УДК 004.738.5 Вестник УрФО № 4(38) / 2020, с. 44–54

Пономарёв К.Ю., Захаров А.А.

DOI: 10.14529/secur200404

МЕТОДЫ РАЗГРАНИЧЕНИЯ ДОСТУПА В СЕТЯХ ИНТЕРНЕТА МЕДИЦИНСКИХ ВЕЩЕЙ НА ОСНОВЕ АТРИБУТИВНЫХ МОДЕЛЕЙ

Термином «Интернет медицинских вещей» («InternetofMedicalThings», «IoMT») называют совокупность устройств и технологий удаленного мониторинга состояния здоровья пациентов с использованием носимых устройств. Одной из проблем, затрудняющих массовое внедрение технологий IoMTявляетсяресурсоёмкая защита пользовательских сведений при передаче информации по незащищенным каналам связи и её хранение в облачных системах.Ставшие уже классическими технологии и методызащиты Интернет-ресурсов и систем массового обслуживанияне подходят в том случае, когда речь идёт о миллионах устройств IoMT, по такимпараметрам как:низкая вычислительная мощность, нехватка памяти, ограниченная емкость батареи питания и др. В работе исследуются возможности использования атрибутивного шифрования ABE («Attribute-basedencryption») для защиты персонифицированной информации всетях IoMT. Изучаются вопросыконфиденциальности данных пациента при передаче и хранении информации в облаке, менеджмент криптографических ключей и контроль за распространением данных. Предлагаются алгоритмы для приемлемого защищенного решения. Предложен фреймворк для обработки данных пациентов с портативных диагностических устройств с использованием методов атрибутивного шифрования. Приведены результаты нагрузочного тестирования прототипа.

Ключевые слова: *телемедицина, электронные персональные медицинские карты, авторизация, интернет вещей, атрибутивный контроль доступа.*

Исследование выполнено при финансовой поддержке гранта: РФФИ и Тюменской области в рамках научного проекта № 20-47-720005 и гранта РФФИ 22/2020.

Ponomarev K.Y., Zaharov A.A.

ACCESS CONTROL METHODS FOR INTERNET OF MEDICAL THINGS NETWORKS BASED ON ATTRIBUTE MODELS

The term «Internet of Medical Things» (IoMT) refers to a set of devices and technologies for remote monitoring of patients' health using wearable devices. One primary problem with patient's data is ensuring privacy and resource intensive protection when it is transmitted over open communication channels and stored in cloud systems. However, when it comes to millions of IoT devices, technologies that have already become classic for Internet resources are not suitable in many aspects at once: low computing power, out of memory, limited battery capacity and etc. The work considered Attribute-based encryption for ensuring security of personified data in IoMT networks. Also, the research studied the issues of patient's data confidentiality in cloud systems, management of cryptographic keys and data sharing control. The algorithms for effective and secure solution were proposed. We have proposed a framework for processing patient data from portable diagnostic devices using ABE methods. The results of load testing of the prototype are presented too.

Keywords: *telemedicine, personal health records, authorization, internet of things, attribute-based access control.*

В современном мире время взаимодействиеврача и пациента ограничено, что обусловливает необходимость диагностировать и определять стратегию лечения в кратчайшие сроки, не теряя при этом качество. Это требует внедрения в практику здравоохранения передовых научных разработок, в том числе достижений в области информационно-коммуникационных технологий, которые стимулируют развитие новых концепций персонализированного здравоохранения. Отметим, что процесс перехода от бумажных носителей к цифровым, делает необходимым переход от управления бумагами к управлению данными, что требует изменения стандартов работы с медицинской информацией.

В настоящее время наиболее распространенными технологиями работы с медицинской информацией являются **электронные медицинские карты (ЭМК)**, представляющие совокупность электронных персональных медицинских записей (ЭПМЗ), относящихся к пациенту, собираемых, хранимых и используемых в рамках одной медицинской организации. Термин ЭМК является аналогом международного термина ElectronicMedical Record (EMR). Отвечая на современные требования к организации распределенной инфраструктуры медицинской помощи,в России вместо стандарта ГОСТ Р 52636-2006 «Информатизация здоровья. Электронная медицинская карта. Электронная медицинская карта, используемая в медицинской организации», разрабатываются два дополнительных стандарта: ГОСТ Р «Информатизация здоровья. Электронная медицинская карта. Интегрированная электронная медицинская карта» и ГОСТ Р «Информатизация здоровья. Электронная медицинская карта. Персональная электронная медицинская карта» [1].

