

8. ВОПРОСЫ КОНФИДЕНЦИАЛЬНОСТИ И ЭТИКИ В HEALTHGRID'e

Медицинское обслуживание связано с хранением и использованием персональных данных пациентов. Данные должны быть строго конфиденциальными и защищенными от нарушения секретности. Грид-технология прежде не учитывала эти требования, поскольку была разработана для нужд физики высоких энергий, где данные об элементарных частицах не нуждаются в защите секретности в отличие от данных о человеке в современном обществе.

Биомедицинские данные часто содержат весьма деликатную информацию о человеке и хотя, вообще говоря, используются для блага общества, но могут быть источником злоупотреблений. Есть соответствующий подход к защите этой информации. Инциденты с злоупотреблением медицинскими данными освещались в СМИ [L03] и служили доказательством серьезности угрозы несанкционированного использования данных. Посмотрите, например, как скажется на обществе доступ банков и страховых компаний к медицинским данным клиентов, раскрывающим их прошлое, настоящее и, возможно, будущее состояние здоровья. Действительно, неправомерное использование медицинских данных может повлиять на каждого из нас, поскольку практически каждый человек когда-то обращается в банк для получения кредита, оформляет страховку или устраивается на работу.

Очевидно, что защита тайны информации имеет прямое влияние на благосостояние как отдельного человека, так и общества в целом. В самом деле, может так случиться, что утечка информации приведет к нашему разорению [C03]. Право на тайну информации расценивается как фундаментальное право человека. Власти отдают себе отчет о последствиях нарушения этого права и прилагают значительные усилия для его юридического оформления [EU95][EU02]. Благодаря возможностям, которые предоставляют современные грид-технологии (таким как трансграничная обработка конфиденциальной информации), большое значение приобретают исследования, касающиеся правовых ограничений в области здравоохранения (см. Гл. 9).

Медицинская практика и медицинские исследования всегда твердо придерживались правил этики. За соблюдением этических норм следят наблюдательные советы, которые обязывают выполнять такие требования как согласие пациента на предоставление информации [M01]. Ученые и специалисты, разрабатывающие грид-технологии, часто не задумываются о соответствующем обращении с медицинской информацией, но для профессионалов-медиков защита конфиденциальности информации – это предмет для беспокойства. Вопросы конфиденциальности и правовые вопросы, поднимаемые healthgrid'ами, возникают из-за прозрачного обмена и обработки медицинской информации в условиях стирания границы между локальными и удаленными ресурсами, предусмотренного грид-технологиями. Конечно, эти проблемы не совсем новы для медицинской информатики. Поэтому крайне важно, чтобы эксперты обменивались опытом разрешения этих проблем в здравоохранении, чтобы они не стали препятствиями на пути реализации healthgrid'a.

8.1. ЗАЩИТА КОНФИДЕНЦИАЛЬНОСТИ, БЕЗОПАСНОСТЬ И HEALTHGRID

8.1.1. Технология безопасности в гриде

С самого начала грид-сообщество прикладывало много усилий к разработке мер по безопасности [W03]. Основное внимание уделяется разработке механизмов **аутентификации** и **авторизации**. Интеграция на нижнем уровне промежуточного программного обеспечения позволяет унифицировать механизмы безопасности (разработчик API) и сделать их интероперабельными (см. [GLOBUS]). Реализация этих механизмов еще находится на ранней стадии. Важно понимать, что дальнейшее развитие технологии безопасности имеет решающее значение для принятия концепции healthgrid'a.

Первый уровень защиты конфиденциальности – это предотвращение неавторизованного доступа к данным. В медицинских приложениях всегда использовались самые современные методы безопасности. Такой же уровень должен быть достигнут и в среде грида. Любые инициативы в области healthgrid'a должны использовать новейшие достижения грида в разработке средств безопасности. Базовые грид-службы, такие как, например, службы интеграции мелкомодульных средств управления доступом на нижнем уровне промежуточного программного обеспечения (например, CAS или VOMS в гриде), должны быть поддержаны биомедицинским сообществом.

Для реализации healthgrid'a требуется дальнейшее развитие и тестирование механизмов безопасности, продолжающееся после той точки, где могут остановиться разработчики классического грида, полагающие, что их приложения уже достаточно защищены.

Технология безопасности, принятая в настоящее время грид-сообществом, могла бы предложить приемлемое решение для первых и наиболее очевидных медицинских приложений – для вычислительных задач в здравоохранении. Применение вычислительных гридов в здравоохранении – это разумный первый шаг к подлинному healthgrid'у, но только первый шаг. Проблемы, возникающие на это шаге, аналогичны проблемам, с которыми сталкивается классический грид.

