DOI: 10.58168/MoInSyTe2024_68-73
УДК 004.384

ОБНАРУЖЕНИЕ АНОМАЛИЙ IOT СЕТИ В ТЕХНОЛОГИИ «УМНЫЙ ДОМ»

Ислам Деван Радуанул[1], А.В. Акименко[1]

[1]ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова»

Аннотация. В данной статье раскрываются широкие возможности технологии умного дома. В работе рассмотрены вопросы безопасности, связанные с практическим применением данной технологии, в частности, проблеме сетевых аномалий. Рассмотрены возможные пути решения этих проблем.

Ключевые слова: «умный дом», безопасность, обнаружение сетевых аномалий, машинное обучение, Интернет вещей.

IOT NETWORK ANOMALY DETECTION IN SMART HOME

Islam Dewan Raduanul[1], A.V. Akimenko[1]

[1]Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. This article reveals the wide possibilities of smart home technology. The paper discusses security issues related to the practical application of this technology, in particular, the problem of network anomalies. Possible ways to solve these problems are considered.

Keywords: smart home, security, network anomaly detection, machine learning, Internet of things.

Бурное развитие современных технологий привело к тому, что Интернет вещей охватил многие сферы жизни человека, включая «умные дома» и «умные пространства». «Умный дом» включает большое количество IoT-объектов, которые работают непрерывно и без перебоев. Повышенная безопасность и аутентификация интеллектуальных устройств обеспечивают спокойную среду для жизни в «умном доме».

Важно отслеживать работу интеллектуальных устройств IoT, чтобы обеспечить их надежность и безотказность. Такие устройства имеют компактные размеры, потребляют относительно немного электроэнергии и прочих ресурсов. Тем не менее, они легко подвергаются атакам злоумышленников. Безопасность и идентификацию устройств «умного дома» можно контролировать, а аномалии обнаруживать с высокой точностью.

Результаты исследований показывают, что алгоритм случайного леса является одной из передовых методологий в интеллектуальных средах. Интернет произвел революцию в мире современных технологий, став неотъемлемой частью повседневной жизни.

Интернет вещей (IoT) – одна из инновационных технологий, охватившая различные сферы человеческой деятельности. Интернет вещей используется в медицине, сельском хозяйстве, торговле, на транспорте, в быту.

Приложения на базе Интернета вещей известны как интеллектуальные приложения. «Умный дом» основан на устройствах, использующих технологию Интернета вещей. Эти устройства обеспечивают работу каждой части «умного дома» с помощью интеллектуальных датчиков и контроллеров. Приложения Интернета вещей интенсивно развиваются, что, в конечном счете, снижает стоимость этих устройств, делает их энергетически эффективными и компактными.

Однако широкое применение устройств Интернета вещей также повышает риск, связанный с их работой. Важной задачей является совершенствование этих устройств с целью повышения их безопасности и защищенности от потенциальных угроз.

Активные исследования ведутся в направлении защиты сетей IoT от неавторизованных пользователей. Технология «умного дома» пользуется все большей популярностью. Это помогает людям, проживающим в квартирах и частных домах управлять бытовой техникой, коммуникациями и прочими системами через единую платформу. Таким образом, люди могут легко контролировать домашние устройства.

Одной из основных задач в технологии «умного дома» является предоставление пользователям возможности контролировать безопасность устройств и принимать соответствующие меры предосторожности. Голосовые контроллеры могут позволить злоумышленникам поставить под угрозу безопасность сети. Пользователь не всегда может своевременно обнаружить подобные вторжения, и защитить от них свое жилище.

Существует два типа систем домашней автоматизации. К ним относятся система с локальным управлением и система с дистанционным управлением.

Локальный контроллер используется для управления внутренними устройствами непосредственно по месту их нахождения. Локально управляемая система может использовать Ethernet, беспроводное соединение или Bluetooth.

Дистанционно управляемые системы работают с использованием подключения к Интернету. Они позволяют управлять устройствами «умного дома» из удаленных мест.

