Вестник Евразийской науки / The Eurasian Scientific Journal https://esj.today

2018, №3, Том 10 / 2018, No 3, Vol 10 https://esj.today/issue-3-2018.html

URL статьи: https://esj.today/PDF/79ITVN318.pdf

Статья поступила в редакцию 31.05.2018; опубликована 23.07.2018

Ссылка для цитирования этой статьи:
Рябоконь В.В., Кузькин А.А., Тутов С.Ю., Махов А.С. Обзор угроз информационной безопасности в концепции граничных вычислений // Вестник Евразийской науки, 2018 №3, https://esj.today/PDF/79ITVN318.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

For citation:
Ryabokon' V.V., Kuzkin A.A., Tutov S.Yu., Mahov A.S. (2018). Review of information security threats in the concept of edge computing. *The Eurasian Scientific Journal*, [online] 3(10). Available at: https://esj.today/PDF/79ITVN318.pdf (in Russian)

УДК 004.75

ГРНТИ 20.15.05

Рябоконь Владимир Владимирович
ФГКВОУ ВО «Академия Федеральной службы охраны Российской Федерации», Орёл, Россия
Сотрудник
Кандидат технических наук
E-mail: mimicria@mail.ru
РИНЦ: http://elibrary.ru/author_profile.asp?id=860017

Кузькин Александр Александрович
ФГКВОУ ВО «Академия Федеральной службы охраны Российской Федерации», Орёл, Россия
Сотрудник
Кандидат технических наук
E-mail: kuzmich313@mail.ru
РИНЦ: http://elibrary.ru/author_profile.asp?id=930410

Тутов Станислав Юрьевич
ФГКВОУ ВО «Академия Федеральной службы охраны Российской Федерации», Орёл, Россия
Сотрудник
E-mail: tutoff@yandex.ru

Махов Александр Сергеевич
ФГКВОУ ВО «Академия Федеральной службы охраны Российской Федерации», Орёл, Россия
Студент
E-mail: dzot952@mail.ru

Обзор угроз информационной безопасности в концепции граничных вычислений

Аннотация. В статье представлен обзор технологии граничных вычислений. В связи с широким распространением информационных сетей и увеличением массивов данных, генерируемых граничными устройствами, традиционная централизованная модель облачных вычислений становится неэффективной в связи с ограничением пропускной способности сети и увеличением количества вычислительных операций. Именно поэтому в последние годы перспективной стала технология граничных вычислений. Основными сервисами данной технологии являются: представление контента, вычисления в режиме реального времени и параллельная обработка данных. Однако, в таких сетях появляются новые проблемы, такие как, безопасности данных и сохранение конфиденциальности. Несмотря на важность граничных

вычислений, в этом направлении произведено недостаточно исследований в области безопасности данных и сохранения конфиденциальности. В этой статье мы представляем анализ угроз безопасности и конфиденциальности данных граничных вычислений. В частности, мы сначала сделаем обзор граничных вычислений, обоснуем необходимость их создания, дадим определение, представим архитектуру и приведем несколько примеров применения граничных вычислений. Далее будет представлен подробный анализ требований к безопасности и конфиденциальности данных, описаны проблемы и механизмы их решения в граничных вычислениях.

Ключевые слова: граничные вычисления; граничный сервер; облачные вычисления; центр обработки данных; безопасность данных; конфиденциальность; аутентификация

Введение

Распространение IoT (англ. Internet of Things – концепция вычислительной сети физических предметов («вещей»), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой [1]) и 5G-сетей способствует развитию новых технологий и приложений, таких как интеллектуальные транспортные системы, «умный город», «умный дом», виртуальная реальность, геолокация и т. д. Однако, технология IoT становится неэффективной в связи с ростом количества устройств, оборудованных различными датчиками, таких как смартфоны, планшеты, бытовая смарт-техника и т. д., которые могут считывать большое количество данных из окружающей среды. Такая проблема заставляет разработчиков двигаться в эпоху IoE (англ. Internet of Everything – концепция интеллектуального подключение людей, процессов, данных и предметов («вещей»)) [1]. По сравнению с IoT, IoE больше ориентирована на интеллектуальной связи людей, процессов, данных и устройств, а не на связи между устройствами IoT[1]. С внедрением технологии IoE устройства граничных сетей превращаются из потребителей в производителей данных с большими возможностями по обработке информации, такими как сбор данных, распознавание образов и интеллектуальный анализ данных. В то же время, граничные устройства снабжены интернет – приложениями, обеспечивающими объединение вычислительных сервисов пользователей с облачными вычислительными центрами.

