МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И.Сатпаева

Институт автоматики и информационных технологий

Кафедра Электроники, телекоммуникации и космической технологии

Тоқтарақын Айгерім Ержанқызы

«Разработка оптимизации обнаружения вторжений в сети связи с использованием студии машинного обучения Azure»

ДИПЛОМНАЯ РАБОТА

Специальность 5В074600 – Космическая техника и технологии

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И.Сатпаева

Институт автоматики и информационных технологий

Кафедра «Электроники, телекоммуникации и космических технологий»

ДОПУЩЕН К ЗАЩИТЕ
Заведующий кафедрой
«Электроники,
телекоммуникации и
космических
технологий»
_____ Таштай Е.
"27" 05 20 22 г.

ДИПЛОМНАЯ РАБОТА

На тему: "Разработка оптимизации обнаружения вторжений в сети связи с использованием студии машинного обучения Azure"

по специальности 5В074600 – Космическая техника и технологии

Выполнил Тоқтарақын А.Е.

Рецензент
Заведующий лабораторией
разработки космических систем
ДТОО «Институт космической
техники и технологий»
_____ Елубаев С.
"26" 05 20 г.

Научный руководитель
магистр технических наук,
лектор кафедры «Электроники,
телекоммуникации и
космических технологий»
_____ Боранбаева А.
"26" 05 20 г.

Алматы 2022

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И.Сатпаева

Институт автоматики и информационных технологий

Кафедра «Электроники, телекоммуникации и космическая технологий»

УТВЕРЖДАЮ
Заведующий кафедрой «Электроники, телекоммуникации и космической технологий»
_____ Таштай Е.
"21" XII 2021 г

ЗАДАНИЕ
К выполнению дипломной работы

Дипломнику: *Тоқтарақын Айгерім Ержанқызы*

Тема «Разработка оптимизации обнаружения вторжений в сети связи с использованием студии машинного обучения Azure»

Утвержден приказом №478 ректора университета *от «24» декабря 2021 г.*

Срок сдачи выполненных работ *«30» апреля 2022 г.*

Исходные данные к дипломной работе:

1) Обоснование актуальности темы работы и анализ состояния исследований в области сети связи

2) Разработка методов классификации Студии машинного обучения Microsoft Azure для решения задачи обнаружения вторжений.

3) Оценка качества обучения и исследование эффективности классификации разными методами

Перечень вопросов, рассматриваемых в дипломной работе:

а) Применение методов машинного обучения в задачах обнаружения вторжений;

- *б) Использование функции автоматизированного машинного обучения Машинного обучения Azure для обучения и развертывания прогнозной модели.*

Перечень графического материала: Студия машинного обучения Azure Microsoft , Использование автоматизированного машинного обучения в службе Машинного обучения Azure, алгоритмы классификации Конструктора машинного обучения Microsoft Azure для решения задачи обнаружения аномалий и вторжений.

ГРАФИК

подготовки дипломной работы

Наименование разделов, перечень разрабатываемых вопросов	**Сроки представления научному руководителю**	**Примечание**
1.Обоснование актуальности темы работы и анализ состояния исследований в области сети связи	1.09.2021-31.12.2021	выполнено
2.Анализ существующих методик обнаружения втрожений и возможностей облачной среды Azure по моделированию методов машинного обучения.	1.01.2022-30.01.2022	выполнено
3. Оценка качества обучения и исследование эффективности классификации разными методами	1.02.2022-15.02.2022	выполнено
4. . Написание дипломной работы	15.04.2022-30.04.2022	выполнено

Подписи

консультантов и нормоконтролера на законченную магистерскую диссертацию с указанием относящихся к ним разделов диссертации

Наименование разделов	Консультанты Ф.И.О. (уч.степень, звание)	Дата подписания	Подпись
Анализ существующих методик обнаружения вторжений по моделированию методов машинного обучения	М.т.н, лектор кафедры ЭТиКТ Боранбаева А.	27.05.2022	
Постановка задачи на исследование	М.т.н, лектор кафедры ЭТиКТ Боранбаева А.	27.05.2022	
Анализ исходных данных и их предварительная обработка	М.т.н, лектор кафедры ЭТиКТ Боранбаева А.	27.05.2022	
Нормоконтролер	м.т.н., лектор кафедры ЭТиКТ Ибекеев С.Е..	27.05.2022	

Научный руководитель Боранбаева А.Т.