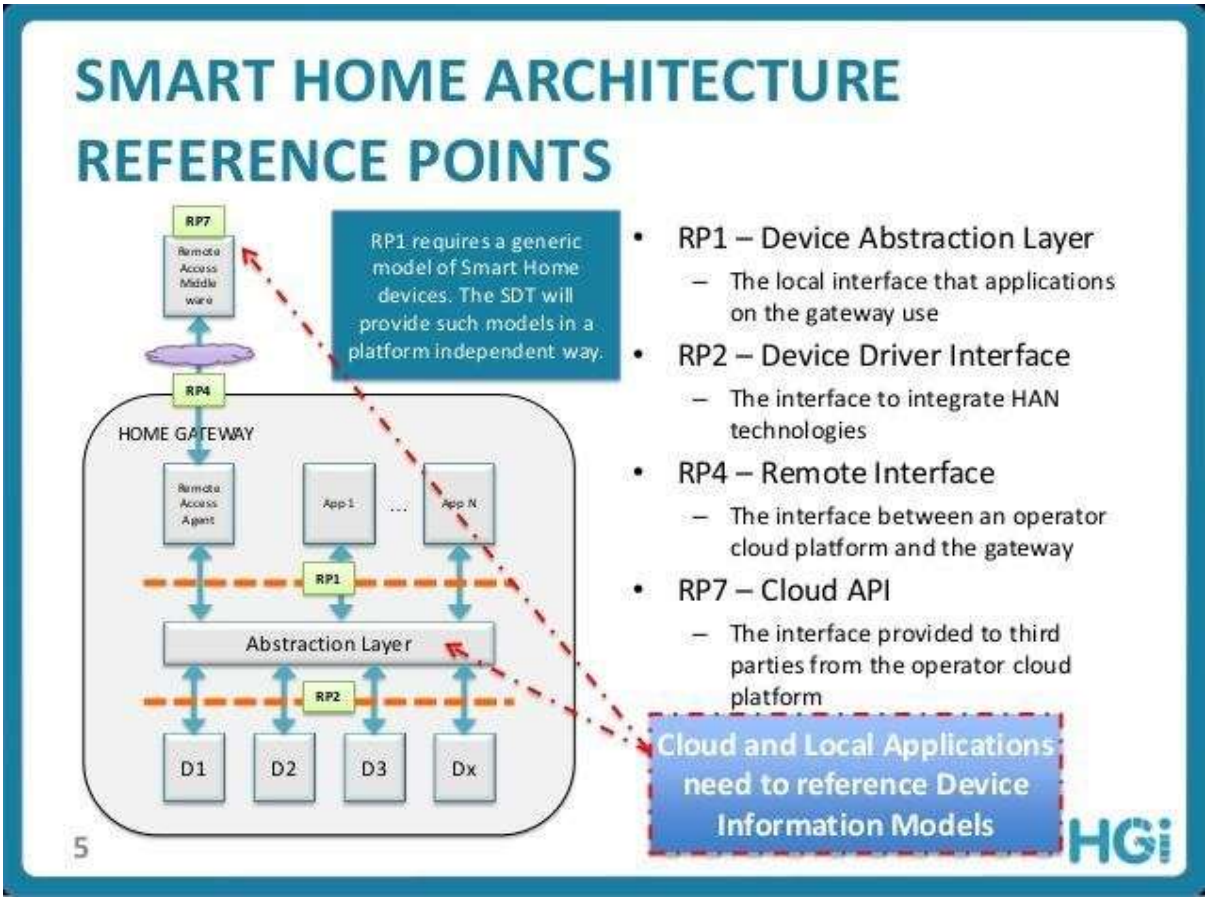

Рисунок 1 – Ориентиры архитектуры «умного дома»

Одним из основных направлений развития умных домашних сред является разработка эффективных, безопасных и надежных технологий и средств обнаружения аномалий и уязвимостей. Основное внимание при этом уделяется выявлению сетевых аномалий. Эти аномалии охватывают ряд вредоносных действий, которые могут включать, помимо прочего:

1. Эксфильтрацию данных (аномалии, связанные с несанкционированной передачей или утечкой данных с устройств Интернета вещей);

2. Действия относительно регистрации нажатий клавиш, которые могут указывать на попытки перехватить конфиденциальную информацию;

3. Отпечатки ОС (аномалии, связанные с попытками идентифицировать операционную систему устройств в сети, часто предшествующие целенаправленным атакам);

4. Сканирование служб (незаконные действия, связанные с исследованием или сканированием служб и портов устройств Интернета вещей);

5. Отклонения в обмене данными UDP (протокол пользовательских дейтаграмм), которые могут указывать на сетевые атаки или подозрительное поведение устройства.