В эпоху IoE, примерно 50 % IoT-сетей имеют ограничения по пропускной способности, а 40 % граничных данных эффективнее анализировать, обрабатывать и сохранять в граничных сетях. В этом случае централизованная модель вычислений показывает врожденные проблемы, которые могут быть обобщены следующим образом:

1. линейный рост вычислительных возможностей облачных вычислений не может соответствовать росту обрабатываемых данных в граничных сетях;
2. пропускная способность сети и скорость передачи данных снижается в связи с тем, что увеличивается количество пользователей. Также значительно увеличивается расстояние передачи между пользователями и облачными центрами, что приводит к большой задержке и пустой трате вычислительных ресурсов;
3. частные данные пользователей в граничных устройствах с большой долей вероятности будут потеряны во время процесса аутсорсинга.

[1] Граничные вычисления: почему об этой технологии следует узнать немедленно? [Электронный ресурс]. URL: https://www.itweek.ru/iot/article/detail.php?ID=198653 (дата обращения 12.06.2017).

Таким образом, традиционные облачные сервисы не могут эффективно поддерживать приложения на основе IoE, поэтому и появляются граничные вычисления. В сочетании с существующими облачными сервисами с помощью граничных вычислений можно решать проблемы эффективной обработки больших данных.

По концепции граничных вычислений данные могут обрабатываться как вблизи к краю, так и на самой границе сети. Краевое устройство обращается к копии сетевого ядра, где связанные объекты совместно обрабатывают данные. Эти объекты могут соединяться в периферийные вычислительные платформы, которые синтезируются с сетью и пользуются хранилищем данных, вычислительными мощностями и другими основными функциями сети. Эти функции значительно разгружают вычислительную и коммуникационную нагрузку ядра сети. Обработка данных вблизи источников данных обеспечивает высокое QoS (англ. quality of service – качество обслуживания) для чувствительных к задержке услуг и обеспечивает высокую конфиденциальность пользователей и безопасность данных[2].

Из-за явных преимуществ парадигмы граничных вычислений, таких как неоднородность распределенной архитектуры, способность обработки больших массивов данных, возможность параллельных вычислений, осведомленность о местоположении и обеспечение поддержки мобильности, традиционные механизмы защиты данных и сохранения конфиденциальности «облачных» вычислений не подходят для защиты данных в граничных вычислениях. В частности, особое внимание уделяется вопросам безопасного хранения данных, безопасной обработки данных, аутентификации, разграничения доступа и защиты конфиденциальности. Безопасность данных и сохранение конфиденциальности в граничных вычислениях выдвигают новые требования:

- *Легкость и мелкомодульность*: новые требования к облегченным методам шифрования данных и мелкомодульным системам совместного использования данных, основанные на двусторонней авторизации в граничных вычислениях.
- *Распределенный контроль доступа*: вопросы контроля распространения данных, переданных от различных источников, и вопросы безопасного управления данными должны войти в состав распределенной вычислительной парадигмы.
- *Ограниченность ресурсов*: вопросы безопасности распределены между крупными граничными сервисами и граничными устройствами с ограниченными ресурсами.
- *Эффективное сохранение конфиденциальности*: новые требования к эффективным механизмам сохранения конфиденциальности для различных граничных сервисов и моделей граничных вычислений.

Проведя анализ литературы, сформировать основные положения этой статьи можно следующим образом:

- Представлен всесторонний обзор граничных вычислений, структуры и архитектуры. Также представлены перспективные применения граничных вычислений.
- Проанализированы безопасность данных и требования к конфиденциальности, основанные на пяти критических метриках: конфиденциальность, доступность,

[2] Граничные вычисления — это не только про IoT. [Электронный ресурс]. URL: http://www.iksmedia.ru/articles/5477030-Granichnye-vychisleniya-eto-ne-tolk.html#ixzz5IOwErpsY (дата обращения 12.06.2017).

целостность, аутентификация и управление доступом и сформулированы требования конфиденциальности.

Статья организована следующим образом. Раздел 1 определяет понятие граничных вычислений, обосновывает необходимость создания граничных вычислений, определение, архитектуру и применение граничных вычислений. Раздел 2 описывает угрозы информационной безопасности, представляет существующие механизмы защиты информации в концепции граничных вычислений.

1. Понятие граничных вычислений

В связи с увеличением количества приложений IoT, внедрением 5G сетевых архитектур, увеличиваются объемы данных, сгенерированных граничным оборудованием сети. Отдельные службы должны работать в режиме реального времени. Поэтому далеко не всегда становится применима традиционная модель «облачных» вычислений. Граничные вычисления представляют собой архитектуру, которая осуществляет разгрузку вычислений и перемещает службы «облачных» вычислений к краю сети. В этом разделе, мы дадим понятие граничных вычислений. Во-первых, обоснуем необходимость создания граничных вычислений, представим область применения граничных вычислений. Затем дадим определение и опишем архитектуру граничных вычислений.