Задание принял к исполнению обучающийся Токтаракын А.Е.

“21” 12 2021 г.

АҢДАТПА

Бұл дипломдық жұмыста Microsoft Azure бағдарламасының екі класты жіктеу әдістерін зерттеу байланыс желісіндегі енуді анықтау мәселесін шешу үшін жүргізілді. Azure мүмкіндіктер гізделген шабуылды анықтау технологиясы әзірленді. Жіктеу алгоритмдері бойынша анықтау сапасы салыстырылады.

АННОТАЦИЯ

В этой дипломной работе выполнено исследование методов двухклассовой классификации Студии машинного обучения Microsoft Azure для решения задачи обнаружения вторжений в сети связи. Разработана технология обнаружения вторжений на основе возможностей Конструктора машинного обучения Azure. Проведено сравнение качества обнаружения алгоритмами классификации.

ANNOTATION

In this thesis, a study of the methods of two-class classification of the Microsoft Azure Machine Learning Studio was carried out to solve the problem of intrusion detection in communication networks. Intrusion detection technology has been developed based on the capabilities of the Azure Machine Learning Constructor. The quality of detection by classification algorithms is compared.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Под информацией понимается любой вид накапливаемых, хранимых и обрабатываемых данных.

Под информационной безопасностью понимают защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Современное развитие мировой экономики характеризуется все большей зависимостью рынка от значительного объема информационных потоков.

Актуальность проблем, связанных с защитой потоков данных и обеспечением информационной безопасности их обработки и передачи, все более усиливается. Проблема защиты информации является многоплановой и комплексной

Обнаружение мошенничества и вторжений являются ключевыми элементами новой национальной задачи по защите критически важных инфраструктур нашей страны.

В дипломной работе также демонстрируется, как методы, разработанные для обнаружения атак, могут быть обобщены и применены к важной области обнаружения вторжений в сетевые информационные системы.

На сегодняшний день, для решения проблем безопасности часто предполагается задействование методов искусственного интеллекта (ИИ), в частности методов машинного обучения. В информационной безопасности ИИ – это программное обеспечение, способное интерпретировать состояние среды, распознавать происходящие в ней события и самостоятельно принимать необходимые меры. ИИ особенно хорошо справляется с распознаванием закономерностей и аномалий, поэтому может быть прекрасным инструментом обнаружения угроз.

Системы машинного обучения – это программное обеспечение, способное самостоятельно обучаться на введенных человеком данных и результатах выполненных действий. Средства машинного обучения способны строить прогнозы, опираясь на сведения о развитии событий в прошлом.

Хорошую базу для создания решений ИИ предоставляют современные облачные сервисы, например, такие как Microsoft Azure. Поэтому тема дипломной работы, которая разработка оптимизации обнаружения вторжений в сети связи с использованием методов машинного обучения является актуальной.

1 ОБОСНОВАНИЕ АКТУАЛЬНОСТИ ТЕМЫ РАБОТЫ И АНАЛИЗ СОСТОЯНИЯ ИССЛЕДОВАНИЙ В ОБЛАСТИ СЕТИ СВЯЗИ

Современный период развития социально-экономических и политических процессов в стране сопровождается развитием информационных ресурсов. В этих условиях существенно повышается роль информации и актуализируется проблема формирования единого информационного пространства страны и перехода от индустриального к информационному обществу. Необходимым условием решения этой проблемы является совершенствование информационного обеспечения деятельности органов государственного управления, научных, промышленных, банковских и других структур на основе предоставления достоверной, своевременной, полной, системно организованной и безопасной информации как основы эффективного управления, безопасности личности, общества и государства.

Решение этих вопросов неразрывно связано с созданием уникальных телекоммуникационных систем и обеспечением их безопасности в условиях широкого использования новых информационных технологий и воздействия внутренних и внешних угроз информационной безопасности. Ярким проявлением таких угроз являются широкомасштабные «информационные войны», несанкционированный доступ к защищаемым информационным ресурсам, недостаточная информированность должностных лиц органов государственного управления при анализе социально–экономических, политических, военных, экологических и других ситуаций.