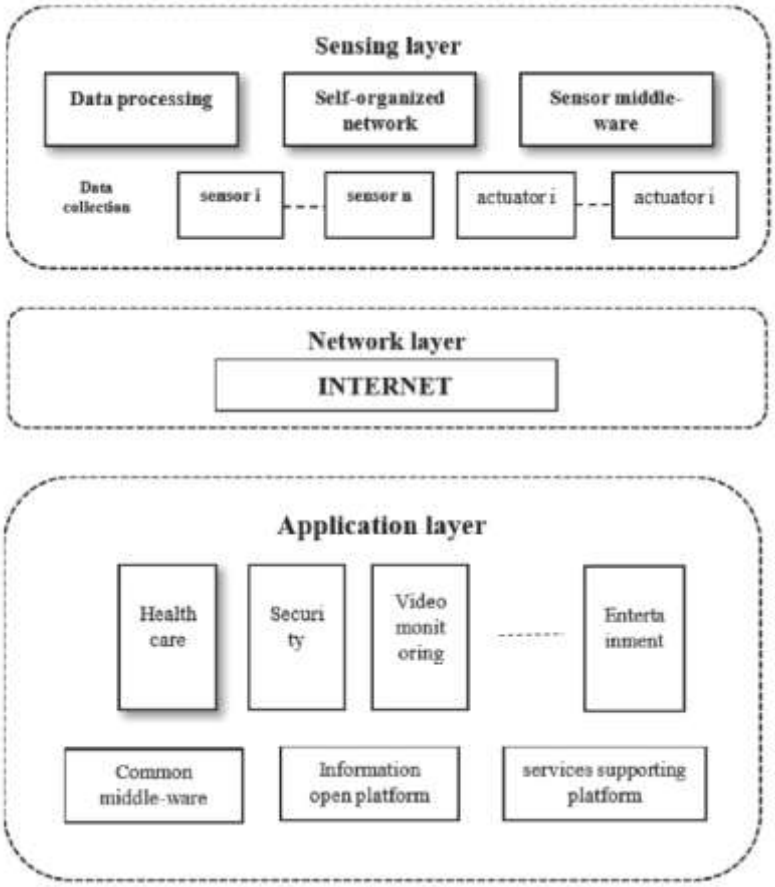

Рисунок 2 – Архитектура системы «умный дом» на базе Интернета вещей.

Одно из предлагаемых решений вышеуказанной проблемы основано на машинном обучении с целью мониторинга аномальной активности в среде умного дома и обнаружения вредоносных действий.

Предлагаемая структура протестирована с использованием шести различных алгоритмов машинного обучения. Дополнительной важной характеристикой этого исследования по обнаружению аномалий является сравнение простых

классификаторов машинного обучения, таких как дерево решений (DT), Ada-Boost (ADA) и случайный лес (RF), со сложными классификаторами, такими как искусственная нейронная сеть (ANN).

Исследование показало следующие результаты:

1. Набор данных для предлагаемой методологии оценивается по шести различным категориям аномалий;

2. Для анализа аномальной активности с помощью алгоритмов машинного обучения реализована система обнаружения аномалий;

3. Предлагаемое исследование имеет высокую производительность и надежные прогнозы для обнаружения аномалий и генерации предупреждений;

4. Основным итогом этого исследования является разработка высокоэффективной модели обнаружения аномалий с использованием машинного обучения.

Умные домашние среды обеспечивают комфорт пользователей и экономию ресурсов. Однако такие системы подвержены атакам из-за недостаточных мер безопасности. Разработка новых технологий, направленных на предотвращение и выявление вредоносной деятельности в сети позволит повысить защищенность компонентов умного дома» от несанкционированных воздействий.

Список литературы

1. Hayes, A. Smart Home: Definition, How They Work, Pros and Cons. – URL: https://www.investopedia.com/terms/s/smart-home.asp (date of the application: 19.03.2024).

2. Odunlade, E. What makes a Smart Home smart? A guide to protocols and applications. – URL: https://www.wevolver.com/article/what-makes-a-smart-home-smart-a-guide-to-protocols-and-applications (date of the application: 20.03.2024).

3. Кущева, И.С. Проблемы ресурсосбережения с учетом специфики некоторых задач двумерного размещения / И.С. Кущева, Е.С. Хухрянская // Моделирование систем и процессов. – 2021. – Т. 14, № 1. – С. 32-38. – DOI: 10.12737/2219-0767-2021-14-1-32-38.

4. Поляков, С.И. Каскадное управление отоплением «умного дома» / С.И. Поляков, В.И. Акимов, А.В. Полуказаков // Моделирование систем и процессов. – 2021. – Т. 14, № 4. – С. 82-89. – DOI: 10.12737/2219-0767-2021-14-4-82-89.

5. Программное обеспечение систем управления «умным» жилым домом / С.И. Поляков, В.И. Акимов, А.В. Полуказаков [и др.] // Моделирование систем

и процессов. – 2021. – Т. 14, № 1. – С. 58-67. – DOI: 10.12737/2219-0767-2021-14-1-58-67.

References

1. Hayes, A. Smart Home: Definition, How They Work, Pros and Cons. – URL: https://www.investopedia.com/terms/s/smart-home.asp (date of the application: 19.03.2024).

2. Odunlade, E. What makes a Smart Home smart? A guide to protocols and applications. – URL: https://www.wevolver.com/article/what-makes-a-smart-home-smart-a-guide-to-protocols-and-applications (date of the application: 20.03.2024).

3. Kushcheva, I.S. Problems of resource saving taking into account the specifics of some problems of two-dimensional placement / I.S. Kushcheva, E.S. Khukhryanskaya // Modeling of systems and processes. – 2021. – T. 14, No. 1. – P. 32-38. – DOI: 10.12737/2219-0767-2021-14-1-32-38.

4. Polyakov, S.I. Cascade control of smart home heating / S.I. Polyakov, V.I. Akimov, A.V. Polukazakov // Modeling of systems and processes. – 2021. – T. 14, No. 4. – P. 82-89. – DOI: 10.12737/2219-0767-2021-14-4-82-89.

5. Software for control systems for “smart” residential buildings / S.I. Polyakov, V.I. Akimov, A.V. Polukazakov [et al.] // Modeling of systems and processes. – 2021. – T. 14, No. 1. – P. 58-67. – DOI: 10.12737/2219-0767-2021-14-1-58-67.