Исследование вопросов безопасности и конфиденциальности в туманных вычислениях

Авторы: Mohana H.K., Nethra H.S., Devaraju Dr. J.T.

Автор перевода: Максименко Д.Л.

Источник: https://www.elibrary.ru/item.asp?id=37604930

Введение

В последнее десятилетие развитие интернет-услуг привело к радикальным изменениям в быстрорастущих облачных вычислениях и распространенных мобильных устройствах. Мотивированные этими двумя тенденциями, было проведено множество исследований для поддержки мобильных облачных вычислений, которые объединяют облако и мобильные устройства, чтобы эффективно переносить интенсивные вычислительные задачи с устройств с ограниченными ресурсами в облако и быстро получать результаты [1]. Однако из-за значительного физического расстояния между центрами обработки данных (DC) поставщика облачных услуг и конечным пользователем (EC) облачные вычисления страдают от значительной сквозной задержки, перегрузки трафика, обработки огромных объемов данных, затрат на связь. Кроме того, непредсказуемая задержка в сети, особенно в мобильной среде, облачные вычисления могут не соответствовать строгим требованиям задержки, безопасности и конфиденциальности или географически ограниченных приложений [1, 2]. Таким образом, возникает необходимость в туманных вычислениях.

Технология туманных вычислений была впервые инициирована Cisco для распространения облачных вычислений на границу сети с меньшими задержками и безопасностью. Туманные вычисления — это платформа с высокой степенью виртуализации, которая обеспечивает вычисления, хранение и сетевые услуги между EC и DC в рамках традиционных облачных вычислений [2]. Слой тумана включает интеллектуальные шлюзы,

маршрутизаторы и сами конечные устройства, и его можно рассматривать как спустившееся облако для эффективного обслуживания ближайших клиентов. Туманные вычисления позволяют устройствам с легкостью подключаться напрямую к месту назначения и позволяют им обрабатывать свои соединения и задачи, используя любую технику без сетевой магистральной инфраструктуры. Следовательно, туманные вычисления улучшают качество обслуживания, сокращают задержку и предлагают более удовлетворительное взаимодействие с пользователем. Дальнейшие туманные вычисления плавно поддерживают появляющиеся свойства Интернета вещей (IoT), такие как автомобили, бытовая техника, умные города, интеллектуальные сети, которые встроены в датчики, позволяющие им отправлять или получать данные. Туманные вычисления могут быть реализованы с использованием базовой системы связи вместо тяжелой магистральной сети.

Таким образом, они имеют более плотное покрытие. Это преимущество упрощает выполнение операций с большими данными в режиме реального времени с возможностью поддержки миллиардов узлов в высоко динамичных и разнообразных средах. Он естественным образом соединяет Интернет вещей (IoT) с существующей вычислительной инфраструктурой Интернета. Текущие и будущие приложения, требующие туманных вычислений, такие как транспортные средства, автопилоты, интеллектуальные сети, беспроводные сенсорные и исполнительные сети, умные дома, умные города, подключенное производство, подключенные нефтегазовые системы, мобильные системы здравоохранения [1, 3].

Однако характеристики туманных вычислений порождают новые проблемы безопасности и конфиденциальности. Следовательно, в этой работе обсуждалось несколько вопросов безопасности и конфиденциальности, связанных с природой туманной архитектуры. Оставшаяся часть текста организована следующим образом. В Разделе 2 дается краткое описание «Обзор архитектуры туманных вычислений». Раздел 3 дает подробное

представление о проблемах безопасности и конфиденциальности в туманных вычислениях, а Раздел 4 завершает статью.