Деление понятия «Электронная медицинская карта» на 3 новых функциональных слоя обеспечит совместное использование данных из медицинских записей,их единообразное пониманиеи трактовку не только сотрудниками различных медицинских организаций, но и даст возможность пациенту проявить заботу о собственном здоровье. Такая организация работы с медицинской информацией характеризуется термином

5П-медицина, отражающим следующие основополагающие принципы: персонализация, предикция, превентивность, парсипативность и прецизионность [2,3]. При этом, хотя реализаций полного спектра 5П в полном объемепока не существует, запрос на новые подходы к сохранению своего здоровья (персонализация, предикция, превентивность) уже сформировал на основе понятия «Интернет вещей» (IoT) термин «Интернет медицинских вещей» (от англ. «Internet of MedicalThings», «IoMT»), как совокупность устройств и технологий удаленного мониторинга состояния здоровья с использованием носимых устройств [4].

СистемыIoMT могут использоваться для объединения доступных медицинских ресурсов и предоставления умных комплексных медицинских услуг, например, в процессе реабилитации пожилых пациентов после инсульта, мониторинга состояния здоровья пациентов с хроническими заболеваниями, в том числе пациентов, живущих в удаленных местах [5-6].

Технологии на базе IoMTиспользуют портативные медицинские устройства, объединённые в беспроводную нательную сеть WBAN (англ. WirelessBodyAreaNetwork) [7] для сбора медицинских данных пациентов и записи информации в электронную персональную медицинскую запись (ЭПМЗ). Совокупность электронных персональных медицинских записей (ЭПМЗ), поступивших из различных источников и относящихся к одному человеку, который осуществляет сбор, управление иназначение права доступа к ЭПМЗ определяет **персональную электронная медицинскую карта (ПЭМК)** – аналог международного термина PersonalHealthRecord (PHR) [8].

ПЭМК - являются основой для создания систем персонализированной медицины, находящихся в облачном защищенном хранилище. Идея, лежащая в основе таких систем, заключается в том, что пользователь хранит собственную ПЭМК и регулирует к ней доступ персоналу медицинских учреждений, сотрудникам страховых компаний, родственникам. Это актуально в современных условиях, когда пользователь может быть связан с большим количеством медицинских организаций, каждая из которых ведёт свою собственную базу пациентов и высокой мобильностью граждан (переезды внутри одного города или в рамках всей страны). Отметим, что в качестве поставщика данных ПЭМК могут выступать сами пациенты, медицинские информационные системы лечебных учреждений, а также портативные диагностические устройства в автоматическом режиме собирающие и передающие данные, например, в облако дляих анализа и хранения.

Совокупность электронных персональных медицинских записей (ЭПМЗ), относящихся к одному человеку, собираемых, передаваемых и используемых несколькими медицинскими организациями формируют **Интегрированную электронную медицинскую карту (ИЭМК)**[9].

Используя данныеИЭМК и ПЭМК можно выявить закономерности изменений состояния здоровья, особенности течения заболеваний и оценить качество медицинского обслуживания. Для извлечения валидной информации из неструктурированных данных ИЭМК и ПЭМК выявления характерных категорий пациентов используются методы data mining иBig Data[10 - 11].

Отметим, что поскольку IoMT тесно интегрирован с ПЭМК и ИЭМК, сетями IoT, аналитическими приложениями и сервисами обработки данных, то в сетях IoMT пристальное внимание должно уделяться разграничению доступа к данным и их конфиденциальности при передаче по открытой сети [12,13], а также хранению в облачном хранилище [14,15]. Поскольку пациент имеет минимальный контроль над своими данными, после того как они были переданы в облачное хранилище, тоэти данные подвержены таким угрозам нарушения конфиденциальности как инсайд со стороны облачного провайдера или администратора приватного облака, потери данных, влияния других виртуальных сред и наличия небезопасных интерфейсов доступа к данным. Отметим также, что на сетевом уровне взаимодействия между устройствами, облаками и промежуточными узлами обычно используются протоколы Wi-Fi, BLE, ZigBee [16], которые уязвимы к таким атакам как «человек посередине» или «повтор сообщений».

Одним из эффективных методов, обеспечивающих безопасность и хранение данных ПЭМК, является криптографическая защита информации. Принципиально важно, что симметричные алгоритмы шифрования менее ресурсоёмки и, следовательно, больше подходят для IoT устройств с низким энергопотреблением, но они являются уязвимыми с точки зрения механизмов обмена ключами.

Перечислим основные свойства систем

ПМЭК с точки зрения информационной безопасности.

• Конфиденциальность: сведения должны быть защищены как в процессе передачи, так и при хранении в облачном хранилище. Необходима защита данных от посторонних наблюдателей в открытой сети, самого облачного провайдера или злоумышленников, нарушивших его целостность.

• Ориентированность на пациента: пользователь имеет полный контроль над своими данными и регулирует политики доступа к ним. С точки зрения врача это означает, что при обращении новый пациент может предоставить доступ ко всей своей истории болезни, включая все детали заключений врачей и все предыдущие анализы.

• Делегирование и отзыв прав: пользователь имеет возможность отозвать доступ у кого-либо к своим сведениям или делегировать право на управление своими записями кому-либо (например, родственникам). Также стоит отметить такой момент, как доступ персонала скорой помощи к пользовательским сведениям в чрезвычайных ситуациях.