В отличие от многих других областей здравоохранения конфиденциальность в таких случаях имеет второстепенное значение. Природа самого приложения такова, что риск разглашения секретной информации снижается. Вычислительным задачам присуще сегментирование обрабатываемых данных, а сами данные обычно не идентифицируемы, поскольку относятся к сложным численным моделям. Таким образом, сходство с приложениями классического грида имеет место и в области безопасности, поэтому нет необходимости в разработке специальных средств 'защиты информации'.

8.1.2. Требования к безопасности в healthgrid'e

Healthgrid не ограничится только использованием грид-технологии для распределенного компьютеринга. Со временем он должен будет предложить общую платформу для всех действующих субъектов (**actors**) в е-здравоохранении. Поэтому важной задачей является также возможность совместного использования больших объемов распределенных гетерогенных данных (или данных различных уровней).

Очевидно, что связывание нескольких распределенных источников данных, относящихся к одному индивидууму в гриде данных чревато риском потери конфиденциальности. (Виртуальная) интеграция большого числа персональных медицинских данных – не единственный предстоящий риск. Несомненно, грид-технология послужит стимулом для использования данных геномики в исследовательских работах. Однако, этот тип данных имеет ряд специфических характеристик, связанных с конфиденциальностью, которых нет у других типов (медицинской) информации:

- генетические данные касаются не только отдельного человека, но и его родственников. Согласие человека на раскрытие его генетической информации означает *de facto* раскрытие информации о других людях, т.е. о его родственниках. В случае геномной медицины существует сложная взаимосвязь между правами отдельного человека и необходимостью совместной работы;
- медицинские данные – это информация о прошлом и настоящем состоянии здоровья человека, но по генетической информации можно прогнозировать будущее состояние здоровья или условия развития заболевания;
- генотип отдельного человека почти уникален и устойчив, поэтому может стать источником увеличивающегося объема информации;
- полный объем информации, содержащейся в геномных данных, пока неизвестен, поэтому трудно оценить, каким он будет в будущем;
- геномные данные легко могут быть неправильно интерпретированы непрофессионалами; утверждение о ‘предрасположенности’ к болезни может быть ошибочным.

Из всего вышесказанного следует, что необходимо найти баланс между двумя противоречащими целями: с одной стороны, необходимо максимизировать возможности охраны здоровья и медицинских исследований и эффективность обработки данных, с другой стороны – требуется защита права человека на частную информацию; эту трудную задачу предстоит решить в ближайшем будущем.

В прошлом в медицинской практике было определено два подхода к защите конфиденциальности. Первый подход заключается в том, что сотрудникам, создающим и сопровождающим информацию, запрещается раскрывать эту информацию лицам, не имеющим права доступа к информации. В основном это сводится к использованию классических мер безопасности (**управление доступом, авторизация**). Healthgrid идеально подходит для дальнейшего развития (и реального применения) технологии грида для обеспечения безопасности, поскольку в здравоохранении существуют жесткие требования безопасности. Первоочередная задача в контексте healthgrid’a – это проведение глубокого анализа новых возникающих рисков и угроз безопасности.

8.1.3. Технология повышения конфиденциальности

Технологию, разработанную специально для защиты конфиденциальности, называют способами или технологиями повышения конфиденциальности (PET - Privacy Enhancing Techniques or Technologies). Один автор дает следующее определение PET [B01]:

‘Согласованная система средств информационно-коммуникационной технологии для защиты конфиденциальности посредством исключения или сокращения персональных данных или посредством предотвращения ненужной и/или нежелательной обработки персональных данных без потери функциональности информационной системы’.

PET’ы представляют собой относительно новую технологию – концепция появилась в 90-е годы и широко разрабатывалась как в США, так и в Европе.

В здравоохранении PET’ы используются, главным образом, для защиты персональных медицинских данных.. PET’ы должны гарантировать анонимность пациентов и, в то же время, предоставлять возможность обработки медицинской информации клиницистам и исследователям. Применение методов защиты конфиденциальности было продемонстрировано несколькими исследовательскими проектами [DC02], эти методы уже широко используются в клинических исследованиях, в изучении болезней, при обмене результатами исследований и при повседневном обращении к медицинским данным. PET’ы, как и средства анонимизации, уже рассматривались при выработке стандартов передачи медицинских данных Комитетом CEN/TC251.

В healthgrid’е доступ к большим объемам полезной персональной информации может быть открытым, если использовать методы защиты конфиденциальности (главным образом, методы деидентификации) [DC04].

8.1.4. Интеграция PET’ов в грид и безопасность

Безопасность и защита конфиденциальности тесно связаны. Однако, при защите конфиденциальности главное внимание уделяется не просто ограничению доступа к данным, но ограничению доступа к идентифицирующей человека информации, содержащейся в данных. Хотя различие между этими двумя ограничениями не всегда очевидно, PET и технология безопасности должны рассматриваться как дополняющие друг друга технологии сохранения конфиденциальности персональной информации.