1.1 Необходимость создания граничных вычислений

Недостатки облачных вычислений. Традиционная концепция «облачных» вычислений – централизованная модель обработки данных в центре удаленных данных. Такая модель порождает ряд недостатков, обусловленных увеличением объемов данных, собранных большим количеством оконечных устройств [7]. Во-первых, данные перцептивного уровня IoT хранятся в огромных массивах, и между этими данными необходимо постоянно выявлять взаимосвязи и противоречия [9]. Это означает, что вычислительные возможности с линейным ростом централизованных облачных вычислений не могут удовлетворить потребности обработки данных из нескольких источников данных. Во-вторых, пропускная способность сетей и скорость передачи данных стали слабым местом из-за увеличения количества пользователей. Например, междугородняя передача данных между пользователем и облачным центром обработки данных (ЦОД), будет приводить к большой задержке по времени и трате вычислительных ресурсов сети. В-третьих, большинство конечных пользователей на краю сети, обычно являются мобильными устройствами, не имеющими достаточных вычислительных ресурсов для хранения и обработки большого количества информации, и ограниченные во время работы от батареи. Таким образом, необходимо перенести некоторые вычислительные задачи граничных устройств без передачи информации на дальние расстояния к ЦОД облака. Наконец, безопасность данных и сохранение конфиденциальности являются сложными задачами в «облачных» вычислениях из-за передачи информации на дальние расстояния и аутсорсинга, поэтому обработка данных на границе облака может снизить риск утечки информации [7].

Чрезмерная нагрузка на глобальный ЦОД. Согласно оценке Cisco Global Cloud Index (GCI) и Internet Business Solutions Group (IBSG), данные, сгенерированные устройствами IoT, к 2021 году превысят 847 зеттабайт (ЗБайт). Однако IP-трафик глобального центра обработки данных сможет поддерживать объем в 19,5 ЗБайт [2], а устройств, соединенных с Интернетом,

79ITVN318
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

будет больше, чем 50 миллиардов[3]. Кроме того, понятие «чувствительная информация» начало постепенно внедряться в системы IoT, ускоряя развитие IoE [9].

От потребителя к полупрофессионалам. В традиционной системе «облачных» вычислений конечный пользователь обычно играет роль потребителя данных, просматривая изображения в веб-браузере, видеоролики или работая с документами в системе управления файлами. Сегодня роль конечного пользователя изменяется от потребителя данных к полупрофессионалу (производитель + потребитель данных). Это означает, что люди генерируют данные со своих устройств IoT. В этом случае обработка данных на границе сети может повысить оперативность работы приложений, требующих больших вычислительных ресурсов [10].

1.2 Определение и структура граничных вычислений

Pacific Northwest National Laboratory (PNNL) представляет граничные вычисления как подход, позволяющий продвинуть границу вычислительных приложений, данных и служб далеко от центральных узлов до логических экстремальных узлов сети, что позволяет анализировать и обрабатывать информацию вблизи источника данных. Edge Computing Consortium (ECC) определяет граничные вычисления как открытую платформу, которая развернута на границе сети, располагается рядом с источником данных и предоставляет интеллектуальные услуги, отвечающие требованиям работы в режиме реального времени, по оптимизации данных, обеспечивает безопасность и конфиденциальность инфраструктуры граничной сети [6]. Таким образом, можно сказать, что граничные вычисления – новая вычислительная модель, которая позволят хранить, обрабатывать данные на границе сети и предоставлять интеллектуальные услуги вблизи источника данных совместно с «облачными» вычислениями.

Рисунок 1 иллюстрирует общую архитектуру граничных вычислений, которая представлена четырьмя функциональными уровнями: базовая инфраструктура, граничные серверы, граничная сеть и граничные устройства. **Базовая инфраструктура** обеспечивает базовый доступ к сети (например, Интернет, мобильная сеть), координирует службы «облачных» вычислений и функции управления мобильных граничных устройств. **Граничные серверы**, которые принадлежат и разворачиваются провайдером, отвечают за обеспечение виртуализации и предоставление услуг управления. На границе сети могут разворачиваться граничные ЦОД, связанные друг с другом и «облака». **Граничная сеть** распознает подключения между граничными устройствами, граничными серверами и базовой инфраструктурой с беспроводной сетью, ЦОД и Интернетом. **Граничные устройства** включают все типы устройств, соединенных с граничной сетью (например, мобильные терминалы, устройства IoT), которые играют роль не только потребителей данных, но и производителей данных.

[3] Граничные вычисления могут подтолкнуть облако к краю. [Электронный ресурс]. URL: http://newseng.ru/post/boundary-calculations-can-push-the-cloud-to-theedge (дата обращения 12.06.2017).

