УДК 336.71

Ахметов Марат Маратович
студент,
Лениногорский филиал
Казанский национальный исследовательский технический
университет им. А.Н. Туполева-КАИ
Россия, г. Лениногорск
e-mail: marat2009@mail.ru

Научный руководитель: Лямов Юрий Олегович
старший преподаватель
Лениногорский филиал
Казанский национальный исследовательский технический
университет им. А.Н. Туполева-КАИ
Россия, г. Лениногорск

БЕЗОПАСНОСТЬ В СФЕРЕ ИНТЕРНЕТА ВЕЩЕЙ

Аннотация: *В статье рассматривается понятие Интернета вещей и анализируются проблемы, связанные с безопасностью Интернета вещей. В заключении автором делается вывод о критериях, которыми необходимо руководствоваться при разработке безопасных решений.*

Ключевые слова: интернет, безопасность, конфиденциальность, алгоритмы.

Akhmetov Marat Maratovich
student,
Leninogorsk branch
Kazan National Research Technical University named after. A.N. Tupolev-KAI
Russia, Leninogorsk
e-mail: marat2009@mail.ru

Scientific supervisor: Lyamov Yuri Olegovich
Senior Lecturer
Leninogorsk branch
Kazan National Research Technical University named after. A.N. Tupolev-KAI
Russia, Leninogorsk

SECURITY IN THE INTERNET OF THINGS

Abstract: *The article discusses the concept of the Internet of Things and analyzes the problems associated with the security of the Internet of Things. In conclusion, the author draws a conclusion about the criteria that must be followed when developing safe solutions.*

Key words: Internet, security, privacy, algorithms.

Интернет вещей (Internet of Things, IoT) представляет собой концептуальную парадигму, объединяющую миллиарды устройств с поддержкой Интернета для обмена данными между собой и окружающей средой. Это позволяет им взаимодействовать интеллектуально и подключаться к цифровым системам. IoT имеет широкий спектр применений в таких областях, как здравоохранение, транспорт, безопасность, домашняя автоматизация и т.д.

Интернет вещей был предложен в 1999 году исследователем Кевином Эштоном с целью поддержки технологии RFID, но с течением времени значительно расширил свои возможности и стал популярным. IoT предоставляет доступ к данным в реальном времени в любом месте и позволяет людям и предприятиям принимать обоснованные бизнес-решения.

Прогнозируется, что к 2027 году число подключенных IoT-устройств достигнет 41 миллиарда. Рынок IoT продолжает расти, и в 2021 году его объем составил 157,9 миллиарда долларов, что является увеличением на 22% по сравнению с предыдущим годом.

Важнейшими компонентами Интернета вещей, составляющими основную долю, являются датчики и исполнительные механизмы. Датчики - это устройства, которые физически воспринимают определенные явления и передают полученные значения другим устройствам (то есть собирают данные и сообщают о своем внутреннем состоянии). Примеры таких датчиков в Интернете вещей включают GPS и ЭКГ.

Для реализации эффективных решений в области Интернета вещей используются компактные встраиваемые системы, что позволяет достичь требуемой экономической эффективности и расширить сферу их применения. Эти сенсорные узлы часто используют 8-разрядные микроконтроллеры с небольшой памятью, что позволяет им снизить энергопотребление и

обеспечивает работу от батарей в течение нескольких лет. В сочетании с различными сетевыми протоколами, адаптированными к существующей инфраструктуре или условиям эксплуатации, это в значительной степени способствует распространению решений Интернета вещей в разных областях.

Исполнительные механизмы также являются физическими устройствами, которые могут изменять физическую среду (то есть выполнять различные действия) в ответ на команды или рекомендации, например термостаты переменного тока или клапаны. Эти устройства должны быть подключены к Интернету и способны обмениваться данными для отправки или получения информации, чтобы быть отнесенными к устройствам Интернета вещей.

Объединение IoT, передовой аналитики данных и искусственного интеллекта открывает возможности для нового поколения приложений, которые способствуют принятию решений в реальном времени. Эти приложения могут повысить качество обслуживания пользователей и предсказывать потребность в техническом обслуживании. Поэтому аналитика данных стала ключевым компонентом для развертывания IoT и будет продолжать расти в популярности и значимости для предприятий с увеличением объема собираемых данных, необходимых для принятия интеллектуальных решений.

Например, в промышленном производстве предиктивное обслуживание позволяет сделать прогнозы о необходимости технического обслуживания с помощью измерения параметров, таких как уровень вибрации и нагрева, что помогает избегать простоев в производстве. Данные IoT также могут предоставить ценные сведения о поведении клиентов (например, предпочтения в вождении и покупках), которые могут быть использованы для улучшения качества обслуживания. Модели машинного обучения и методы искусственного интеллекта могут извлекать уроки из этих наблюдений и рекомендовать действия, которые способствуют принятию разумных решений.

