежності від часу та місцезнаходження. Модель CBAC надає гнучкість у врахуванні контексту, але може бути складним у налаштуванні та має ризик неправильного надання доступу через недостатнє розуміння контексту. Нарешті, TMAC пропонує динамічний доступ із залежністю від діяльності користувачів, але може бути складним у керуванні та ресурсами.

Отже, враховуючи особливості медичної галузі, кожна модель може запропонувати цікаві рішення, проте ABAC є найбільш відповідною для лікарні, забезпечуючи високий рівень конфіденційності, гнучкість у керуванні доступом та врахування контексту. Однак при створенні інформаційних систем, які орієнтовані на окремі бізнес-процеси медичної галузі, також перспективними можуть бути такі моделі як CBAC та TMAC.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Guide to Attribute Based Access Control (ABAC) Definition and Considerations / Vincent C. Hu, David Ferraiolo, Rick Kuhn [et al] // National Institute of Standards and Technology, 2019. – P. 47. – Mode of access: https://doi.org/10.6028/NIST.SP.800-162 (date of access: 13.03.2024).
2. A dynamic access control model / Narhimene Boustia, Aicha Mokhtari // Applied Intelligence. – 2012. – Vol. 36 – P. 190 – 207. – Mode of access: https://doi.org/10.1007/s10489-010-0254-z (date of access: 13.03.2024).
3. Contexts and Context-Based Access Control / Eduardo B. Fernandez, Maria M. Larrondo-Petrie, Alvaro E. Escobar // Third International Conference on Wireless and Mobile Communications (ICWMC'07). – 2007. – P. 73. – Mode of access: https://doi.org/10.1109/ICWMC.2007.30 (date of access: 13.03.2024).
4. Team-based access control (TMAC) a primitive for applying role-based access controls in collaborative environments / Roshan K. Thomas // Proceedings of the second ACM workshop on Role-based access control – 1997. – P. 13 – 19. – Mode of access: https://doi.org/10.1145/266741.266748 (date of access: 13.03.2024).

Клиш Вікторія Миколаївна — студентка групи 1БС-20б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: vklysh71@gmail.com

Баришев Юрій Володимирович — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: yuriy.baryshev@vntu.edu.ua.

Viktoriia Klysh — student of 1БС-20б group, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : vklysh71@gmail.com.

Yurii Baryshev — PhD (eng), associated professor of information protection department, Vinnytsia National Technical University, Vinnytsia, email: yuriy.baryshev@vntu.edu.ua.