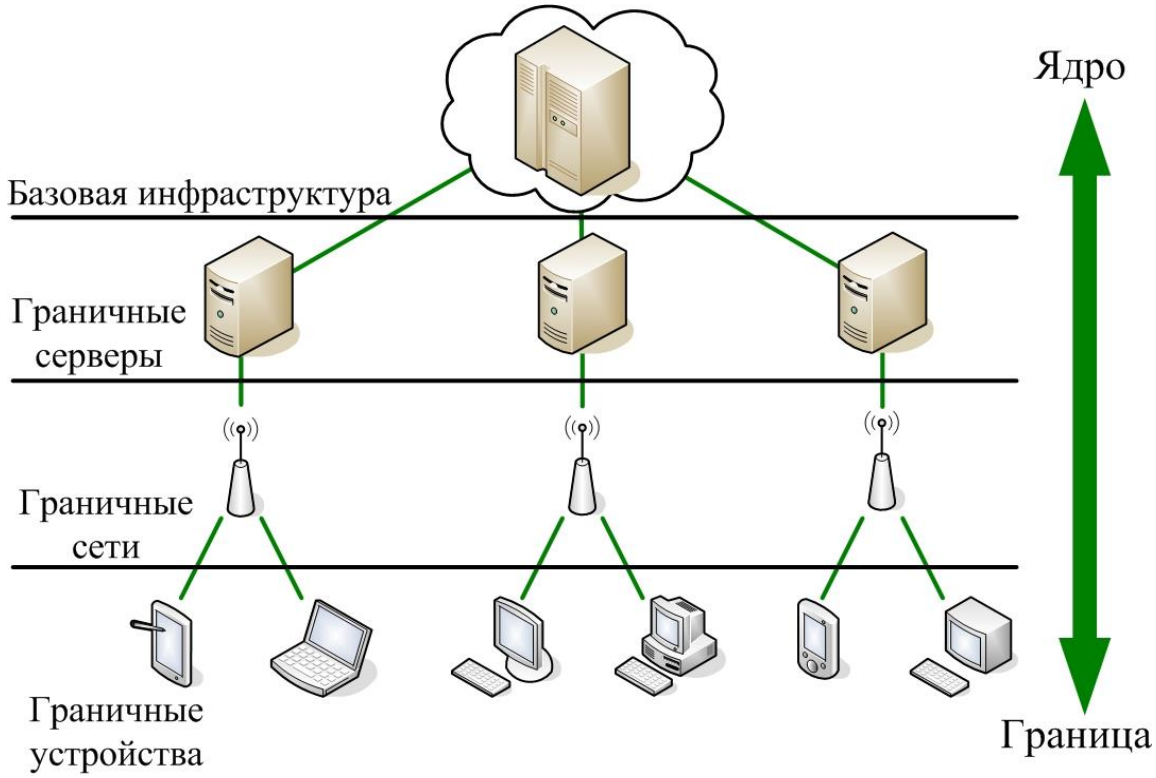

Рисунок 1. *Общая архитектура граничных вычислений (составлено автором)*

1.3 Применение граничных вычислений

По сравнению с традиционной централизованной «облачной» архитектурой исследователи нашли, что граничным вычислениям можно найти много перспективных вариантов применения в различных сферах.

Облачная разгрузка. С быстрым увеличением количества конечных устройств (например, смартфонов, планшетов, ноутбуков, интернет-телевизоров), все больше приложений требует минимальной временной задержки (например, самоходный автомобиль, виртуальная реальность, программы для удаленной работы). В традиционной системе «облачных» вычислений данные и запросы, произведенные конечными пользователями, обычно обрабатываются в облаке, что увеличивает задержку из-за передачи информации в ЦОД на большие расстояния. В граничных вычислениях у граничных объектов есть вычислительные ресурсы, которые могли обеспечить возможность снизить нагрузки на сеть, кэшируя данные и операции на границе облака. Такая идея подобна традиционной сети доставки содержимого (CDN) [8], но различие состоит в том, что в граничных вычислениях необходимо кэшировать и данные, и операции по обработке, в то время как в CDN кэшируются только данные. Развитие граничных вычислений повышает эффективность работы чувствительных ко времени приложений.

Видеоаналитика. Видеоаналитика, как развивающаяся технология, может быть определена как автономное распознавание событий, происходящих в месте, за которым наблюдает множество видеокамер. Одно из возможных применений видеоаналитики в граничных вычислениях – система видеонаблюдения. Системы видеонаблюдения еще не способны к автономному анализу сложных событий от большого количества камер. Традиционные «облачные» вычисления не могут проанализировать видеопотоки в режиме реального времени из-за высокой задержки передачи данных по сети. С развитием граничных

79ITVN318
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

вычислений функции видеоаналитики могут передаваться от облака локальным граничным серверам в указанной области. При таком подходе видеоаналитика может повысить оперативность обработки видео за счёт уменьшения времени на передачу данных и обработку результатов анализа [9].