Интернет вещей обладает огромным спектром применения и множеством преимуществ, однако есть и недостатки. Один из них – недостаточная защищенность устройств IoT. Для создания и внедрения полных решений по

обеспечению безопасности в сфере IoT, необходимо идентифицировать угрозы и проблемы, связанные с сетями IoT, устройствами IoT, приложениями IoT. Он включает в себя такие проблемы, как клонирование устройств IoT ненадежным производителем, замена ценных вещей опасными вещами низкого качества, атака «человек посередине» во время установки и отсутствие надлежащих механизмов аутентификации и авторизации. Другие угрозы безопасности включают замену вредоносного кода прошивки злоумышленником, утечку конфиденциальных данных, атаку типа «отказ в обслуживании», маршрутизацию атаки, подслушивание в плохо настроенных сетях IoT, а также получение параметров безопасности из физически незащищенных устройств IoT. В будущих исследованиях по безопасности IoT следует заняться следующими ключевыми проблемами:

Важность идентификации устройств: Надлежащая идентификация IoT-устройств играет ключевую роль. DNS-серверы присваивают имена подключенным устройствам IoT. Однако DNS тоже восприимчив к различным атакам, включая "человека посередине" и атаки на позиционирование DNS-кэша. Злоумышленники могут повторно использовать украденные или взломанные идентификаторы устройств для проведения различных вредоносных действий в сети.

Идентификация и разрешение доступа: Сети Интернета вещей состоят из многочисленных устройств, которые должны быть гибко подключены к сети в любое время. Поскольку эти устройства работают с конфиденциальными данными, они должны пройти процесс идентификации для получения и передачи данных через шлюз. Использование заводских установленных паролей по умолчанию или слабых паролей увеличивает уязвимость системы безопасности. Разрешение доступа не менее важно, чем идентификация. Устройства Интернета вещей должны иметь возможность читать и записывать данные только в определенную область базы данных, а не в другие. Если устройство подвергается компрометации, злоумышленники могут получить доступ на чтение или запись конфиденциальной информации.

Внедрение алгоритмов безопасности: Применение облегченных алгоритмов шифрования является важным аспектом обеспечения безопасности IoT-устройств. Из-за ограниченных возможностей этих устройств, использование сложных криптографических алгоритмов невозможно. Это может привести к возможности атак через побочные каналы и обратный инжиниринг данных. Однако, разработка и внедрение облегченных алгоритмов шифрования может снизить вероятность подслушивания и обеспечить защиту данных в сетях IoT.

Безопасность передачи данных: Обеспечение безопасной передачи конфиденциальной информации IoT в реальном времени через Интернет является важным аспектом. Как было упомянуто ранее, многие устройства IoT не шифруют данные при передаче через Интернет. Введение защищенной частной сети может уменьшить уязвимость, но в случаях, когда данные IoT нужно обменивать с разными устройствами, такое решение может быть непрактичным. Еще одним способом смягчения проблемы может быть упаковка данных IoT на промежуточном уровне, например, в пограничной сети. Для решения этой проблемы требуется дальнейшее исследование и разработка соответствующих решений.

Безопасность приложений: Защита данных пользователя в приложениях IoT является сложной задачей, так как информация, хранящаяся в облаке, Интернете и на мобильных устройствах, включает в себя чувствительные данные, такие как информация о банковском счете, медицинские данные и местоположение. Даже при использовании безопасной связи, защита данных пользователя может быть нарушена, если злоумышленник получит доступ к ним из Интернета, облака или мобильных устройств. Поэтому обеспечение безопасности данных IoT, хранящихся в облаке и на мобильных устройствах, является важной задачей.

Обнаружение и управление уязвимостями: Задача обнаружения и управления уязвимостями в узлах IoT является сложной. Поскольку сети IoT включают в себя множество устройств, обнаружение зараженного узла

представляет собой непростую задачу. Для решения этой проблемы можно провести дальнейшие исследования с целью разработки новых структур.

Оперативность и надежность обслуживания: важно, чтобы IoT-устройства работали непрерывно и были доступны для мониторинга и сбора данных. Возможность компрометации, физического повреждения или кражи IoT-устройств может привести к прерыванию обслуживания. Поэтому обеспечение высокой доступности IoT-устройств играет ключевую роль в системах мониторинга в реальном времени.

Обеспечение конфиденциальности и целостности данных: Обеспечение конфиденциальности и целостности данных представляет собой сложную задачу. Только авторизованные пользователи должны иметь доступ к личным данным. Прежде чем предоставить доступ к данным другому лицу, необходимо получить разрешение от пользователя. Если данные больше не требуются, они должны быть надежно удалены.

Человеческий фактор: Работа с рассеянными пользователями IoT-устройств является сложной задачей с точки зрения человеческого фактора. Например, если владелец автомобиля не заменит неисправное устройство, это может создавать опасность для его жизни и жизни окружающих людей.

Когда речь идет о разработке решений для безопасности, важно учитывать три основных аспекта: конфиденциальность, целостность и доступность. Конфиденциальность данных означает, что только авторизованные лица имеют к ним доступ. Целостность гарантирует, что данные остаются неизменными и не подвергаются несанкционированным изменениям. Доступность, в свою очередь, обеспечивает наличие данных и возможность к ним доступа в любое время. В настоящее время интернет вещей активно проникает во все сферы жизни, включая умные города, сельское хозяйство, управление дорожным движением, автомобили без водителя, логистику, здания, электросети, навигацию по GPS, экологическое управление, промышленный мониторинг, медицинское обслуживание и так далее. При разработке безопасных систем интернета вещей

очень важно обеспечить конфиденциальность, целостность и доступность конфиденциальных данных, собираемых из всех этих умных систем.