МИНОБРНАУКИ РОССИИ
Институт проблем передачи информации им. А.А. Харкевича РАН
Юго-Западный государственный университет
Институт программных систем им. А.К. Айламазяна РАН
Институт информационных технологий, Баку, Азербайджан

ОБЛАЧНЫЕ И РАСПРЕДЕЛЕННЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ

ОРВС – 2023

В РАМКАХ

НАЦИОНАЛЬНОГО СУПЕРКОМПЬЮТЕРНОГО ФОРУМА (НСКФ – 2023)

Сборник трудов 4-й международной научно-технической конференции

28 ноября – 1 декабря 2023 года

Переславль-Залесский 2024

УДК 621.383.68.3: 681.785
ББК 32.971.35

Облачные и распределенные вычислительные системы в электронном управлении. ОРВС – 2023: сборник трудов 4-й международной научно-технической конференции (28 ноября – 1 декабря 2023 года) / ред. кол.: И.И. Курочкин [и др.]; ИПС РАН. Переславль-Залесский. – Курск: Изд-во ЗАО «Университетская книга», 2024. - 127 с.

ISBN 978-5-00261-018-1
DOI 10.47581/2024.Oblokj-Raspredelenie-OPBC-2023

Сборник содержит труды 4-й международной научно-технической конференции «Облачные и распределенные вычислительные системы» (Переславль-Залесский, 28 ноября – 1 декабря 2023), проводимой в рамках Национального суперкомпьютерного форума (НСКФ – 2023). Целью конференции является ознакомление с имеющимися достижениями по созданию облачных и распределенных вычислительных систем и их внедрение в научные исследования, учебный процесс и промышленность.

Сборник предназначен для научных сотрудников, преподавателей, аспирантов и студентов вузов.

Издание осуществлено с авторских оригиналов.

Редакция не несет ответственности за ошибки авторов.

Материалы для публикации одобрены программным комитетом Международной научно-технической конференции.

ISBN 978-5-00261-018-1

УДК 621.383.68.3: 681.785
ББК 32.971.35

Содержание

Секция «Решение задач оптимизации в среде высокопроизводительных вычислений»

Алекперов О.Р.

Институт информационных технологий, Баку, Азербайджан

ПРОБЛЕМЫ БЕЗОПАСНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ В МОБИЛЬНЫХ ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

Аннотация. В статье подробно исследуются проблемы, связанные с безопасностью и конфиденциальностью, возникающие при использовании мобильных облачных вычислений (МОВ), а также предлагаются предложения и механизмы решения вопросов безопасности. Из-за использования мобильных вычислений, облачных вычислений и беспроводной связи мы сталкиваемся со многими проблемами безопасности в мобильных облачных вычислениях. Проблемы безопасности МОВ включают проблемы безопасности, возникающие в облачных вычислениях, мобильных вычислениях и беспроводных сетях. В МОВ программные приложения и данные располагаются не на мобильных устройствах, а в основном на удаленных облачных серверах, хранятся, обрабатываются и предоставляют услуги пользователям в соответствии с их требованиями. Безопасность мобильных облачных вычислений охватывает широкий спектр аспектов безопасности и затрагивает все компоненты облака (мобильные устройства, сетевую инфраструктуру, облачные серверы и т. д.).

Ключевые слова: мобильные облачные вычисления, беспроводные сети, конфиденциальность, аутентификация.