С учетом этого обеспечение информационной безопасности предполагает наличие эффективной системы администрирования и контроля безопасности информации на телекоммуникационных объектах, по результатам функционирования которой реализуется комплекс адекватных методов устойчивой защиты от угроз, разработкой научно обоснованных методов обеспечения защиты информации в условиях неопределенности, риска, внешних воздействий и динамичных внутренних изменений объектов деятельности. В настоящее время известно значительное количество работ, посвященных отдельным, частным аспектам рассматриваемой проблемы. Однако большинство авторов основное внимание уделяли вопросам создания технических средств, систем обработки, защиты информации и, в меньшей степени, вопросам, проблемам теоретического и системного плана, в основе которых лежат управленческие аспекты обеспечения безопасности информации.

1.1 Анализ существующих методик обнаружения вторжений по моделированию методов машинного обучения.

По мере того, как достижения в области сетевых технологий помогают соединить отдаленные уголки земного шара, а Интернет продолжает расширять свое влияние как средство коммуникации и торговли, угроза со стороны спамеров, злоумышленников и криминальных

предприятий также соответственно возросла. Распространенность таких угроз привела к тому, что системы обнаружения вторжений — киберпространственный эквивалент охранной сигнализации — заняли место в ряду с брандмауэрами в качестве одной из фундаментальных технологий сетевой безопасности. Однако сегодняшние коммерчески доступные системы обнаружения вторжений представляют собой преимущественно основанные на сигнатурах системы обнаружения вторжений, предназначенные для обнаружения известных атак путем использования сигнатур этих атак. Такие системы требуют частых обновлений базы правил и обновлений сигнатур и не способны обнаруживать неизвестные атаки. В противоположность, системы обнаружения аномалий, подмножество систем обнаружения вторжений, моделируют нормальное поведение системы/сети, что позволяет им быть чрезвычайно эффективными в обнаружении и отражении как известных, так и неизвестных атак или атак «нулевого дня». Хотя системы обнаружения аномалий концептуально привлекательны, необходимо решить множество технологических проблем, прежде чем они смогут получить широкое распространение. Эти проблемы включают в себя: высокий уровень ложных срабатываний, невозможность масштабирования до гигабитных скоростей и т. д

Современные сетевые системы испытывают много проблем из-за уязвимостей в системе безопасности, таких как переполнение буфера, ошибки в Microsoft Internet, слишком простой протокол маршрутизации сенсорной сети, недостатки безопасности приложений и операционных систем. Более того, беспроводные устройства, такие как смартфоны, персональные цифровые помощники (КПК) и датчики, стали экономически целесообразными благодаря технологическим достижениям в области беспроводной связи и производства небольших и недорогих датчиков. Существуют типологии уязвимостей, которые будут использоваться в этих устройствах. Для повышения безопасности используются многие механизмы, включая аутентификацию, криптографию, контроль доступа и системы обнаружения вторжений (IDS).

В целом методы обнаружения вторжений можно разделить на две группы: обнаружение неправильного использования и обнаружение аномалий. Системы обнаружения злоупотреблений используют шаблоны хорошо известных атак или слабые места систем для выявления вторжений. Слабость систем обнаружения злоупотреблений заключается в том, что они не могут обнаружить какое-либо будущее (неизвестное) вторжение до тех пор, пока соответствующие сигнатуры атак не будут введены в базу данных сигнатур. Методы обнаружения аномалий пытаются определить, является ли отклонение от установленных нормальных моделей использования или нет. Критический успех обнаружения аномалий зависит от модели нормального поведения.

Однако, несмотря на совершенствование мер защиты, угрозы информационной безопасности в СС продолжают существовать и прежде всего в виде целенаправленных атак.

С ростом популярности спутникового интернета в бизнес-сфере появилась и проблема защиты информации. С проблемой реализации шифрования столкнулись спутниковые интернет - провайдеры. Связано это с

задержкой передачи данных в спутниковом интернете. Ведь для спутникового интернета вместо обычного протокола интернета TCP/IP используется протокол TCP (TCPA), который позволяет сократить время загрузки страниц за счёт буферизации больших объектов и посылки информации в сжатом виде. Однако, протокол TCPA не может работать с зашифрованными пакетами. Поэтому большинство пользователей спутникового интернета не передают через спутниковые каналы связи конфиденциальную информацию. Основное решение данной проблемы – асинхронное шифрование. Данные шифруются на компьютере пользователя и передаются на сервер спутникового провайдера, где запрос дешифровывается и с помощью протокола TCPA ответ сжимается и передаётся на спутник и со спутника обратно пользователю. Это делает связь намного безопаснее, но ставит проблему для безопасных сетей и VPN, где используются свои методы шифрования. Только параллельное развитие алгоритмов шифрования и ускорителей спутниковых провайдеров по введению определённых стандартов способно решить эту проблему.