Правомерен вопрос, нужно ли интегрировать в healthgrid эти средства безопасности и защиты конфиденциальности. Не вызывает сомнения, что все healthgrid’ы должны учитывать жесткие требования защиты медицинских данных. Однако, средства защиты можно было бы разрабатывать совершенно независимо от того, что приложение будет выполняться в гриде. В таком случае эти средства лишь незначительно отличались бы от имеющихся *ad hoc* решений (защита конфиденциальности медицинских данных безотносительно к грид-технологии).

С другой стороны, значительные преимущества могла бы дать интеграция специфических средств защиты конфиденциальности в грид-службы. Эти средства близки классическим способам защиты (которые составляют значительную часть промежуточного программного обеспечения грида), поэтому интеграция этих средств в грид не только логична, но и может служить стимулом для использования технологии

защиты конфиденциальности, ведущей к защите данных 'по умолчанию', в каждом медицинском грид-приложении. Интеграция PЕТ'ов в нижний уровень промежуточного программного обеспечения должна быть, вероятно, ограничена (в данном контексте, см. ниже, политикой управления). Нижний уровень промежуточного программного обеспечения (такой как Globus) предоставляет широкий набор инструментальных программных средств для развития грида. Специфические средства биомедицинской информатики для безопасности и защиты конфиденциальности не являются главной целью разработчиков промежуточного программного обеспечения грида.

Как и в нескольких других разработках, связанных с объединением данных, средства безопасности и защиты конфиденциальности медицинских данных можно было бы интегрировать в верхний уровень промежуточного программного обеспечения, сохранив, тем самым, общие возможности, находящиеся в распоряжении широкого сообщества пользователей, но, не перегружая набор инструментальных средств для других областей исследований, где не требуются такие жесткие меры безопасности и защиты.

Основная часть средств защиты конфиденциальности будет, по крайней мере, в начале сосредоточена на уровне приложений. Это не означает, что разработка средств защиты будет происходить вне healthgrid-инициативы. Напротив, поскольку обязательная защита данных является необходимым условием для применения информационных технологий в здравоохранении, стандартизация PЕТ-технологии может получить поддержку посредством создания специальных грид-служб, таких как служба псевдоанонимизации, которая позволит центрам обработки информации автоматически деидентифицировать их базы данных при помощи грид-служб (гарантируя использование новейшей технологии) перед обменом информацией с другим центром.

По мере разработки и запуска пилотных проектов станет ясно, какая часть технологии должна быть реализована и на каком уровне.

8.1.5. Проблемы healthgrid'a

Чтобы проиллюстрировать необходимость специальных исследований в любой healthgrid-инициативе, рассмотрим некоторые типичные проблемы, возникающие из-за жестких требований медицины. Представленные здесь примеры проблем достаточно очевидны и поэтому были уже сформулированы раньше [GK02]. Однако, они не были решены. С появлением healthgrid'a требования к конфиденциальности и защите данных возрастают.

Грид предоставляет доступ к гетерогенным ресурсам, таким образом, в healthgrid'e хранение и обработка секретных персональных данных будут выполняться на удаленных ресурсах. Конечный пользователь должен доверять этим ресурсам. Но кто может определить степень доверия? Простое и очевидное решение – использовать 'закрытые' системы, а это означает, что любой ресурс в гриде известен и определен заранее. Однако, такое решение приходит в противоречие с представлением о динамическом гриде, в котором связи устанавливаются по мере необходимости.

Решение следует искать при помощи разъяснений и согласований. Ресурсы должны обладать способностью информировать пользователя о том, как будут обрабатываться данные, какая политика будет применяться, какие PЕТ'ы используются, кто имеет доступ

к данным и т.д. Про такие методы иногда говорят, что это не настоящие РЕТ'ы, поскольку они не накладывают ограничений на совокупность персональных идентифицируемых данных и не гарантируют реальную обработку. Ресурс может объявить, что придерживается жестких правил, но проверить это практически невозможно.

Первые шаги в направлении политики управления были сделаны разработчиками грида. Их усилия были направлены на разработку стандартов, таких, как WS-Privacy, WS-Policy и Enterprise Privacy Authorization Language (EPAL), но на сегодняшний день внедрение стандартов довольно ограничено и исследование всех возможностей этой технологии не будет проводиться до тех пор, пока это не коснется области здравоохранения – главной области приложений. Healthgrid может стать идеальной средой для проверки и дальнейшего развития РЕТ'ов.

Эти соображения непосредственно касаются специфических механизмов грида, таких, как репликация данных. Механизм репликации состоит в автоматическом копировании данных, находящихся на ресурсе, для повышения эффективности (например, чтобы избежать задержки при пересылке данных). Для медицинских данных это недопустимо. Ресурс, на который будет помещена реплика данных, должен иметь, по крайней мере, такую же степень доверия, как и источник данных, и должен подчиняться таким же жестким правилам. Healthgrid должен обладать способностью действовать в таких случаях автономно, чтобы не утратить свою динамическую природу (и эффективность).