Введение

Безопасность мобильных облачных вычислений охватывает широкий спектр аспектов безопасности и затрагивает все компоненты облака (мобильные устройства, сетевую инфраструктуру, облачные серверы и т.д.). К вопросам безопасности относятся безопасность и конфиденциальность персональных данных мобильных пользователей, безопасность облачных сервисов, анализ рисков облачных конфигураций, аудит расчетов и управления данными, регистрация (учет) распределения ресурсов, аутентификация пользователей и устройств и т.д. Среди всех этих вопросов мы сосредоточим внимание на вопросах полноты (целостности), конфиденциальности и доступности, которые тесно связаны с реализацией дополнений программного обеспечения. Целостность означает предотвращение потери или изменения данных во время передачи по общедоступной сети. Проблема полноты возникает из-за того, что мобильные устройства менее надежны и мобильные приложения загружаются в облако. Результаты, полученные при использовании ненадежных устройств и загруженных программ, должны быть проверены и проверены для обеспечения полноты. Конфиденциальность является ключевым требованием в мобильных облачных сетях, поскольку данные мобильных пользователей обрабатываются через общедоступную сеть и хранятся на ее серверах. Таким образом, существует высокая вероятность доступа злоумышленников к данным мобильных пользователей, поэтому вопрос конфиденциальности является большой проблемой для поставщиков (провайдеров) мобильных облачных услуг. Проблема конфиденциальности связана с разделением (отладкой) кода и данных в настройках облака. Персональные данные пользователей, хранящиеся на их мобильных устройствах, можно получить из облака в случае их утери, поскольку варианты резервного копирования данных уже размещены в облаке. Доступность означает, что поставщики облачных услуг должны иметь возможность предоставлять данные пользователям круглосуточно и без выходных. Существуют различ-

ные атаки, которые влияют на доступность, но поставщики услуг мобильных облачных вычислений должны предотвращать их и всегда обеспечивать доступность услуги для мобильных пользователей. Проблемы доступности могут возникнуть в мобильных вычислительных системах из-за ограниченности ресурсов (например, каналов мобильного доступа). В облаке злоумышленники повышают доступность программного обеспечения, переполняя ресурсы ненужными запросами.

Меры безопасности в мобильных облачных вычислениях обычно требуют дополнительных процедур безопасности для шифрования загруженных мобильных приложений и данных, аутентификации мобильных устройств и пользователей, а также поддержания безопасной связи между мобильными устройствами и облаком путем обмена и обновления учетных данных (между пользователем и поставщиком). Таким образом, безопасность требует больше ресурсов для хранения учетных данных и выполнения функций безопасности, что приводит к дополнительным затратам с точки зрения времени обработки и энергопотребления.

Архитектуры мобильных облачных вычислений уязвимы к различным и более широким спектрам атак, чем традиционные вычислительные системы [1]. Это обусловлено, прежде всего, следующими причинами:

- **Мобильные устройства.** Мобильные устройства, такие как смартфоны и планшеты, часто используются в разнообразных средах и подключаются к различным сетям. Они могут быть потеряны, украдены или подвергнуты атакам.
- **Беспроводные сети.** Мобильные устройства часто подключаются к открытым или недостаточно защищенным беспроводным сетям, что делает их более уязвимыми для атак на сетевом уровне.
- **Передача данных.** Мобильные устройства передают данные через интернет и мобильные сети, что предоставляет дополнительные возможности для перехвата и атак на данные.
- **Мобильные приложения.** Мобильные приложения могут быть уязвимыми к атакам, и некачественные приложения могут собирать и передавать личные данные без согласия пользователя.
- **Комплексность архитектуры.** Мобильные облачные вычисления включают в себя множество компонентов, в том числе мобильные устройства, облачные серверы, сети и приложения. Это создает больше точек входа для потенциальных атак.
- **Политики и управление безопасностью.** Управление безопасностью в среде мобильных облачных вычислений может быть более сложным из-за разнообразия устройств и местоположений пользователей.
- **Интеграция облачных сервисов.** Мобильные устройства часто интегрируются с различными облачными сервисами. Это увеличивает поверхность атаки, так как данные перемещаются между устройством и облаком.
- **Потеря или кража устройства.** Потеря или кража мобильного устройства может представлять серьезную угрозу, если данные на устройстве не защищены или если нет возможности удаленного стирания данных.

Применение современных методов шифрования, сетевых мер безопасности, усиленного управления доступом и обучения пользователей может снизить уязвимость и обеспечить более надежную защиту в такой сложной среде.