В традиционным подходе к защите информации криптосистемам необходимо явно указать получателя данных (например, используя его сертификат открытого ключа), но это неприменимо в рассматриваемой медицинской прикладной области: пациент, загружая сведения, может не знать конкретных потребителей информации. Таким образом, современные средства защиты на основе симметричных и асимметричных криптосистем малоэффективны при работе с ПЭМК.

Перспективы безопасного интернета медицинских вещей обсуждаются в работе [17-21]. Авторы обсуждают подходы к решению таких проблем IoT eHealth, как управление данными, масштабируемость, правила, совместимость интерфейсов устройств IoMIT-сеть-человек, а также безопасность и защиту конфиденциальности объектов и пользователей. В работе [22]авторы в качестве эффективного метода защиты пользовательских сведений предложили алгоритмы атрибутивного шифрования - ABE («attributebasedencryption»). Их идея заключается в том, что в криптосистеме с открытым ключом в качестве публичного ключа используется набор открытых параметров - атрибутов субъекта доступа. За генерацию соответствующих приватных ключей ответственен выделенный атрибутивный центр. Использование таких алгоритмов для защиты ЭМК позволяет решить множество проблем, описываемых разработчиками системперсонализированной медицины: конфиденциальность данных пациента при хранении в облаке, упрощенные механизмы менеджмента криптографических ключей, контроль за распространением данных самим пациентом.

1. Шифрование на основании атрибутов

Шифрование на основе атрибутов берёт своё начало из схем личностного шифрования («Identity-basedencryption»), которые являются разновидностью криптосистем с открытым ключом[23]. В роли открытого ключа в них используются параметры или атрибуты самого пользователя, например, адрес электронной почты. Каждый такой открытый параметр отображается в открытый криптографический ключ, а для расшифрования сообщений, сформированных с помощью этого ключа в центре генерации ключей, формируется соответствующий закрытый ключ [24].

В работе [25]набор открытых параметров шифртекста соответствует структуре доступа к данным, а набор открытых параметров пользователя – его атрибутам, на основании которых центр генерации ключей формирует ему секретный ключ. Пользователь, имеющий определённый закрытый ключ, может расшифровать шифртекст, тогда и только тогда, когда структура доступа соответствует атрибутам пользователя. В дальнейшем исследователи разрабатывали различные способы соответствия между этими наборами параметров, например, структура доступа может представлять собой булевскую формулу над пользовательскими атрибутами.

Основная сущность в ABE-схемах - атрибутивный центр («AttributeAuthority»). Он несёт ответственность за формирование и управление криптографическими ключами, верификацию атрибутов.

Существуют два вида схем атрибутивного шифрования – «Key-Policy» (KP-ABE) и «Ciphertext-Policy» (CP-ABE).Их основное отличие заключается в том, где располагается структура доступа к данным: в первом случае – в секретном ключе пользователя, во втором – в шифртексте. CP-ABE криптосистемы принято считать более гибкими и практическими полезными. Любая такая схема предоставляет следующие функции: формирования открытого и секретного мастер ключа; генерации приватного ключа на основании множества атрибутов; формирования шифртекста на основе открытого текста и структуры до-

ступа; расшифрования на основании шифртекста, структуры доступа и секретного пользовательского ключа.

2. Платформа обработки и хранения медицинских данных

Рассмотрим IoMT платформу, состоящую из следующих основных сущностей:

• Облачное хранилище медицинских данных (*Cloud*): хранит записи в разрезе пациентов, предоставляет API для доступа к медицинским сведениям.

• Атрибутивный центр (A*ttributeAuthority, AA*): служит центром регистрации для всех субъектов платформы - пациентов, врачей, IoT устройств, различных сервисов обработки и анализа данных. Хранит атрибуты для каждого из них, генерирует ключи схемы атрибутивного шифрования. Пациенты указывают политики доступа к своим данным в облачных хранилищах в виде атрибутивных правил. Атрибутивный центр имеет общий секретный ключ с каждым из зарегистрированных субъектов.

• Персональное дистанционное устройство (ПДУ, *Device*): собирает или агрегирует медицинские показатели с других устройств пациента, отправляет на дальнейшую обработку в облачное хранилище. Пациент имеет возможность зарегистрировать свои ПДУ в атрибутивном центре.

• Сервис генерации токенов (Token Generation Service, TGS): необходим для проверки прав доступа к API облачного хранилища.

Пошагово опишем процессы передачи данных - показателей жизнедеятельности пациента - в облако и их обработки.

1. Пациент выполняет процедуру регистрации для себя и своих ПДУ в атрибутивном центре. В итоге для каждого ПДУ будет указан список атрибутов, используемый для генерации приватного ключа, и секретный ключ, используемый при аутентификации в *АЦ*. Для верификации атрибутов возможен контроль со стороны медицинского персонала.