1. Архитектура туманных вычислений

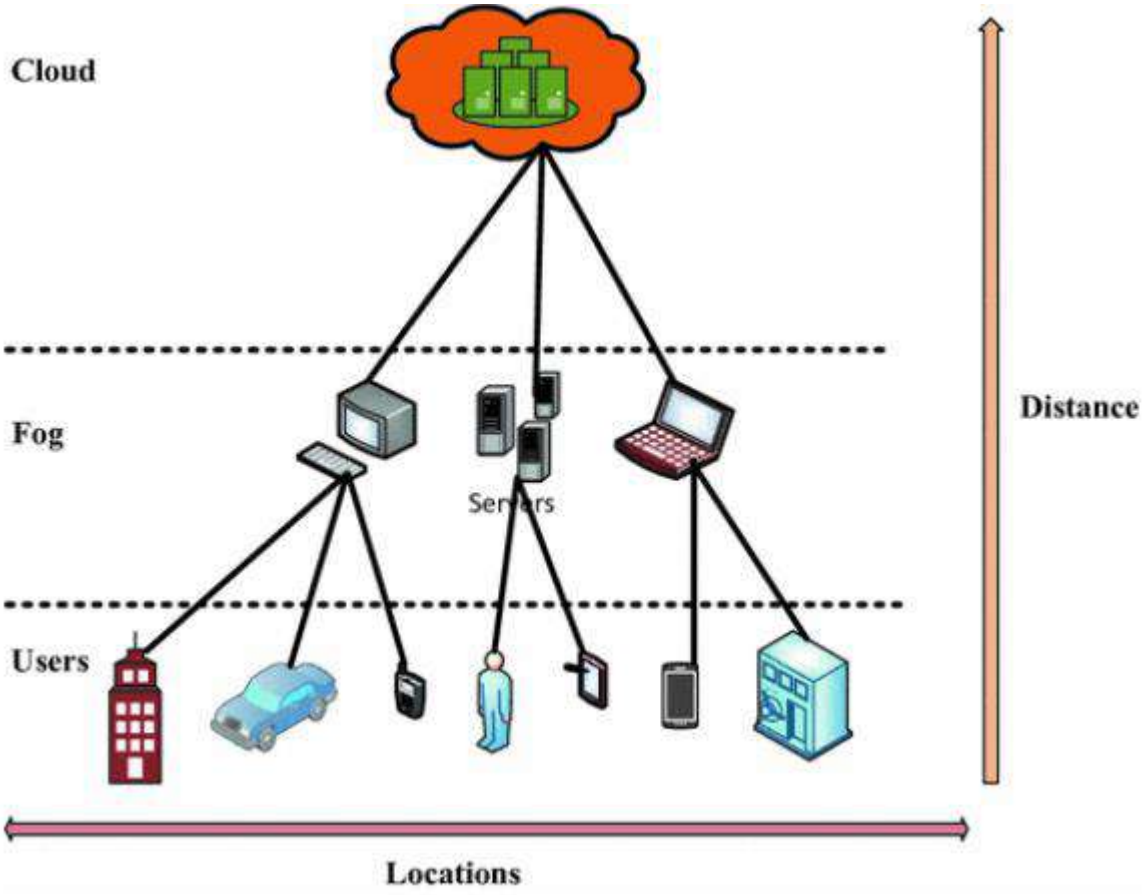

Рисунок 1 - Иерархическая архитектура туманных вычислений

Туманные вычисления - это трехуровневая архитектура, которая действует как промежуточный уровень между уже существующими облачными сетями и устройствами конечных пользователей [4]. Существующая облачная сеть обычно имеет ядро, известное как центры обработки данных, которое имеет соединение с конечным пользователем через сеть, такую как Интернет. Туман ликвидирует разрыв между конечным пользователем и ядром, создавая между ними еще один слой [5]. Первый уровень в этой архитектуре состоит из устройств с поддержкой Интернета вещей (IoT), включая узлы датчиков, интеллектуальные портативные устройства конечных пользователей, такие как смартфоны, планшеты и смарт-

часы, и другие. Эти конечные устройства часто называют терминальными узлами (TN). Предполагается, что эти TN оснащены глобальной системой позиционирования (GPS) [2, 5].

Второй уровень в этой архитектуре называется уровнем туманных вычислений. Узлы тумана на этом уровне состоят из сетевых устройств, таких как маршрутизатор, шлюз, коммутатор и точки доступа (AP). Эти туманные узлы могут совместно использовать хранилище и вычислительные ресурсы. Они обрабатывают запросы, чувствительные к задержке и отвечают конечным узлам в режиме реального времени. Обычно они находятся на маленьком расстоянии от конечного узла и подключаются с помощью готовых беспроводных интерфейсов, таких как WI-FI и Bluetooth. Такие устройства, как маршрутизаторы и базовые станции, могут работать как серверы на этом уровне, расширяя свои вычислительные возможности и возможности хранения. Самым верхним уровнем по-прежнему является уровень облака, состоящий из основных устройств, таких как центры обработки данных, которые будут предоставлять мощную вычислительную инфраструктуру для конечных пользователей и подключены к серверам на втором уровне с помощью технологий 3G/4G/широкополосной связи. Огромный объем данных после обработки слоем тумана хранится в облачных центрах, и передовые технологии интеллектуального анализа данных используются для получения систематического и долгосрочного анализа, который является неотъемлемой частью умных городов [2, 4, 5].