Уязвимости в стеке протоколов связи (TCP/IP) приводят к намеренным атакам распределенного отказа в обслуживании. Атаки могут быть обнаружены с использованием существующих методов искусственного интеллекта , точнее, машинного обучения.

Искусственный интеллект — это способность компьютерной системы имитировать когнитивные функции человека, такие как обучение и решение проблем. Искусственный интеллект позволяет компьютерной системе применять математику и логику для моделирования рассуждений, используемых людьми для получения новых сведений и принятия решений.

Хотя ИИ и машинное обучение тесно связаны, это разные понятия. Машинное обучение считается подмножеством ИИ.

Машинное обучение является применением ИИ. Это процесс использования математических моделей данных для обучения компьютера без прямых инструкций. Оно позволяет компьютерной системе продолжить обучение и самостоятельное улучшение на основе опыта.

«Интеллектуальный» компьютер использует ИИ, чтобы мыслить как человек и самостоятельно выполнять задачи. Машинное обучение — это способ развития интеллекта компьютерной системой.

Один из способов обучить компьютер имитировать мышление человека — использовать нейронную сеть. Это серия алгоритмов, смоделированных по принципу работы человеческого мозга. Нейронная сеть помогает компьютерной системе создать искусственный интеллект на основе глубокого обучения. Такая тесная связь объясняет, почему при сравнении ИИ и машинного обучения полезно рассмотреть, как они работают вместе. При оценке различий между искусственным интеллектом и машинным обучением полезно понять, как тесно они связаны и как они взаимодействуют. ИИ и машинное обучение работают вместе так:

Шаг 1.Система ИИ создается с использованием машинного обучения и других техник.

Шаг 2.Модели машинного обучения создаются на основе выявления закономерностей в данных.

Шаг 3.Специалисты по обработке и анализу данных оптимизируют модели машинного обучения с учетом закономерностей в данных.
Шаг 4.Процесс повторяется и совершенствуется до тех пор, пока точность модели не станет достаточно высокой для выполнения нужных задач.

Преимущества ИИ и машинного обучения-связь между искусственным интеллектом и машинным обучением обеспечивает значительные преимущества для компаний практически в любой отрасли, причем новые возможности появляются регулярно. Это лишь некоторые из основных преимуществ:больше источников входных данных;улучшенное и ускоренное принятие решений

1.2 Категории методов обнаружения вторжений

Ряд исследований и обзорных статей посвящен технологиям обнаружения вторжений или интеллектуального анализа данных в конкретных приложениях.

Поскольку принципы обнаружения вторжений были впервые введены Деннингом в 1987 году, было разработано большое количество систем реактивной защиты. В работе методы обнаружения вторжений категоризируются по 3 категориям, а именно, единичные (single), гибридные и ансамбли. Рассмотрим гибридную категорию. Гибридные системы обнаружения вторжений сочетают в себе методы обоих этих подходов. Каждая техника имеет свои преимущества и недостатки. Некоторые преимущества методов обнаружения аномалий по сравнению с другими можно сформулировать следующим образом. Во- первых, они способны обнаруживать инсайдерские атаки. Например, если какой-либо пользователь использует какую-либо украденную учетную запись и выполняет такие действия, которые выходят за рамки обычного профиля пользователя, система обнаружения аномалий генерирует сигнал тревоги. Во- вторых, система обнаружения основана на заказных профилях. Злоумышленнику становится очень трудно осуществлять какую-либо деятельность, не вызывая тревоги. Наконец, он может обнаруживать атаки, которые ранее не были известны.

Системы обнаружения аномалий ищут аномальные события, а не атаки. В этой работе мы сосредоточимся на различных методах обнаружения аномалий.