2. Пациент указывает в *АЦ* какие атрибутивные структуры доступа следует использовать при доступе к его данным. В дальнейшем для простоты будем считать, что используются только операции чтения и записи.

3. Пациент конфигурирует свои ПДУ: он должен указать им ключ доступа к атрибутивному центру, созданный при регистрации на первом шаге.

4. При старте работы ПДУ запрашивает в атрибутивном центре приватный ключ *ABE* схемы, который будет использоваться для авторизации в облачном хранилище. Для аутентификации и авторизации в *AA* используется ключ доступа, указанный на предыдущем шаге.

5. ПДУ инициирует запрос в *Cloud* на передачу показаний жизнедеятельности пациента.

6. ПДУ, облачное хранилище и *TGS* совместно выполняют протокол атрибутивного контроля доступа с целью проверки прав доступа на запись сведений.

7. В случае успешной проверки в хранилище происходит запись данных пациента в зашифрованном виде, такие образом с помощью *ABE* сведения будут защищены от облачного провайдера или от злоумышленника в случае его компрометации.

8. Автоматизированные сервисы обработки данных также получают от АЦ приватный ключ схемы атрибутивного шифрования. Они обращаются в API облачного хранилища за данными по пациентам, выполняют протокол атрибутивного контроля доступа с целью проверки прав доступа на чтение. Предполагается, что эти сервисы могут выявлять возможные отклонения в данных пациента, и в критических случаях уведомляют об этом пациента и его лечебное учреждение.

На основании описанных процессов можно выделить следующие требования к механизмам авторизации и аутентификации в рассматриваемой IoMT платформе. Эти требования соответствуют свойствам ЭМК, указанным ранее.

1. Пациент должен самостоятельно определять политики доступа на различные операции со своими данными в облаке, например, на запись и чтение. Для проверки прав доступа к данным пациента через API облачного хранилища должны использоваться указанные пациентом политики доступа.

2. Облачное хранилище знает, какому пациенту принадлежат передаваемые данные, однако не имеет к ним доступа, поскольку медицинские данные пациентов хранятся в зашифрованном виде.

3. Передача информации в открытой сети должна идти по защищенному каналу связи.

Внедрение методов атрибутивного контроля доступа и алгоритмов атрибутивного шифрования повышает эффективность механизмов безопасности IoMT платформ. Отметим, следующие положительные стороны предлагаемого подхода:

• используемая атрибутивная модель доступа является наиболее подходящей для современных динамичных сетей Интернета вещей и позволяет использовать гибкие и гранулированные политики доступа;

• *ABE* используется как для проверки прав доступа, так и для защиты информации в процессах её передачи по открытой сети и хранении в облаке;

• за счёт применения *ABE* реализуется механизм единого входа (SingleSignOn), когда приватный ключ, полученный от атрибутивного центра, может использоваться для доступа к различным облачным ресурсам;

• за счёт применения *ABE* упрощаются механизмы управления ключами, т.к. отправителю и получателю не нужно выполнять процедур по предварительному обмену ключами.

количество запросов к платформенным сервисам. Методика тестирования заключалась в выполнении процесса передачи данных по представленному ранее сценарию и измерении времени, прошедшего с момента отправки запроса от ПДУ до момента получения ответа на запрос. Данная величина включает в себя время, необходимое запрашиваемым сервисам на обработку запроса, в том числе на запросы к другим сервисам. Мы будет называть её временем отклика или временем выполнения запроса. Тестовый стенд был развёрнут на ресурсах платформы для облачных вычислений «Яндекс.Облако» (*http://cloud.yandex.ru*). Использовались виртуальные машины и диски сервиса *ComputeCloud*, их список приведён в таблице ниже. Все машины располагались в одной зоне доступно-

Рис. 1. Схема взаимодействия внутри IoMT платформы

Табл. 1

Характеристики виртуальных машин тестового стенда

Название	Количество виртуальных ядер (*vCPU*)	Гарантированная доля *vCPU*	Размер оперативной памяти, ГБ (*RAM*)	Размер *HDD* диска, ГБ
abe-vm1	2	5%	1	8
abe-vm2	2	100%	2	8
abe-vm3	2	100%	2	5

3. Нагрузочное тестирование прототипа IoMT платформы

В данной части будут представлены результаты нагрузочного тестирования прототипа IoMT платформы. Целью является выяснение возможности применения представленной модели в реальных системах Интернета вещей, для которых характерно большое

сти (*ru-central1-c*), то есть находились в одном дата-центре. На всех машинах была установлена операционная система *Ubuntu 18.04 LTS*.

