УДК 004.89

РАЗРАБОТКА РЕШЕНИЯ НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ВЫЯВЛЕНИЯ АНОМАЛИЙ В IOT УСТРОЙСТВАХ

Захаров А.С., студент гр. 615, II курс
Московский государственный университет имени М.В. Ломоносова, г. Москва

Интернет вещей (IoT) представляет собой сеть устройств, обеспечивающих сбор и обмен данными без участия человека. Однако, с ростом числа подключенных устройств возникают новые вызовы в области безопасности. В данной статье предлагается решение на основе методов машинного обучения для выявления аномалий в данных IoT устройств. Мы рассмотрим основные принципы работы системы, использующей методы обнаружения аномалий, а также проведем анализ результатов и оценим эффективность предложенного подхода [1-4].

IoT устройства становятся все более распространенными в различных областях, таких как умный дом, промышленность, здравоохранение и транспорт. Однако, большое количество подключенных устройств увеличивает риск возникновения аномального поведения, которое может привести к угрозам безопасности и нарушению работы системы. Для борьбы с этими угрозами необходимо разработать эффективные методы обнаружения аномалий.

Методы обнаружения аномалий в IoT: В данной работе предлагается использовать методы машинного обучения для обнаружения аномалий в данных IoT устройств. Эти методы позволяют автоматически обучать модели на основе исторических данных и выявлять аномалии, которые выходят за пределы ожидаемого поведения. В качестве примеров методов машинного обучения могут быть использованы алгоритмы кластеризации, методы деревьев решений или нейронные сети [5-8].

Архитектура системы: предлагаемая система состоит из следующих компонентов:

1. Сбор данных: Данные с IoT устройств собираются и передаются на центральный сервер для анализа.
2. Подготовка данных: Данные предобрабатываются для удаления шума, заполнения пропущенных значений и нормализации.
3. Обучение модели: Модель машинного обучения обучается на исторических данных для выявления нормального поведения устройств.
4. Обнаружение аномалий: Обученная модель применяется к новым данным для выявления аномалий.

5. Уведомление: В случае обнаружения аномалий генерируется уведомление для оператора системы.

Эксперименты и результаты. Для оценки эффективности предложенного метода проводятся эксперименты на реальных данных IoT устройств. Анализируются метрики качества, такие как точность обнаружения, ложные срабатывания и время обработки данных.

Предложенное решение на основе методов машинного обучения представляет собой эффективный способ обнаружения аномалий в данных IoT устройств. Разработанная система может быть внедрена для обеспечения безопасности и надежности IoT сетей в различных областях применения.

Список литературы:

1. Al-Garadi M. A. A survey of machine and deep learning methods for Internet of Things security / M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, M. Guizani // IEEE Communications Surveys & Tutorials. – 2020. – Vol. 22, № 3. – P. 1646–1685. – DOI: 10.1109/COMST.2020.2988293.
2. Ferrag M. A. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study / M. A. Ferrag, L. Maglaras, S. Moschoyiannis, H. Janicke // Journal of Information Security and Applications. – 2020. – Vol. 50. – Article 102419. – DOI: 10.1016/j.jisa.2019.102419.
3. Miettinen M. IoT SENTINEL: Automated device-type identification for security enforcement in IoT / M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A.-R. Sadeghi, S. Tarkoma // Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems. – Atlanta : IEEE, 2017. – P. 2177–2184. – DOI: 10.1109/ICDCS.2017.283.
4. Anthi E. A supervised intrusion detection system for smart home IoT devices / E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos, P. Burnap // IEEE Internet of Things Journal. – 2019. – Vol. 6, № 5. – P. 9042–9053. – DOI: 10.1109/JIOT.2019.2926365.
5. Diro A. A. Distributed attack detection scheme using deep learning approach for Internet of Things / A. A. Diro, N. Chilamkurti // Future Generation Computer Systems. – 2018. – Vol. 82. – P. 761–768. – DOI: 10.1016/j.future.2017.08.043.
6. Doshi R. Machine learning DDoS detection for consumer Internet of Things devices / R. Doshi, N. Apthorpe, N. Feamster // Proceedings of the 2018 IEEE Security and Privacy Workshops. – San Francisco : IEEE, 2018. – P. 29–35. – DOI: 10.1109/SPW.2018.00013.
7. Meidan Y. N-BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders / Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, D. Breitenbacher, A. Shabtai, Y. Elovici // IEEE Pervasive Computing. – 2018. – Vol. 17, № 3. – P. 12–22. – DOI: 10.1109/MPRV.2018.03367731.

8. Mirsky Y. Kitsune: An ensemble of autoencoders for online network intrusion detection / Y. Mirsky, T. Doitshman, Y. Elovici, A. Shabtai // Proceedings of the Network and Distributed System Security Symposium. – San Diego : Internet Society, 2018. – DOI: 10.14722/ndss.2018.23211.