Обнаружение вторжений — это процесс поиска паттернов в наборе данных, поведение которых не является нормальным в ожидаемом режиме. Это неожиданное поведение также называют аномалиями или выбросами. Аномалии не всегда можно классифицировать как атаку, но это может быть удивительным поведением, которое ранее не было известно. Это может быть вредно, а может и нет. Когда данные должны быть проанализированы, чтобы найти связь или предсказать, используются известные или неизвестные методы интеллектуального анализа данных. К ним относятся методы кластеризации, классификации и машинного обучения. Кроме того, для достижения более высокого уровня точности обнаружения аномалий создаются гибридные подходы. При таком подходе авторы пытаются объединить существующие

алгоритмы интеллектуального анализа данных для получения лучших результатов. Таким образом, обнаружение аномального или неожиданного поведения или аномалий даст возможность изучить и классифицировать его в новый тип атак или любой конкретный типвторжений.

Хотя существуют различные подходы к поиску аномалий, их можно свести к общему алгоритму, как показано на рис.1.1.

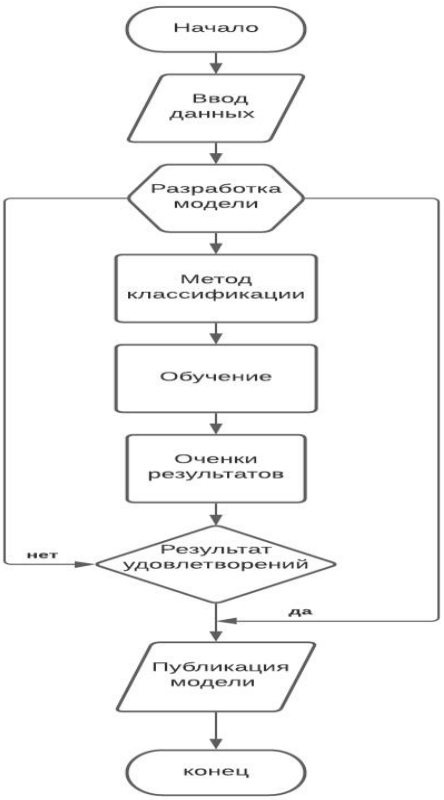

Рисунок 1.1 – Алгоритм функционирования методов машинного обучения

Этап обучения*:* модель строится на основе нормального (или ненормального) поведения системы. Существуют различные способы, которые могут быть выбраны в зависимости от рассматриваемого типа обнаружения аномалий. Он может быть как ручным, так и автоматическим.

Стадия обнаружения*:* когда модель для системы доступна, она сравнивается с (параметризованным или предопределенным) наблюдаемым трафиком. Если обнаруженное отклонение превышает (или меньше, чем в случае моделей аномалий) заданный порог, то срабатывает сигнал тревоги.

1.3 Анализ методов машинного обучения

Методы обнаружения аномалий на основе кластеризации

Кластеризация может быть определена как разделение данных на группы сходных объектов. Каждая группа, или кластер, состоит из объектов, которые похожи друг на друга и непохожи на объекты других групп [13]. Алгоритмы

кластеризации способны обнаруживать вторжения без предварительного знания. Существуют различные методы выполнения кластеризации, которые могут быть применены для обнаружения аномалий. Ниже приводится описание некоторых из предложенных подходов

K-средних*:* кластеризация — k-средних-это метод кластерного анализа, где мы определяем к непересекающихся кластеров на основе функции стоимости объектов должны быть сгруппированы. Здесь k-это определяемый пользователем параметр. Существует подход сетевого интеллектуального анализа данных (NDM), который использует алгоритм кластеризации K-mean для разделения временных интервалов с нормальным и аномальным трафикомв обучающем наборе данных. Полученные центроиды кластеров затем используются для быстрого обнаружения аномалий при мониторинге новых данных.

K-Medoids*:* этот алгоритм очень похож на алгоритм k-Means. Она отличается главным образом в своем представлении различных кластеров. Здесь каждый кластер представлен наиболее центрированным объектом в кластере, а не неявным средним значением, которое может не принадлежать кластеру. Метод k-medoids является более надежным, чем алгоритм k-means,в присутствии шума и выбросов, поскольку медоид меньше подвержен влиянию выбросов или других экстремальных значений, чем среднее значение. Этот метод обнаруживает сетевые аномалии, которые содержат неизвестное вторжение. Он был сравнен с различными другими алгоритмами кластеризации и обнаружил, что когда дело доходит до точности, он дает гораздо лучшие результаты, чем k-Means.