Существенное влияние на время выполнения алгоритмов атрибутивного шифрования оказывает количество атрибутов. Поэтому в каждом эксперименте их количество постепенно увеличивалось, на каждый размер

множества атрибутов запускался тестовый сценарий. Также тестовые сценарии вначале запускались в одном потоке, потом параллельно в нескольких - с целью симуляции нагрузки на сервисы. На измеряемое время отклика могли влиять следующие факторы:

• на тестовом стенде размер коллекции в БД для хранения списка зарегистрированных устройств состоит из десятка записей, в реальных системах - это сотни тысяч записей, затраты на поиск в БД остаются неучтёнными в данном тесте, так как на практике это зависит от выбора конкретной СУБД и архитектуры масштабирования;

• в прототипе используется стороннее ПО для выполнения алгоритмов атрибутивного шифрования, что требует запросов к файловой системе, которые могут вносить задержки в измеряемое время.

ности и эффективности. С целью проверки возможностей подсистемы при горизонтальном масштабировании мы увеличивали количество экземпляров сервисов. В системах Интернета вещей масштабируемость сервисов и приложений имеет критическое значение, так как именно она обеспечивает доступность и позволяет выдерживать большие нагрузки. Для балансировки нагрузки использовался веб-сервер *nginx* с простым циклическим алгоритмом (*roundrobin*) балансировки.

Результаты нагрузочных экспериментов сильно зависят от используемой атрибутивной криптосистемы, деталей реализации, используемых языков программирования, фреймворков, СУБД и систем хранения данных. Поэтому они могут сильно отличаться в каждой конкретной информационной системе. Тем не менее, повысить эффективность

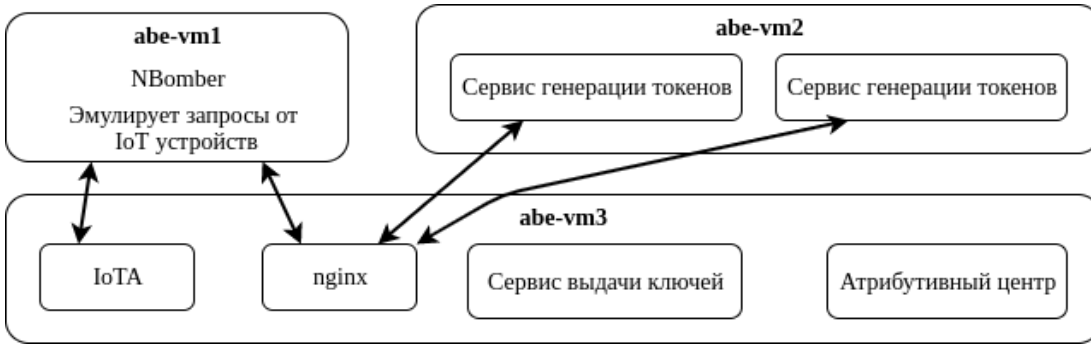

Рис. 2. Схема стенда для тестирования IoMT платформы

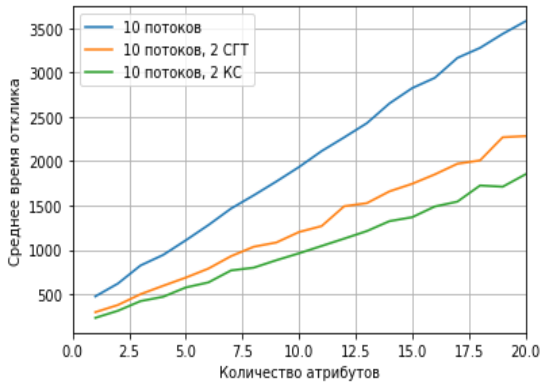

Рис. 3. Среднее время отклика при тестировании сервисов контроля доступа

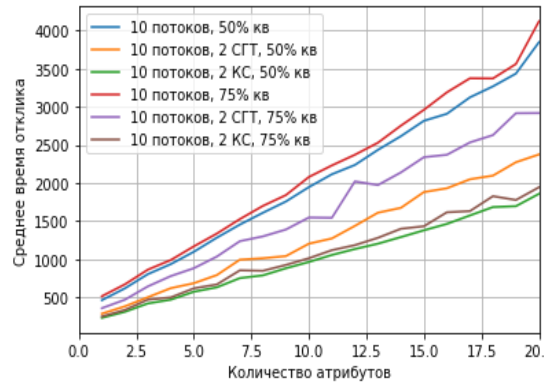

Рис. 4. Квантили времени отклика при тестировании сервисов контроля доступа

Из графиков становится ясным, что время выполнения запроса имеет практически линейную зависимость от размера множества атрибутов, это явление характерно для большинства схем атрибутивных криптосистем. Схемы *ABE* с таким свойством более распространены, а значит, имеют больше практически полезных свойств и лучше изучены, однако они ограничены в плане производительности системы можно масштабируя сервисы. При выборе того, у каких сервисов подсистемы атрибутивного контроля доступа необходимо увеличивать количество одновременно работающих экземпляров, следует учитывать следующие факторы:

• какие сервисы выполняют самые трудоёмкие криптографические операции схемы атрибутивного шифрования;

• какие сервисы испытывают большую нагрузку со стороны пользователей и устройств Интернета вещей;

• время жизни сессии взаимодействия между ПДУ и облаком, от этого зависит, как часто будет выполняться протокол атрибутивного контроля доступа, и соответственно нагрузка на сервисы генерации токенов;

• время жизни приватных криптографических ключей схемы *ABE*, от этого зависит нагрузка на сервисы раздачи ключей и атрибутивный центр.