Интеллектуальная сеть. Интеллектуальная сеть – разработка нового поколения для поставки электричества. Интеллектуальная сеть является электрической сетью, к которой добавлены информационно-коммуникационные технологии (ICT). Каждая инфраструктура интеллектуальной сети состоит из нескольких функциональных объектов, таких как уникальные операционные центры, коммуникационные шлюзы и пользователи, которые соединены с «облаками». Данные потребляемой электрической мощности, собранные умными счетчиками, используются для анализа в ЦОД. При применении системы граничных вычислений возможно сохранить и обработать данные потребляемой мощности умных счетчиков на граничных серверах, что позволит снизить загрузку «облачных» ЦОД.

Беспилотные автомобили. В транспортных сетях автомобили могут соединяться с дорожной инфраструктурой с помощью технологии (V2I автомобиль – дорожная инфраструктура) и с другими автомобильными терминалами (V2V автомобиль – автомобиль) посредствам модулей RSU. (Road Side Units – англ. модуль дорожной стороны). Модуль RSU должен решать в реальном времени множество сложных вычислительных задач и предоставлять результаты большому количеству автомобилей. Каждый «умный» автомобиль должен быть оборудован модулем вычисления, чтобы распознавать трафик интеллектуальных приложений. В такой архитектуре бортовая сеть может эффективно пользоваться ресурсами автомобилей, развернув граничные серверы на модулях RSU, тем самым продвинуть «облачный» сервис к краю сети – на модули RSU, интегрировав в них механизмы обмена данными и вычислений.

2. Угрозы информационной безопасности и механизмы защиты информации

Граничные вычисления могут освободить ЦОД от выполнения некоторых функций хранения и вычисления, передав эти функции границе сети, но при этом могут возникать проблемы, связанные с вопросами конфиденциальности и безопасности. Этот раздел посвящен угрозам информационной безопасности данных, требованиям конфиденциальности и механизмам обеспечения информационной безопасности в концепции граничных вычислений.

2.1 Требования конфиденциальности

Как в «облачных», так и в граничных вычислениях, конфиденциальные данные конечного пользователя должны быть частично или полностью обработаны ЦОД («облачным» или «граничным»). В связи с этим, данные пользователя могут быть утеряны, перехвачены злоумышленником, подвержены недопустимым операциям (репликация, публикация, распространение). Поэтому безопасность данных при аутсорсинге является все еще основной проблемой граничных вычислений [10].

- *Конфиденциальность*: конфиденциальность – фундаментальное требование, которое гарантирует, что только владелец данных может получить доступ к частной информации, находящейся на граничных серверах. Это предотвращает несанкционированный доступ третьих лиц к данным, когда персональные данные пользователей передаются и получаются на границе облака или базовой сетевой инфраструктуре, или хранятся и обрабатываются ЦОД («облачным» или «граничным»).

- *Целостность*: целостность гарантирует корректную доставку данных авторизованному пользователю (пользователям) без любой модификации информации. Отсутствие мер по контролю целостности может значительно снизить конфиденциальность данных пользователей.
- *Доступность*: для граничных вычислений доступность гарантирует, что любой пользователь может получить доступ к граничным и «облачным» сервисам согласно своим требованиям и правам доступа. Это также означает, что данные пользователя, которые хранились на граничном или «облачном» ЦОД в зашифрованном виде, могут быть обработаны в соответствии с требованиями пользователя.
- *Аутентификация и управление доступом*: аутентификация гарантирует, что пользователь действительно является тем, за кого он себя выдает, и какие имеет права доступа. Управление доступом определяет, кто может получить доступ к ресурсам (аутентификация) и какие действия им могут быть выполнены, такие как чтение (конфиденциальность) и запись (целостность).
- *Требование конфиденциальности*: механизмы безопасности должны гарантировать, что при аутсорсинге вся информация о пользователях, такая как персональные, идентификационные данные, информация о местоположении, должны быть скрыты как от других пользователей, так и от злоумышленников.

2.2 Проблемы обеспечения информационной безопасности в граничных сетях

Граничные вычисления используют много новых технологий, таких как разгрузка, виртуализация и аутсорсинг, чтобы перенести вычисления ближе к источникам данных [3]. В этом случае безопасность данных и сохранение конфиденциальности становятся главными требованиями по защите конечных пользователей. Кроме того, безопасность и конфиденциальность должны обеспечиваться на каждом уровне при разработке граничных вычислительных систем. В этом подразделе мы рассмотрим потенциальные проблемы конфиденциальности на основе четырехуровневой архитектуры граничных вычислений.

