АНАЛИЗ МЕТОДОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ В ИНТЕРНЕТЕ ВЕЩЕЙ

Блинов Роман Викторович

студент, Сибирский государственный индустриальный университет, РФ, г. Новокузнецк

Бычков Кирилл Вячеславович

студент, Сибирский государственный индустриальный университет, РФ, г. Новокузнецк

Кирчева Алина Сергеевна

студент, Сибирский государственный индустриальный университет, РФ, г. Новокузнецк

Мамедов Илькин Вахид оглы

студент, Сибирский государственный индустриальный университет, РФ, г. Новокузнецк

Современный мир становится все более связанным и информационно насыщенным, и интернет вещей (Internet of Things, IoT) играет ключевую роль в этом процессе. IoT представляет собой сеть физических объектов, включая устройства, транспортные средства, домашние приборы и другие предметы, которые обмениваются данными и взаимодействуют между собой. Значительное увеличение распространения устройств Интернета вещей (IoT) было вызвано в основном снижением стоимости аппаратного обеспечения. В 2021 году общий оборот был оценен в 124 миллиарда долларов, а количество устройств IoT достигло порога в 35 миллиардов [1]. Однако, с ростом количества подключенных устройств и объема обрабатываемых данных, вопросы безопасности и конфиденциальности данных в IoT становятся все более актуальными и критически важными для защиты персональных данных и предотвращения кибератак, так как устройства IoT используются в широком диапазоне приложений, включая промышленность, здравоохранение, транспорт и многое другое.

Концепция "Интернета вещей" может быть определена как стандарт, который относится к большой сети, соединяющей различные датчики, исполнительные механизмы и микроконтроллеры, встроенные в различные объекты. Большое количество взаимосвязанных устройств, таких как смартфоны, промышленное оборудование, компьютеры, автомобили, медицинские инструменты, системы орошения, телевизоры или холодильники, может быть частью Интернета вещей. Интернет вещей включает в себя очень большое количество гибридных терминалов. Поскольку большинство этих устройств могут быть подключены к Интернету, они обычно поддерживают общие веб-технологии, включая HTTP, JSON, XML и т.д. Одним из преимуществ этой технологии является то, что она хорошо поддерживается и может быть адаптирована к различным существующим инфраструктурам. Кроме того, некоторые новые протоколы специально рассматриваются для Интернета вещей, например, CoAP и MQTT являются альтернативами HTTP, а 6LoWPAN также является альтернативой IPv4/IPv6.

С логической точки зрения, система IoT может быть описана как набор умных устройств, взаимодействующих на основе сотрудничества для достижения общей цели. На технологическом уровне, развертывание IoT может использовать различные архитектуры обработки и коммуникации, технологии и методологии проектирования в зависимости от целей системы. Например, одна и та же система IoT может использовать возможности беспроводной сети датчиков (WSN), которая собирает информацию об окружающей среде в определенной области, и набор смартфонов, на которых работают приложения мониторинга.

Блинов Р.В., Бычков К.В., Кирчева А.С. [и др.] АНАЛИЗ МЕТОДОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ В ИНТЕРНЕТЕ ВЕЩЕЙ // Молодежный научный форум: электр. сб. ст. по мат. CCXII междунар. студ. науч.-практ. конф. № 21(212).
URL: https://nauchforum.ru/archive/MNF_interdisciplinarity/21(212).pdf *(дата обращения: 09.09.2025)*

В середине может быть применен стандартизированный или собственный промежуточный слой, который облегчит доступ к виртуальным ресурсам и сервисам. Промежуточный слой, в свою очередь, может быть реализован с использованием облачных технологий, централизованных оверлеев или систем peer-to-peer [2].

Сложность управления безопасностью в сетях IoT не ограничивается ее реализацией, а распространяется на необходимость найти правильный баланс между уровнем гарантированной защиты и достигнутой производительностью. В настоящее время существуют несколько методов, которые обеспечивают одно или несколько требований безопасности, но многие из них не применимы во всех сценариях IoT. Например, не все устройства IoT способны выполнять некоторые типы криптографических вычислений, или они не могут завершить их в приемлемые сроки. Кроме того, устройства с ограниченными возможностями энергопотребления в системах IoT часто находятся в критических или недоступных местах, что затрудняет или делает невозможным замену их батарей. Однако цель безопасности в системах IoT заключается не только в предотвращении нарушения конфиденциальной информации или предотвращении доступа злоумышленников: злоумышленник может быть просто заинтересован в получении контроля над устройством для совершения совершенно разных целей. Наконец, доверие является фундаментальным вопросом, поскольку среда Интернета вещей характеризуется различными устройствами, которые должны обрабатывать и управлять данными в соответствии с потребностями и правами пользователей [2]. Таким образом, важность обеспечения безопасности в системах IoT, от физического до прикладного уровня, становится очевидной.

Существует множество различных видов атак на интернет вещи (IoT). Некоторые из наиболее распространенных типов атак включают:

Отказ в обслуживании (DoS) – это атака на безопасность, которая направлена на предотвращение легитимного доступа пользователя и сущности к ресурсам сети. Она считается наиболее популярной и доминирующей атакой. Обычно злоумышленники могут использовать атаку перегрузки, чтобы истощить ресурсы системы, включая память, ЦП и пропускную способность. Атака либо предотвращает предоставление услуг системой, либо делает ее неэффективной. В ней пираты могут использовать множество методов, таких как отправка нежелательных пакетов или перегрузка сети множеством сообщений. Таким образом, легитимным пользователям предотвращается использование услуг [3].