4. Заключение

Разработка новых механизмов и моделей безопасности для систем персонализированного здравоохранения и сетей Интернета вещей является актуальной научной задачей. В данной статье была рассмотрена методы атрибутивного контроля доступа к ПЭМК пациентов для систем Интернета медицинских вещей. Нами были представлены: архитектурная модель платформы Интернета медицинских вещей, результаты нагрузочного тестирования прототипа. Непосредственно из работы следует необходимость в разработке следующих методов:

• системы атрибутивного контроля для платформ Интернета вещей с несколькими атрибутивными центрами - иерархическими, децентрализованными - и методы их применения на практике;

• разработка способов интеграции атрибутивных моделей в существующие платформы и решения;

• способность представленной модели противостоять атакам типа «отказ в обслуживании», или DDOS атакам;

• изучение возможностей дальнейшей эффективной работы и защиты пользовательских данных при компрометации атрибутивного центра;

• методы и протоколы отзыва атрибутов и секретных ключей схемы шифрования на основании атрибутов;

• производительность и эффективность схем атрибутивного шифрования на устройствах Интернета вещей.

Литература

1. Проект ГОСТ Электронная медицинская карта. Термины и определения.URL: http://portal.egisz.rosminzdrav.ru/materials/310 (дата обращения: 01.11.2020)

2. Щербо С. Н., Щербо Д. С. Медицина 5П: прецизионная медицина //Медицинский алфавит. – 2015. – Т. 4. – №. 18. – С. 5-10.

3. Zakharov A., Potapov A., Zakharova I., Kotelnikov A., Panfilenko, D. Infrastructure of the Electronic Health Record Data Management for Digital Patient Phenotype Creating. // 7th Scientific Conference on Information Technologies for Intelligent Decision-Making Support (ITIDS 2019). – Atlantis Press. -2019.

4. Joyia G. J. et al. Internet of Medical Things (IOMT): applications, benefits and future challenges in healthcare domain //J Commun. – 2017. – Т. 12. – №. 4. – С. 240-247.

5. ZakharovA. A., Potapov A. P., Zakharov, I. G., Olennikov E. A. Telemetric Medical System to Support Cardiological Screening. // In 2018 XIV International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE). – IEEE. - 2018. - С. 116-120.

6. Hassan M. K. et al. A Hybrid Real-time remote monitoring framework with NB-WOA algorithm for patients with chronic diseases //Future Generation Computer Systems. – 2019. – Т. 93. – С. 77-95.

7. Khan J. Y. et al. Wireless body area network (WBAN) design techniques and performance evaluation //Journal of medical systems. – 2012. – Т. 36. – №. 3. – С. 1441-1457.

8. ISO/TR 20514:2005 «Health informatics – Electronic health record – Definition, scope and context». URL: https://www.iso.org/standard/39525.html (дата обращения 20.10.2020)

9. Зарубина Т.В., Швырев С.Л., Соловьев В.Г., Раузина С.Е., Родионов В.С., Пензин О. В., Сурин М. Ю. // Интегрированная электронная медицинская карта: состояние дел и перспективы. Врач и информационные технологи. -2016. - № 2.

10. Gehrmann,S., Dernoncourt F., Li Y., Carlson E. T., Wu J. T., Welt J., Celi, L. A. Comparing deep learning and concept extraction based methods for patient phenotyping from clinical narratives// PloS one. – 2018.

11. Zakharov A., Kotelnikov A., Potapov A., Panfilenko D., Gayduk P. Information and Analytical Support for Biomedical Research in the Field of the Cardiovascular Disease Risk Prediction. // 8th Scientific Conference on Information Technologies for Intelligent Decision-Making Support (ITIDS 2020). - Atlantis Press. - 2020.

Исследование выполнено при финансовой поддержке Минобрнауки России (Грант ИБ).

12. Masood I. et al. Towards Smart Healthcare: Patient Data Privacy and Security in Sensor-Cloud Infrastructure //Wireless Communications and Mobile Computing. – 2018.

13. Kołodziej J. et al. Ultra Wide Band Body Area Networks: Design and Integration with Computational Clouds //High-Performance Modelling and Simulation for Big Data Applications. – Springer, Cham, 2019. – C. 279-306.