Другой пример – это делегирование прав. Делегирование прав очень важно в среде грида, но в медицинском мире это далеко не очевидно. Если один пользователь передает свои права (ресурсы) другому пользователю, он становится ответственным за действия, которые выполняются от его имени. В медицинской среде это имеет серьезные последствия в смысле ответственности. Подходящим решением для медицинских приложений может быть использование ограниченных прокси-сертификатов, но ясно, что поиск решений должен быть продолжен.

Важным вопросом для healthgrid'a будет политика управления, как для безопасности (например, политика авторизации), так и для защиты данных (политика сохранения конфиденциальности). Трудной задачей в этом контексте является принудительное и гарантированное проведение в жизнь политики управления.

Столь же важной и связанной с этим вопросом является проблема реализации **механизмов аудита**. Все действия в медицине должны регистрироваться заслуживающим доверия способом. Строгое выполнение обязательств в сочетании с соблюдением правовых норм может помочь решению проблемы ответственности в здравоохранении.

Наряду с упомянутыми выше проблемами существует еще и ряд требований, предъявляемых медицинскими грид-приложениями, которые могли бы быть удовлетворены, например, на верхнем уровне промежуточного программного обеспечения грида и дали бы преимущества большому сообществу людей, занятых в здравоохранении. Сюда относится шифрование медицинских данных (далеко не очевидная проблема) и заслуживающая доверия интеграция исследовательских баз данных – виртуальное объединение маленьких 'сот' деидентифицированных данных (например, данные географического региона или больницы) может уменьшить риск раскрытия идентифицирующих пациента данных (за счет расширения набора анонимных данных).

Наконец, появляется ряд PЕТ'ов, которые хорошо работают в распределенных средах – это система PIRS (Private Information Retrieval and Storage), куда входят не нарушающее конфиденциальности извлечение информации из данных, обработка зашифрованных данных и другие технологии. Но путь к развитой, требуемой для е-здравоохранения, защищающей конфиденциальность структуре еще долг и усеян техническими трудностями, которые должны разрешаться последовательно.

Очевидно, что грид-технология может быть успешно применена в биомедицинской среде, только если технологические решения, которые постоянно изменяются с появлением новых потребностей, будут учитывать этические и правовые требования.

8.2. ССЫЛКИ

- [G96] Goodman KW. Ethics, Genomics, and Information Retrieval. *Comput. Biol. Med.* 1996; vol 26, no.3:223-229.
- [M02] Martin-Sanchez F. Integrating Genomics into Health Information Systems. In: *Methods Inf Med* 2002; 41:25-30.
- [LCG] Website: <http://lcg.web.cern.ch/lcg/>
- [L03] Lazarus D. A tough lesson on medical privacy: Pakistani transcriber threatens UCSF over back pay. *San Francisco Chronicle* Wednesday, October 22, 2003
- [C03] Caloyannides M. Society Cannot Function Without Privacy. *IEEE Security & Privacy*, May-June 2003 (Vol. 1, No. 3).
- [EU95] Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- [EU02] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
- [M01] Mehlman MJ. The effect of Genomics on Health Services Management: Ethical and Legal Perspectives. *Frontiers of Health Services Management*; 17;37:17-26. 2001.
- [W03] Welch, V., Siebenlist, F., Foster, I., Bresnahan, J., Czajkowski, K., Gawor, J., Kesselman, C., Meder, S., Pearlman, L. and Tuecke, S., Security for Grid Services. in 12th IEEE International Symposium on High Performance Distributed Computing, (2003).
- [GLOBUS] Website: <http://www.globus.org/>
- [IBM04] Martin-Sanchez F et al. Synergy between medical informatics and bioinformatics: facilitating genomic medicine for future health care. *J Biomed Inform.* 2004 Feb;37(1):30-42.
- [HG] Website: <http://www.healthgrid.org/>
- [B01] Borking J, Raab C. Laws, PETs and Other Technologies for Privacy Protection. *The Journal of Information, Law and Technology (JILT)*, 2001.
- [DC02] De Meyer F, Claerhout B, De Moor GJE. The PRIDEH project: taking up Privacy Protection Services in e-Health Proceedings MIC 2002 'Health Continuum and Data Exchange'. IOS Press, 2002, p. 171-177.
- [DC04] De Moor GJE, Claerhout B. Privacy Protection for Healthgrid Applications (Accepted for *Methods Inf Med* 2004)

[GK02] Guy L, Kunszt P, Laure E, Stockinger H, Stockinger K. Replica Management in Data Grids. Technical report, Global Grid Forum Informational Document, GGF5, Edinburgh, Scotland, July 2002.