2. Вопросы безопасности и конфиденциальности в туманных вычислениях

Туманные вычисления в большей степени обеспечивают безопасность облачной среды. Однако отличительные характеристики чувствительности к местоположению, возможности беспроводного подключения и географической доступности создают новые проблемы и проблемы безопасности. Следовательно, в этом исследовании была предпринята

попытка обсудить несколько вопросов безопасности и конфиденциальности в туманных вычислениях.

2.1 Авторизация и аутентификация: в туманных вычислениях начальным шагом безопасности является идентификация каждого узла и подтверждение того, является ли присоединенный узел аутентичным или нет. Поскольку туманные вычисления позволяют миллиардам граничных устройств подключаться к сети через узлы для обработки данных и общаться с удаленным пользователем. Следовательно, очень важно иметь идентификацию каждого подключенного узла как проверенного узла. Это важно для предотвращения проникновения неавторизованных узлов. После идентификации гарантия безопасности должна быть определена для каждого подключенного узла, потому что в туманных вычислениях все узлы могут иметь разные причины подключения [5].

2.2 Сетевая безопасность: туманные вычисления привели к более серьезным проблемам в безопасности, поскольку затронуты другие передовые технологии беспроводного доступа. Эти проблемы обычно возникают между туманным узлом и централизованной системой. В туманных вычислениях узлы находятся на границе сети для предоставления услуг. Таким образом, сетевым поставщикам необходимо управлять узлами, чтобы они работали на низком уровне абстракции для сетевых сервисов. Таким образом, разработчик сети использует механизм SDN (Software Defined Networking), чтобы упростить управление и повысить масштабируемость за счет снижения стоимости сети. Дальнейшая система мониторинга сети и обнаружения вторжений необходима для мониторинга сетевого трафика, системы изоляции трафика и приоритизации для предотвращения общих ресурсов. Кроме того, система управления доступом к сетевым ресурсам важна для приложений реального времени и системы совместного использования сети для маршрутизатора туманного узла, чтобы она была открыта для пользователей, учитывая также вопросы безопасности [6].

2.3 Механизм управления доступом: Управление доступом — это метод безопасности чтобы убедиться, что только авторизованные объекты могут получить доступ к гарантированному ресурсу. В условиях туманных вычислений контроль доступа жизненно важен, чтобы убедиться, что узел находится в пределах ограничений локальной сети, а авторизация гарантирует, что узел имеет право доступа, поскольку он выполняет все необходимые условия, чтобы быть частью сети. Следовательно, система безопасности должна быть способна реализовать механизм контроля доступа с гарантированной авторизацией [5, 7].

2.4 Обнаружение вторжений: методы обнаружения вторжений обнаруживают ненадлежащее поведение пользователей или устройств и уведомляют других в сети о необходимости принятия соответствующих действий. Характеристики сред туманных вычислений затрудняют обнаружение атак внутренних и внешних нарушителей на таких универсальных платформах. Кроме того, сложная конструкция методов обнаружения вторжений в сочетании с ограниченными ресурсами является еще одной сложной задачей. Теперь ключевая задача состоит в том, как спроектировать и настроить систему обнаружения, которая может работать в крупномасштабных, широко географически распределенных и высокомобильных средах [7] .

2.5. Man-in-the-Middle Attack: Атаку Man-in-the-Middle легко начать, но трудно устранить. В реальном мире ни один из методов зашифрованной связи не защищен от этой атаки, поскольку злоумышленники могут настроить терминал и воспроизвести обмен данными без дешифрования. В различных обстоятельствах сложные методы шифрования и дешифрования могут не подходить, например, в системе 3G методы шифрования и дешифрования потребляют много энергии батареи мобильного устройства. В туманных вычислениях подвергаются риску этой атаки, поскольку многие пользователи Интернета общаются друг с другом с помощью MSN (Micro Soft Network), а

эти данные не зашифрованы и могут быть изменены. Дальнейшая работа необходима для противодействия атаке в туманных вычислениях [8, 9].

2.6 Защита данных: в туманных вычислениях данные от устройств IoT отправляются в ближайшие узлы тумана. Однако из-за нехватки спектра очень сложно обрабатывать большой объем данных от пользователей. Следовательно, данные разделяются на различные части и отправляются в несколько узлов тумана для обработки, а содержимое данных должно быть проанализировано без раскрытия. Перед началом вычислений узлы тумана должны быть доверены друг другу, потому что нет узла тумана, который управляет другим узлом тумана. Дальнейшее распространение и обработка данных необходимо объединить. Однако из-за ограниченных ресурсов сложно зашифровать или расшифровать данные пользователей. Таким образом, в туманных вычислениях важны алгоритмы шифрования или методы маскировки [8]. Также для облегчения работы с большим объемом данных узлы тумана, которые аутентифицируются облаком, должны быть расположены только в среде тумана. Требуется протокол аутентификации [8].