Безопасность базовой инфраструктуры. Стоит отметить, что, все граничные системы могут поддерживаться несколькими базовыми инфраструктурами, такими как централизованный «облачный» сервис и системы управления. Этими базовыми инфраструктурами управляют сторонние провайдеры, например операторы мобильных сетей. В связи с этим возникают проблемы, такие как утечка конфиденциальности, вмешательство в данные, атаки типа «отказ в обслуживании». В связи с этим, базовой инфраструктуре можно или доверять не полностью, или абсолютно не доверять, поскольку к персональным данным пользователя и к его личной информации могли получить доступ другие пользователи. Кроме того, граничные вычисления позволяют обмениваться информацией непосредственно между граничными устройствами и граничными ЦОД в обход «облачных» ЦОД. Для базовой инфраструктуры злоумышленник может реализовать обмен ложной информацией, если получит контроль над службами граничных ЦОД. Кроме того, информационным потоком может управлять и внутренний злоумышленник, у которого есть достаточные права доступа для подмены информации и запуска вредоносных служб. Из-за децентрализованной и распределенной природы граничных вычислений, этот класс угроз безопасности является одним из самых серьезных.

Безопасность граничных серверов. Граничные серверы (или граничные ЦОД) отвечают за службы виртуализации и некоторые службы управления сетью. Географически

граничные ЦОД разворачиваются в разных местах, реализуя принцип «мультиоблачности». Зная местоположение граничного ЦОД, и внутренние, и внешние злоумышленники могут получить доступ к нему и похитить или изменить информацию пользователей. Если злоумышленник получил достаточно полномочий по управлению граничным ЦОД, то он может выступить в роли администратора, что позволит ему управлять службами. Как следствие, нарушитель может выполнить несколько типов атак, таких как атаки «противник посередине», атаки «отказ в обслуживании» и т. д. Кроме того, есть ситуации, когда злоумышленник может управлять всем граничным сервером и может создать ложную инфраструктуру, тогда он может полностью управлять всеми службами и направить информационный поток в свой ЦОД. Другая проблема безопасности – физическое отключение граничного ЦОД. Главная причина для этого типа атаки заключается в том, что физическая защита граничного сервера слабая или отсутствует совсем.

Безопасность граничных сетей. Граничные вычисления позволяют соединить устройства IoT, такие как мобильная сеть, беспроводная сеть и Интернет, и датчики, встроенные во множество различных устройств. Такой принцип коммуникации порождает много проблем сетевой безопасности. Используя граничные серверы, традиционные сетевые атаки, такие как «отказ в обслуживании» (DOS) и «атаки распределенного отказа в обслуживании» (DDOS), могут характеризоваться ограниченной эффективностью. Такие атаки навредят только ближайшей граничной сети и не вызовут серьезных последствий как те же DOS или DDoS-атаки, произошедшие в базовой инфраструктуре. Только атака типа «противник посередине» может существенно повлиять на все функциональные элементы граничной сети, считывая информацию о сетевом потоке и данные пользователей. Другая проблема безопасности граничной сети – шлюз злоумышленника. В этом типе атаки вся инфраструктура граничной сети вводится в сетевой трафик, становится известна нарушителю и сводится, в конечном счете, к атаке «противник посередине».

Безопасность граничных устройств. В граничных вычислениях граничные устройства играют роль активных участников распределения вычислительной мощности на различных уровнях, таким образом, чтобы даже скомпрометированные граничные устройства не могли бы привести к серьезным последствиям для всей граничной системы. Например, любые устройства, которыми управляет злоумышленник, могут попытаться изменить службы сети, внедряя ложную информации или развернуть систему с вредоносным программным обеспечением. Кроме того, устройства злоумышленника могут управлять службами по определенным сценариям, согласно которым злоумышленники получили бы полномочия по управлению другими устройствами сети. Например, граничное устройство, находящееся в доверенном домене, может выступать в роли ЦОД других устройств.

2.3 Реализация механизмов защиты информации

Чтобы создать безопасную жизнеспособную систему граничных вычислений, крайне важно реализовать различные типы механизмов безопасности и конфиденциальности, предотвратить любую возможность проникновения злоумышленников [4]. В этом разделе рассматриваются существующие механизмы обеспечения безопасности и конфиденциальности, которые мы предлагаем использовать в граничных вычислительных системах.

На рисунке 2 схематично показаны методы обеспечения информационной безопасности, которые мы предлагаем использовать в граничных вычислениях.

79ITVN318
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Рисунок 2. *Методы обеспечения информационной безопасности граничных вычислений (составлено автором)*

Конфиденциальность персональных данных. В граничных вычислениях персональные данные пользователя сохранены на граничном сервере. Пользователь арендует у провайдера дисковое пространство и получает от него набор необходимых функций по обработке данных. Физического контроля за своими данными пользователь обеспечить не может. Кроме этого, персональные данные, обрабатываемые на стороне сервера, чрезвычайно уязвимы. Они могут быть потеряны, переданы не по назначению, с информацией могут произойти недопустимые операции (например, копирование, удаление и распространение). Чтобы предотвратить эти угрозы, должна быть предложена подходящая модель обеспечения конфиденциальности данных. Это означает, что пользовательские данные на граничных устройствах должны быть зашифрованы, прежде чем граничный сервер их обработал. В настоящее время конфиденциальность данных и безопасные схемы совместного использования данных обычно реализуются методами шифрования. Чаще всего производитель данных шифрует произведенные данные и отправляет их в ЦОД. Традиционные способы шифрования используют симметричные алгоритмы шифрования (например, AES, DES и ADES) и асимметричные алгоритмы шифрования (например, RSA, Диффи-Хеллмана и ECC), но последующая обработка текста, зашифрованного перечисленными способами крайне трудна. В последние годы объединяются такие методы, как шифрование по идентификатору, основанные на атрибуте шифрования, перешифрование по доверенности и гомоморфное шифрование, чтобы объединить несколько методов шифрования данных для создания безопасной системы хранения данных.