Атака повтора (Replay attack) является одной из старых атак на коммуникационные сети, особенно на протоколы аутентификации и обмена ключами. Она позволяет злоумышленнику захватить и сохранить фрагмент или целую захваченную сессию в легитимном трафике. После того, как злоумышленник завоевал доверие в общественной сети, он либо отправляет захваченное сообщение участнику исходной сессии, либо другому назначению. Поэтому в сетях Интернета вещей атака повтора рассматривается как уязвимость безопасности, при которой определенные данные хранятся без какого-либо разрешения до их отправки получателю. Цель этой атаки заключается в том, чтобы запутать человека в несанкционированной операции. Например, в системе умного дома используется датчик температуры для обнаружения температуры, после чего измеренные значения отправляются контроллеру системы. Основываясь на этих значениях, система может запустить или остановить кондиционер, чтобы адаптировать температуру воздуха так, как это требуется персоналу. Однако, если злоумышленник взломал датчик температуры, он может сохранить значения за день и отправить их ночью. В результате кондиционер не будет функционировать нормально.

Чтобы бороться с атакой повтора, текущие решения используют три основных механизма, включая отметку времени, одноразовый номер и ответ-вызов. Первый механизм помогает обнаружить атаку повтора, проверяя свежесть полученного сообщения. Тем не менее, сложно гарантировать синхронизацию времени между объектами IoT. Второй механизм - одноразовый номер, представляет собой серию случайных цифр. Однако проблема этого механизма заключается в том, что узел не имеет достаточной памяти для хранения списка полученных номеров. Последний механизм - ответ-вызов, имеет целью проверить, что другая сторона может решать некоторые проблемы. Но для этой техники необходимо, чтобы два устройства имели заранее общий ключ.

Из-за важности пароля в процессе аутентификации и его широкого использования во многих протоколах аутентификации, злоумышленники придумали различные атаки, чтобы получить необходимый пароль. Самая часто используемая атака — это угадывание пароля. В частности, эта атака может быть выполнена как в онлайн-режиме, так и в оффлайн-режиме.

В контексте безопасности сети, атака по перехвату идентификатора представляет собой ситуацию, когда ненадлежащий субъект создает искаженный параметр. Цель этой атаки - заставить серверы поверить, что злоумышленник является авторизованным лицом.

В области кибербезопасности внутренняя атака (insider attack) происходит, когда уполномоченный субъект с авторизованным доступом пытается нанести вред системе. Действие субъекта может быть как преднамеренным, так и случайным. В обоих случаях система считается уязвимой.

Все эти типы атак могут привести к серьезным последствиям, включая утечку конфиденциальных данных, нарушение работы устройств и систем, а также угрозы безопасности пользователей. Поэтому важно принимать меры для защиты устройств IoT от этих атак.

Некоторые методы обеспечения безопасности и конфиденциальности данных в IoT включают в себя:

Аутентификация и авторизация: это процесс подтверждения легитимности устройств и пользователей, имеющих доступ к данным. Используют механизмы аутентификации, такие как пароли, цифровая подпись и биометрические данные, чтобы проверять подлинность устройств и пользователей.

Шифрование: это процесс преобразования данных в неразборчивый вид, который может быть прочитан только теми, у кого есть ключ для дешифровки. Для шифрования могут использоваться различные алгоритмы, такие как AES, RSA или ECC.

Контроль доступа. Применяют ACL (Access Control List) и другие механизмы контроля доступа для регулирования того, какие устройства и пользователи могут получить доступ к различным ресурсам и данным.

Защита на уровне устройства. Использование firewall, защиты от DoS-атак и других методов защиты непосредственно на устройствах Интернета вещей.

Обнаружение вторжений. Системы обнаружения вторжений, которые могут обнаруживать и блокировать попытки несанкционированного доступа к ресурсам Интернета вещей.

Обновление ПО. Регулярное обновление ПО устройств Интернета вещей, чтобы исправлять уязвимости безопасности.

Помимо вышеуказанных требований безопасности, также необходимо удовлетворять двум важным свойствам безопасности:

Прямая секретность: если узел сбора данных IoT покидает сеть, то любые сообщения, передаваемые после его выхода, должны быть запрещены.

Обратная секретность: если в сеть добавляется новый узел сбора данных IoT, он не должен иметь доступ к любым ранее переданным сообщениям [4].

В целом, безопасность и конфиденциальность данных в IoT зависят от правильной реализации этих методов и от выбора правильных технологий и протоколов для каждого конкретного случая использования.

Список литературы:

1. Rizzardi A., Sicari S., Coen-Porisini A. Analysis on functionalities and security features of Internet of Things related protocols //Wireless Networks. – 2022. – Т. 28. – №. 7. – С. 2857-2887.

2. Sicari S. et al. Security, privacy and trust in Internet of Things: The road ahead //Computer networks. – 2015. – Т. 76. – С. 146-164.

3. Azrour M. et al. Internet of things security: challenges and key issues //Security and Communication Networks. – 2021. – Т. 2021. – С. 1-11.

4. Das A. K., Zeadally S., He D. Taxonomy and analysis of security protocols for Internet of Things //Future Generation Computer Systems. – 2018. – Т. 89. – С. 110-125.