14. Kennedy Edemacu, Hung Kook Park, Beakcheol Jang, Jong Wook Kim. Privacy Provision in Collaborative Ehealth With Attribute-Based Encryption: Survey, Challenges and Future Directions //IEEE Access. - 2019. – 7.

15. Li M. et al. Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings //International conference on security and privacy in communication systems. – Springer, Berlin, Heidelberg, 2010. – C. 89-106.

16. Sundaravadivel P., Kougianos E., Mohanty S. P., Ganapathiraju, M. K. Everything you wanted to know about smart health care: Evaluating the different technologies and components of the Internet of Things for better health. // IEEE Consumer Electronics Magazine. -2017. - 7(1), - C.18-28.

17. Farahani B. et al. Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare //Future Generation Computer Systems. – 2018. – T. 78. – C. 659-676.

18. Лебедев Г.С., Шадеркин И.А., Фомина И.В., Лисненко А.А., Рябков И.В., Качковский С.В., Мелаев Д.В. ИНТЕРНЕТ МЕДИЦИНСКИХ ВЕЩЕЙ: ПЕРВЫЕ ШАГИ ПО СИСТЕМАТИЗАЦИИ // Журнал телемедицины и электронного здравоохранения. - 2017. - №3 (5).

19. Минаев Антон Андреевич, Купер Дмитрий Витальевич, Иващенко Антон Владимирович Современные тенденции по реализации распределенной медицинской диагностики на базе Интернета вещей // Известия Самарского научного центра РАН. - 2016. - №4-4.

20. Бухарев Д.А., Вагин С.В., Соколов А.Н. Защита устройств интернета вещей от mirai-подобных вирусных программ-червей //Вестник УрФО. Безопасность в информационной сфере. – 2018. – №. 4. – С. 11-19.

21. Маслова М.А. Принципы безопасности интернета вещей //Вестник УрФО. Безопасность в информационной сфере. – 2018. – №. 3 (29). – С. 38-42.

22. Wang C., Liu X., Li W. Design and implementation of a secure cloud-based personal health record system using ciphertext-policy attribute-based encryption //International Journal of Intelligent Information and Database Systems 4. – 2013. – Т. 7. – №. 5. – С. 389-399.

23. A. Shamir. Identity-based cryptosystems and signature schemes. // Workshop on the theory and application of cryptographic techniques. – Springer, Berlin, Heidelberg. - 1984. – С. 47-53.

24. D. Boneh. M. Franklin. Identity-based encryption from the Weil pairing. //Annual international cryptology conference. - Springer, Berlin, Heidelberg. - 2001. – С. 213-229.

25. A. Sahai, and B. Waters. Fuzzy identity-based encryption. //Annual International Conference on the Theory and Applications of Cryptographic Techniques. - Springer, Berlin, Heidelberg. - 2005. – С. 457-473.

References

1. Proekt GOST Jelektronnaja medicinskaja karta. Terminy i opredelenija. Available at: http://portal.egisz.rosminzdrav.ru/materials/310 (accessed 1 November 2020).

2. S.N. Shcherbo, D.S. Shcherbo. 5P-medicine: precision medicine. Medicine Alphabet. 2015, vol. 18, no. 4, pp. 5 – 10.

3. Zakharov A., Potapov A., Zakharova I., Kotelnikov A., Panfilenko D. (2019, May). Infrastructure of the Electronic Health Record Data Management for Digital Patient Phenotype Creating. In 7th Scientific Conference on Information Technologies for Intelligent Decision-Making Support (ITIDS 2019).Atlantis Press.

4. Joyia G.J., Liaqat R.M., Farooq A., & Rehman S. (2017). Internet of Medical Things (IOMT): applications, benefits and future challenges in healthcare domain. J Commun, 12(4), 240-247.

5. Zakharov A. A., Potapov A. P., Zakharova I. G., Olennikov E. A. (2018, October). Telemetric Medical System to Support Cardiological Screening. In 2018 XIV International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE) (pp. 116-120).

6. Hassan M.K., El Desouky A.I., Elghamrawy S.M., & Sarhan A.M. (2019). A Hybrid Real-time remote monitoring framework with NB-WOA algorithm for patients with chronic diseases. Future Generation Computer Systems, 93, 77-95.

7. Khan, J. Y., Yuce, M. R., Bulger, G., & Harding, B. (2012). Wireless body area network (WBAN) design techniques and performance evaluation. Journal of medical systems, 36(3), 1441-1457.

8. ISO/TR 20514:2005 «Health informatics – Electronic health record – Definition, scope and context». Available at: https://www.iso.org/standard/39525.html (accessed 20 October 2020)

9. Zarubina T.V., Shvyrev S.L.,Solovyev V.G., Rauzina S.E., Radionov V.S., Penzin O.V., Surin M.Y. Integrated electronic health record: Status and Prospects.Vrachiinformacionnyetehnologi. 2016, no. 2.