Целостность данных. Целостность данных – важная проблема безопасности граничных вычислений. Данные пользователей хранятся на арендованных серверах, поэтому целостность данных может быть под угрозой. Владельцы данных должны проверять целостность и доступность обрабатываемых данных, чтобы удостовериться, что нет никаких скрытых модификаций данных. В граничных вычислениях исследование целостности данных должно сосредоточено на следующих четырех функциональных аспектах: пакетный аудит, динамический контроль, сохранение конфиденциальности, и низкая сложность.

Безопасный поиск данных. Безопасный поиск данных – другая важнейшая проблема, которая должна быть решена в граничных вычислениях. Данные конечных пользователей обычно обрабатываются на стороне граничных серверов в форме зашифрованного текста. В этом случае безопасный поиск данных – самая сложная задача, поскольку пользователь должен осуществить поиск по ключевым словам в зашифрованных файлах. Усилиями разработчиков созданы несколько методик для поиска в зашифрованных файлах без их расшифрования.

79ITVN318
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Аутентификация. Граничные вычисления – распределенная интерактивная вычислительная система с доверенными доменами, где сосуществует множество функциональных агентов, служб и инфраструктур. Без механизмов аутентификации для внешних злоумышленников довольно просто получить доступ к ресурсам инфраструктуры. Внутренние злоумышленники могут стереть следы доступа к чужим данным благодаря своим законным правам доступа. В этом контексте необходимо исследовать аутентификацию в граничных вычислениях, чтобы защитить пользователей от существующей опасности и решить проблемы конфиденциальности, минимизировав внутренние и внешние угрозы. Кроме того, граничные вычисления не только должны требовать проверки идентификационных данных для каждого объекта в одном доверенном домене, но также нужно, чтобы в объектах была взаимная аутентификация друг друга, если они находятся в разных доменах. В настоящее время надлежащие методы аутентификации включают внутридоменную аутентификацию, междоменную аутентификацию и аутентификацию при передаче.

Разграничение доступа. Из-за аутсорсинга граничных вычислений, при отсутствии эффективных механизмов аутентификации, злоумышленники без санкционированных идентификационных данных могут пользоваться ресурсами системы в граничной или базовой инфраструктуре. Это представляет большую проблему безопасности, поскольку нарушитель может изменить ресурс виртуализации граничного сервера, чтобы получить доступ к данным граничных устройств. Кроме того, в распределенных системах граничных вычислений есть несколько доверенных доменов с различными инфраструктурами, существующие в одной граничной системе. Таким образом, важно разработать мелкомодульную систему управления доступом в каждом доверенном домене. Однако большинство традиционных механизмов управления доступом обычно обращается к одному доверенному домену, и не поддерживают несколько доверенных доменов. Существуют базовые криптографические решения, которые основаны на шифровании атрибутов, методы на основе шифрования роли, которые могут использоваться, чтобы достигнуть гибкого и мелкомодульного управления доступом. Кроме того, существует механизм управления доступом на основе TPM, который мог бы подойти для систем граничных вычислительных.

Сохранение конфиденциальности. Конфиденциальность – одна из основных проблем в любых вычислительных системах, поскольку данные конечных пользователей и персональные данные считываются с граничных устройств на удаленные серверы. В граничных вычислениях проблема конфиденциальности более значима. Злоумышленниками в таких системах выступают, как правило, авторизованные пользователи, цель которых состоит в том, чтобы получить доступ к наиболее уязвимой информации, которая может использоваться различными способами [5]. В этой ситуации невозможно знать, защищен ли поставщик услуг в такой открытой системе с различными доверенными доменами. Например, в интеллектуальной сети, частная информация домашнего хозяйства может быть раскрыта от чтения данных умных счетчиков или других устройств IoT. В частности, утечка частной информации, такой как идентификационные данные, местоположение может привести к очень серьезным последствиям. Во-первых, граничные серверы и датчики устройств могут собирать уязвимые данные от конечных устройств. Такие методы как агрегация данных на основе гомоморфного шифрования могут обеспечивать сохранение конфиденциальности данных без дешифрования. Вероятностное шифрование с открытым ключом и псевдослучайная перестановка могут использоваться, чтобы разработать несложные алгоритмы, которые сохраняют конфиденциальность данных. Во-вторых, в динамической и распределенной вычислительной среде, пользователям необходимо защитить их информацию об идентификационных данных во время аутентификации. Наконец, информация о местоположении пользователей довольно предсказуема, поскольку у них обычно существует относительно фиксированная точка стояния, что означает, что пользователи будут, вероятно, неоднократно использовать одни и те

79ITVN318
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

же граничные серверы. В этом случае мы должны уделить больше внимания защите нашей конфиденциальности.