Проблемы конфиденциальности на мобильных устройствах

Безопасность и конфиденциальность данных. Чтобы защитить безопасность и конфиденциальность данных, поставщики облачных услуг должны внедрить процедуры, позволяющие определить, где и в каком состоянии находятся данные. Поставщики облачных услуг должны информировать заказчика о протоколах, обеспечивающих безопасность и кон-

фиденциальность данных пользователей, находящихся в облаке. Пользователи мобильных облаков серьезно обеспокоены конфиденциальностью и безопасностью своих данных, расположенных на облачных серверах. Вопрос защиты конфиденциальности данных является одной из проблем, которая не позволяет пользователям размещать свои данные в облаке (полагаясь на облачных провайдеров) [2]. Угрозы конфиденциальности в мобильных облачных вычислениях связаны с возможностью несанкционированного доступа, использования или раскрытия конфиденциальной информации, которая передается или хранится в облаке через мобильные устройства. Вот некоторые из основных угроз конфиденциальности в этой области:

- **Утечка личных данных.** Мобильные приложения и облачные службы могут собирать и хранить личные данные пользователей, такие как имена, адреса, номера телефонов и адреса электронной почты. Нарушение безопасности может привести к утечке этих личных данных.
- **Угрозы в сети.** Передача данных между мобильными устройствами и серверами облачных провайдеров через интернет может подвергать данные риску перехвата или прослушивания. Необходимо обеспечить безопасность передачи данных с использованием шифрования.
- **Недостаточная политика конфиденциальности.** Многие пользователи могут не обращать внимание на политику конфиденциальности мобильных приложений и услуг облачных провайдеров, что может привести к несанкционированному сбору и использованию их данных.
- **Вредоносные приложения.** Злоумышленники могут создавать вредоносные мобильные приложения, которые могут собирать и передавать конфиденциальную информацию без согласия пользователя.
- **Утеря или кража устройства.** Потеря или кража мобильного устройства может означать доступ к конфиденциальным данным, если устройство не было защищено паролем или если данные не были зашифрованы.
- **Отсутствие контроля над данными.** Если пользователь не имеет полного контроля над тем, как его данные собираются и используются, это может привести к нарушению конфиденциальности.
- **Утечка данных из облака.** Нарушение безопасности на стороне облачного провайдера может привести к утечке данных, так как многие пользовательские данные хранятся в облаке.
- **Социальная инженерия.** Злоумышленники могут использовать методы социальной инженерии для обмана пользователей и получения доступа к их учетным записям и данным.

Для защиты конфиденциальности данных в мобильных облачных вычислениях важно применять меры безопасности, такие как соблюдение политик конфиденциальности, использование шифрования, управление разрешениями приложений, регулярное обновление приложений и операционных систем, а также обучение пользователей основам безопасности и конфиденциальности.

Конфиденциальность — одна из серьезных проблем в мобильных облачных вычислениях. Обнаружение географического местоположения мобильного пользователя представляет угрозу безопасности личной информации пользователя (даты рождения, данных кредитной карты, истории болезни и т.д.) [3]. Если мобильные устройства используют технологию GPS, это позволяет очень легко определить их физическое местоположение. Провайдеры могут передавать конфиденциальную информацию пользователей государственным органам по запросу без их согласия. После того как данные пользователя будут размещены на облачных серверах, должна быть гарантия, что доступ к этим данным будет ограничен теми, кто уполномочен поставщиками. Доступ к пользовательским данным неавторизованного облачного персонала представляет собой потенциальный риск для облачных данных отдельных лиц. Клиенты должны быть уверены и должны применяться соответствующие правила, а политики и процедуры конфиденциальности должны обеспечивать безопасность информации пользователей на облачных серверах. Пользователи облака должны быть уверены, что данные, хранящиеся в облаке, надежно защищены. Для защиты конфиденциальности данных пользователей были предложены многочисленные политики и схемы, которые позволяют провайдерам реализовывать ряд строгих процедур контроля [4]. Компании, которые собирают информацию и данные, должны принять и соблюдать определенные политики и процедуры для их безопасной обработки, хранения и удаления. В облаке есть законные пользователи и внутренние сотрудники. Иногда они пытаются украсть или неправильно использовать данные и информацию. Также внешние пользователи могут получить доступ к персональным данным из облака, поскольку такие стороны становятся проблемой для надежности облачной платформы. Меры по распределению риска нарушения конфиденциальности между взаимосвязанными системами, мониторинга, кражи и мошенничества могут быть сокращены. Разработав политику использования социальных сетей и внедрив несколько процедур безопасности для защиты инфраструктуры, компании могут самостоятельно решать проблемы безопасности. Наиболее эффективным способом защиты целостности и конфиденциальности данных является шифрование. Шифрование защищает данные от внешнего вмешательства в процессе их хранения, передачи и обработки [5]. Решение проблем конфиденциальности в мобильных облачных вычислениях требует комплексного подхода и применения различных мер безопасности. Вот некоторые решения и меры для обеспечения конфиденциальности данных в этой среде.