10. Gehrmann, S., Dernoncourt, F., Li, Y., Carlson, E. T., Wu, J. T., Welt, J., Celi, L. A. (2018). Comparing deep learning and concept extraction based methods for patient phenotyping from clinical narratives. PloS one, 13(2), e0192360.

11. Alexander A. Zakharov, Alexander A. Kotelnikov, Alexander P. Potapov, Dmitry V. Panfilenko, Pavel Y. Gayduk. (2020, October) Information and Analytical Support for Biomedical Research in the Field of the Cardiovascular Disease Risk Prediction. In 8th Scientific Conference on Information Technologies for Intelligent Decision-Making Support (ITIDS 2020). Atlantis Press.

12. Masood, I., Wang, Y., Daud, A., Aljohani, N. R., &Dawood, H. (2018). Towards smart healthcare: Patient data privacy and security in sensor-cloud infrastructure. Wireless Communications and Mobile Computing, 2018.

13. Kołodziej, J., Grzonka, D., Widłak, A., &Kisielewicz, P. (2019). Ultra Wide Band Body Area Networks: Design and Integration with Computational Clouds. In High-Performance Modelling and Simulation for Big Data Applications (pp. 279-306). Springer, Cham.

14. Edemacu, K., Park, H. K., Jang, B., & Kim, J. W. (2019). Privacy Provision in Collaborative Ehealth With Attribute-Based Encryption: Survey, Challenges and Future Directions. IEEE Access, 7, 89614-89636.

15. Li, M., Yu, S., Ren, K., & Lou, W. (2010, September). Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. In International conference on security and privacy in communication systems (pp. 89-106). Springer, Berlin, Heidelberg.

16. Sundaravadivel, P., Kougianos, E., Mohanty, S. P., &Ganapathiraju, M. K. (2017). Everything you wanted to know about smart health care: Evaluating the different technologies and components of the Internet of Things for better health. IEEE Consumer Electronics Magazine, 7(1), 18-28.

17. Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., &Mankodiya, K. (2018). Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. Future Generation Computer Systems, 78, 659-676.

18. Lebedev G.S., Shaderkin I.A., Fomina I.V., Lisnenko A.A., Ryabkov I.V., Kachkovsky S.V., Melaev D.V. Internet of medical things: first steps in systematization. Zhurnal telemediciny i jelektronnogo zdravoohranenija. 2017, no. 3(5).

19. MinaevA.A., KuperD.V., Ivaschenko A.V. Moderntrendsindistributed medical diagnostics automation based on the Internet-of-things. Izvestija Samarskogo nauchnogo centra Rossijskoj akademiinauk. 2016, no. 4-4.

20. Bukharev DA, Vagin SV, Sokolov AN Protection of devices of the Internet of things from mirai-like virus worm programs // Journal of the Ural Federal District Information security. - 2018. - No. 4. - S. 11-19.

21. MASLOVA MA Security principles of the Internet of things // Journal of the Ural Federal District Information security Information security. - 2018. - No. 3 (29). - S. 38-42.

22. Wang, C., Liu, X., & Li, W. (2012, September). Implementing a personal health record cloud platform using ciphertext-policy attribute-based encryption. In 2012 Fourth International Conference on Intelligent Networking and Collaborative Systems (pp. 8-14). IEEE.

23. Shamir, A. (1984, August). Identity-based cryptosystems and signature schemes. In Workshop on the theory and application of cryptographic techniques (pp. 47-53). Springer, Berlin, Heidelberg.

24. Boneh, D., & Franklin, M. (2001, August). Identity-based encryption from the Weil pairing. In Annual international cryptology conference (pp. 213-229). Springer, Berlin, Heidelberg.

25. Sahai, A., & Waters, B. (2005, May). Fuzzy identity-based encryption. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 457-473). Springer, Berlin, Heidelberg.

ЗАХАРОВ Александр Анатольевич, доктор технических наук, профессор, заведующий базовой кафедрой «Безопасные информационные технологии Умного города», Институт математики и компьютерных наук, Тюменский государственный университет. 625003, г. Тюмень, ул. Володарского, 6. E-mail: azaharov@utmn.ru

ПОНОМАРЁВ Кирилл Юрьевич, старший преподаватель кафедры информационной безопасности, Институт математики и компьютерных наук, Тюменский государственный университет. 625003, г. Тюмень, ул. Володарского, 6. E-mail: drmckay-kirill@yandex.ru

ZAHAROV Aleksandr, D. Sc. (Tech.), Professor, Head of the Smart City's Secure Information Technologies Department, Institute of Mathematics & Computer Science, Tyumen State University. 625003, Tyumen, Volodarskogo, 6. E-mail: azaharov@utmn.ru

PONOMAREV Kirill, Senior Lecturer of Information Security Department, Institute of Mathematics & Computer Science, Tyumen State University. 625003, Tyumen, Volodarskogo, 6. E-mail: drmckay-kirill@yandex.ru