Заключение

В этой статье мы проанализировали и обобщили проблемы безопасности и защиты данных, а также предлагаем контрмеры в концепции граничных вычислений. Во-первых, обоснована необходимость развития граничных вычислений, в том числе описаны недостатки облачных вычислений. Затем представлены архитектура и несколько важных применений граничных вычислений. Во-вторых, проанализированы потенциальные угрозы информационной безопасности и сохранения конфиденциальности, а также предложены возможные механизмы обеспечения информационной безопасности.

ЛИТЕРАТУРА

1. Kevin Ashton. That ‘Internet of Things’ Thing. In the real world, things matter more than ideas. (англ.). RFID Journal (22 июля 2009). [Электронный ресурс]. URL: http://www.rfidjournal.com/articles/view?4986 (дата обращения 12.06.2017).
2. D. Evans, “The internet of everything: How more relevant and valuable connections will change the world”, Cisco IBSG, с. 1-9, Дек. 2012.
3. M. Aazam and E.N. Huh, “Fog computing and smart gateway based communication for cloud of things”, in Proceedings of the second International Conference on Future Internet of Things and Cloud. (FiCloud), Barcelona, Spain, Авг. 2014, с. 464-470.
4. P. Neirotti, A. De Marco, A.C. Cagliano, G. Mangano and F. Scorrano, “Current trends in smart city initiatives: Some stylised facts”, Cities, вып. 38, №. 5, с. 25-36, Июнь 2014.
5. A. Taherkordi, F. Eliassen and G. Horn, “From iot big data to iot big services”, in Proceedings of the 32th SIGAPP Symposium on Applied Computing. (SAC), Marrakech, Morocco, Апр. 2017, с. 485-491.
6. Y.C. Hu, M. Patel, D. Sabella, N. Sprecher and V. Young, “Mobile edge computing at a key technology towards 5g”, ETSI White Paper, вып. 11, № 11, с. 1-16, Сен. 2015.
7. R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg and I. Brandic, “Cloud computing and emerging it platforms: Vision, hype and reality for delivering computing as the 5th utility”, Future Generation computer systems, вып. 25, № 6, с. 599-616, Июнь 2009.
8. V. Turner, J.F. Gantz, D. Reinsel and S. Minton, “The digital universe of opportunities: Rich data and the increasing value of the internet of things”, IDC Analyze the Future, Апр. 2014.
9. M.B. Mollah, M.A.K. Azad and A. Vasilakos, “Security and privacy challenges in mobile cloud computing: Survey and way ahead”, Journal of Network and Computer Applications, вып. 84, с. 38-54, Апр. 2017.
10. D.E. Culler, “The once and future internet of everything”, GetMobile: Mobile Computing and Communications, вып. 20, № 3, с. 5-11, Июль 2016.

Ryabokon' Vladimir Vladimirovich
The academy of federal security guard service of the Russian Federation, Orel, Russia
E-mail: mimicria@mail.ru

Kuzkin Alexander Alexandrovich
The academy of federal security guard service of the Russian Federation, Orel, Russia
E-mail: kuzmich313@mail.ru

Tutov Stanislav Yur'evich
The academy of federal security guard service of the Russian Federation, Orel, Russia
E-mail: tutoff@yandex.ru

Mahov Alexandr Sergeevich
The academy of federal security guard service of the Russian Federation, Orel, Russia
E-mail: tutoff@yandex.ru

Review of information security threats in the concept of edge computing

Abstract. The article presents an overview of the technologies of edge computing. With the wide spread of information networks and the increase in data sets generated by edge devices, the traditional centralized model of cloud computing becomes inefficient due to the limitation of network throughput and upturn in the amount of computing operations. That is why in recent years the technology of edge computing has become promising. The main services of the given technology are presentation of a content, real-time computing and parallel data processing. However, there are new problems in that kind of networks, such as data security and preservation of privacy. Despite the importance of edge computing, there have been insufficient numbers of studies in the field of data security and preservation of privacy. In this article, we present an analysis of the security and confidentiality threats of the given edge computing. In particular, we will start with the review of the edge computing, let us justify the necessity of their creation, will give a definition, represent the architecture and provide some examples of the edge computing. Further, a detailed analysis of the requirements for data security and preservation of privacy will be presented problems and mechanisms for their solution in edge computing will be described.

Keywords: edge computing; edge server; cloud computing; data center; data security; privacy; authentication