- **Шифрование данных.** Использование шифрования данных в покое и в движении. Это защитит данные от несанкционированного доступа в случае утери устройства или перехвата данных в сети.
- **Многофакторная аутентификация.** Внедрение многофакторной аутентификации для усиления процесса входа в облачные учетные записи. Это усложнит задачу злоумышленников при попытке взлома учетных записей.
- **Правильное управление доступом.** Установление жесткой политики доступа и аутентификации для контроля, кто и как может получать доступ к данным и приложениям.
- **Контроль разрешений приложений.** Пользователи должны иметь полный контроль над тем, какие разрешения предоставляют мобильным приложениям. Ограничение разрешения на минимум и предоставление их только тогда, когда они необходимы.
- **Безопасное хранение данных.** Для мобильных устройств установление шифрования данных на уровне устройства и использование безопасных методов хранения данных.
- **Политика конфиденциальности.** Необходимо убедиться, что мобильные приложения и облачные провайдеры следуют строгим политикам конфиденциальности и политикам обработки данных.
- **Защита от вредоносных приложений.** Использование антивирусного и антималварного программного обеспечения на мобильных устройствах для выявления и удаления вредоносных приложений.
- **Защита от социальной инженерии.** Обучение пользователей методам социальной инженерии, чтобы они могли узнавать попытки обмана.

Комбинирование этих мер позволяет усилить безопасность и конфиденциальность в мобильных облачных вычислениях, предостерегая от угроз и рисков, которые могут возникнуть в этой сложной среде.

Заключение

На мобильные облачные вычисления могут повлиять перебои в обслуживании или проблемы с безопасностью на мобильных устройствах, облачных объектах или в публичной среде. Широкий спектр исследований демонстрирует различные формы проблем безопасности и конфиденциальности в облачных и мобильных облачных вычислениях. Однако не су-

ществует простого и универсального решения, которое можно было бы применить к этому методу. Облачная инфраструктура состоит из разнообразных систем и технологий, что усложняет реализацию стандартного механизма безопасности или системы. Отсутствие структуры безопасности облачных вычислений делает облачные сервисы уязвимыми для различных видов рисков безопасности и конфиденциальности, таких как атаки между виртуальными машинами, внедрение вредоносных команд, нежелательный доступ, потеря и повреждение данных. В этой статье мы последовательно обсудили проблемы безопасности и конфиденциальности мобильных облачных вычислений. Затем мы предоставили подходящие системы, такие как защита от вредоносного ПО, безопасность конфиденциальности, сетевое распределение и шифрование, контроль доступа и т.д. в зависимости от проблем. Будем надеяться, что с обновлением новейших технологий мобильные облачные вычисления станут более надежными благодаря повышению безопасности и конфиденциальности системы.

Библиографический список

1. Shim Y.C. Effects of cloudlets on interactive applications in mobile cloud computing environments // International Journal of Advanced Computer Technology, 2015, vol.4, no.1, pp.54–62.
2. Ələkbərov R.Q., Ələkbərov O.R. Mobil hesablama buludlarında təhlükəsizlik və konfidensiallıq məsələləri // İnformasiya Texnologiyaları Problemləri, 2018, №1, s.92–102.
3. Bahar A.N, Habib A., Islam M. Security architecture for mobile cloud computing // International Journal of Scientific Knowledge Computing and Information Technology, 2013, vol.3, no.3, pp.11–17.
4. Schoo P., Fusenig V., Souza V., Melo M., Murray P., Debar H., Medhioub H., Zeghlach D. Challenges for Cloud Networking Security // 2nd International ICST Conference on Mobile Networks and Management, 2010, pp.2–16.
5. Pang Z., Sun L., Wang Z., Tian E., Yang S. A Survey of Cloudlet based Mobile Computing // 2015 International Conference on Cloud Computing and Big Data, 2015, pp.268–275.