2.7 Конфиденциальность данных и местоположения: в туманных вычислениях конфиденциальность данных находится под угрозой, поскольку пользовательские данные передаются на аутсорсинг узлам тумана, размещаются рядом с конечными пользователями и географически распределены. Кроме того, местоположение конечных пользователей находится под угрозой из-за пространственной корреляции между узлами тумана и пользователями. Поскольку пользователям обычно назначают свои задачи на ближайший узел тумана, узел предполагает, что пользователь закрыт для этого узла и находится вдали от других. Проблема, связанная с этой проблемой, заключается в том, чтобы скрыть пользователей идентификации от узла тумана. Эта проблема связана с первой проблемой, потому что сокрытие личности пользователя необходимо для связи с удаленным пользователем. Это противоречит целям разработки туманных вычислений.

Эта проблема не может быть решена с использованием существующих методов сохранения конфиденциальности в туманных вычислениях. Для сокрытия истинной личности пользователей требуется участие третьей стороны в любом существующем протоколе сохранения конфиденциальности. Следовательно, цель проекта по уменьшению задержки путем выполнения вычислений в ближайшем туманном узле нарушена. Решение этой проблемы заключается в том, что предприятия, использующие туманные службы для управления своими машинами, могут захотеть скрыть свои шаблоны использования, скрывая свою личность [10]. В туманных вычислениях конфиденциальность также является основной проблемой методов безопасности, чтобы обеспечить конфиденциальность конечным узлам. Утечка конфиденциальности пользовательской информации, такой как данные, местоположение и использование, привлекает внимание исследовательского сообщества. Поскольку пользователи имеют право делиться своей информацией с кем хотят, а не с другими. Точно так же они имеют право держать это в секрете от других, чтобы избежать того, какими услугами они пользуются в данный момент. Они имеют право хранить в секрете свое местоположение от других, которые могут раскрыть о них много информации. Туманные вычисления должны гарантировать все эти права, чтобы сделать эту систему более надежной и защищенной [5, 7].

Заключение. Туманные вычисления — это парадигма распределенных вычислений, добавленная к интеллектуальной технологии для расширения услуг облачных вычислений до границ сети для поддержки более низкой задержки и лучшего качества обслуживания. Однако несколько отличительных характеристик туманных вычислений могут вызвать новые угрозы безопасности и конфиденциальности. Следовательно, в этой статье была сделана попытка обсудить основные проблемы безопасности и конфиденциальности, такие как вопросы доверия и аутентификации, контроль доступа, обнаружение вторжений, защита данных, конфиденциальность данных и местоположения. Чтобы преодолеть эти проблемы, необходимо

внести вклад в исследования для решения различных задач туманных вычислений для поддержки более качественных услуг в реальном и не реальном времени.

Список источников:

1. Songqing Chen, Tao Zhang, Weisong Shi “Fog Computing”.
2. 2. Mithun Mukherjee, Rakesh Matam, Lei Shu, Leandros Maglaras, Mohamed Amine Ferrag, Nikumani Choudhury, And Vikas Kumar, “Security and Privacy in Fog Computing: Challenges”.
3. Intense School “Introduction to Fog Computing”, February 25, 2016.
4. Ning Chen, Yu Chen, Xinyue Ye, Haibin Ling, Sejun Song and Chin-Tser Huang “Smart City Surveillance in Fog Computing”.
5. Bushra Zaheer Abbasi, Munam Ali Shah “Fog Computing: Security Issues, Solutions and Robust Practices”, Proceedings of the 23rd International Conference on Automation & Computing, University of Hudders field,Hudders field, UK, 7-8 September 2017
6. Praveen Kumar, Nabeel Zaidi and Tanupriya Choudhur, “Fog Computing: Common Security Issues and Proposed Countermeasures”, Proceedings of the SMART -2016, IEEE Conference ID: 39669, 5th International Conference on System Modeling & Advancement in Research Trends, 25th to 27th November, 2016.
7. rwa Alrawais, Abdulrahman Alhothaily, Chunqiang Hu, and Xiuzhen Cheng Fog Computing for the Internet of Things: Security and Privacy Issues
8. Ivan Stojmenovic, Sheng Wen, “The Fog Computing Paradigm: Scenarios and Security Issues”, Proceedings of the 2014 Federated Conference on Computer Science and Information Systems –pp. 1–8.
9. Nabil Abubaker, Leonard Dervishi and Erman Ayday, “Privacy-Preserving Fog Computing Paradigm”, The 3rd IEEE Workshop on Security and Privacy in the Cloud (SPC 2017).