Волошинов В.В., Соколов А.В.

Институт проблем передачи информации им. А.А Харкевича РАН, Москва

РАЗВИТИЕ МЕТОДОВ КУСОЧНО ЛИНЕЙНЫХ АППРОКСИМАЦИЙ В ОБРАТНЫХ ЗАДАЧАХ С ДИФФЕРЕНЦИАЛЬНЫМИ УРАВНЕНИЯМИ

Аннотация. Численные методы SvF-технологии сбалансированной идентификации развиваются для математических моделей с дифференциальными уравнениями (ДУ), правая часть которых есть композиция неизвестных функций (подлежащих идентификации). Предлагаемый подход основан на сеточном представлении обеих функций и на кусочно линейной аппроксимации (КЛА) функции правой части ДУ. Рассматриваются один из способов применения КЛА для дискретизации обратной задачи в виде конечномерной задачи математического программирования (ЗМП): путем «сглаживания» кусочно линейной функции в точках излома. Это приводит к ЗМП с гладкими функциями, где эффективны алгоритмы локальной оптимизации, но трудно искать глобальный оптимум. Данный подход применяется к обыкновенным ДУ с одной переменной и к автономным ДУ с двумя переменными.

Ключевые слова: сбалансированная идентификация, дискретизация дифференциальных уравнений, кусочно-линейные аппроксимации.

Введение

Работа посвящена развитию численных методов SvF-технологии [1, 2, 3] сбалансированной идентификации математических моделей, в части дискретизации дифференциальных уравнений (ДУ) исследуемой модели, когда в правой части ДУ стоит композиция неизвестных функций. В статье [4] были рассмотрены возможные приемы дискретизации для случая, когда эти дифференциальные уравнения являются автономными. Рассматривался пример следующей обратной задачи: определить функции *x(t)* на интервале $[t_{\mathbf{L}}, t_{\mathbf{U}}]$ и функцию *F(x)* предполагая, что эти функции связаны дифференциальным уравнением (ДУ) 1-го или 2-го порядка на основании набора неточных (!) измерений функции *x(t)* на заданном наборе значений {*td*}

$$\begin{aligned}&\dot{x}=F(x(t)) \text{ или } \ddot{x}=F(x(t)),\ x\in\mathbb{R}^1,\ t\in[t_{\mathbf{L}},t_{\mathbf{U}}],\\&\{(\bar{x}_d,t_d):d=1{:}N_d\},\bar{x}_d=x(t_d)\pm\mathsf{err}\end{aligned} \tag{1}$$

Опуская важные детали SvF-технологии, в этом случае она требует многократного решения задач оптимизации (фактически, вариационных задач) вида (2), где первое слагаемое целевой функции отвечает за точность приближения решения *x(t)* к экспериментальным данным, а второе, с заданным коэффициентом регуляризации α — за гладкость неизвестной заранее функции *F(x)*. В ходе выполнения сценария SvF-расчетов требуется решать задачу (2) для различных значений коэффициента регуляризации α.

$$\begin{aligned}&\frac{1}{D}\sum_{d=1:D}(\bar{x}_d-x(t_d))^2+\alpha\int_{x_{\mathbf{L}}}^{x_{\mathbf{U}}}\left(F''(x)\right)^2dx\to\min_{x(\cdot),F(\cdot)},\\&\dot{x}=F(x(t)) \text{ или } \ddot{x}=F(x(t)),\ t\in[t_{\mathbf{L}},t_{\mathbf{U}}],\\&x(\cdot)\in\mathrm{C}^2[t_{\mathbf{L}},t_{\mathbf{U}}],F(\cdot)\in\mathrm{C}^2[x_{\mathbf{L}},x_{\mathbf{U}}])).\end{aligned} \tag{2}$$

На практике, вместо вариационной задачи (2) решается задача математического программирования (ЗМП), полученная в результате дискретизации интегралов и дифференциальных уравнений. В данной статье будут рассмотрены возможные способы дискретизации