Кластеризация ЭМ: этот алгоритм можно рассматривать как расширение среднего значения k, которое присваивает объект кластеру, на который он похож, на основе среднего значения кластера. В этом подходе вместо назначения объекта в выделенном кластере назначьте объект кластеру в соответствии с весом, представляющим вероятность членства. Другими словами, между кластерами нет строгих границ. Здесь новое среднее вычисляется на основе весовых мер. По сравнению с k-средними и k-медоидами ЭМ превосходила их и приводила к более высокой точности.

Алгоритмы обнаружения выбросов: обнаружение выбросов — это метод поиска паттернов в данных, которые не соответствуют ожидаемому поведению. Поскольку выброс может быть определен как точка данных, которая сильно отличается от остальных данных, основанных на определенных мерах. Существует несколько схем обнаружения выбросов. Пользователь может выбрать любой из них на основе его эффективности и того, как он может справиться с проблемой обнаружения аномалий. Одним из таких подходов является дистанционный подход. Он основан на алгоритме ближайших соседей и реализует четко определенную метрику расстояния для обнаружения выбросов. Чем больше расстояние от объекта до его соседа, тем больше вероятность того, что он будет выбросом. Это эффективный подход к обнаружению зондирующих атак и атак типа "отказ в обслуживании" (DoS). Другой - основанный на плотности подход к локальнымвыбросам. Обнаружение выбросов на основе расстояния зависит от общего или глобального

распределения данного набора точек данных. Данные распределены неравномерно, поэтому дистанционный подход сталкивается с различными трудностями при анализе данных. Основная идея этого методаоснованного на плотностисостоит в том чтобы присвоить каждому примеру данных степень выброса которая называется локальным фактором выброса (LOF).Фактор выброса является локальным в том смыслечто рассматривается только ограниченная окрестность каждого объекта.Для обнаружения аномалий в беспроводных сенсорных сетях (WSN) предлагаются различные другие алгоритмы.Была предложена иерархическая структура для преодоления проблем в WSN,где точная модель аппроксимированная модель изучаются на удаленных узлах сервера и приемника.Также предлагается аппроксимированный алгоритм локального фактора выбросакоторый может быть изучен в узлах приемника для модели обнаружения в WSN.Они обеспечивают более эффективные и точные результаты.

Классификация может быть определена как задача идентификации категории новых экземпляров на основе обучающего набора данных, содержащего наблюдения (или экземпляры или кортежи), принадлежность которых к категории известна. Эту категорию можно назвать меткой класса. Различные экземпляры могут принадлежать к одной или многим меткам класса. В машинном обучении классификация рассматривается как пример контролируемого обучения, например обучения, в котором имеется обучающий набор правильно идентифицированных наблюдений. Алгоритм, реализующий классификацию, называется классификатором. Он построен для предсказания категориальных меток или атрибутов меток классов. В случае обнаружения аномалий он будет классифицировать данные в целом на две категории, а именно нормальные или ненормальные. Ниже приведены общие технологии машинного обучения для обнаружения аномалий экспертные значения для сложной задачи. При таком подходе данные классифицируются на основе различных статистических показателей.

Дерево классификации*:* в машинном обучении дерево классификации также называется моделью прогнозирования или деревом принятия решений. Это древовидный шаблон графа, который похож на структуру блок-схемы; внутренние узлы являются тестовым свойством, каждая ветвь представляет результат теста, а конечные узлы или листья представляют класс, к которому принадлежит любой объект. Наиболее фундаментальным и распространенным алгоритмом, используемым для классификации дерева, является ID3 и C4. 5 Существует два метода построения дерева: построение сверху вниз и обрезка снизу вверх. ID3 и C4. 5 относятся к построению дерева сверху вниз. Дальнейшие подходы к дереву классификации при сравнении с наивной классификацией Байеса результат, полученный из деревьев решений, оказался более точным .

Нечеткая логика: она выводится из теории нечетких множеств, которая имеет дело с рассуждениями, которые являются приближенными, а не точно выведенными из классической логики предикатов. Прикладная сторона теории нечетких множеств имеет дело с хорошо продуманными экспертными значениями реального мира для сложной задачи. При таком подходе данные

классифицируются на основе различных статистических показателей.

Эти части данных применяются с помощью правил нечеткой логики, чтобы классифицировать их как нормальные или вредоносные. Существуют различные другие методы нечеткого интеллектуального анализа данных для извлечения паттернов, представляющих нормальное поведение для обнаружения вторжений, которые описывают различные модификации существующих алгоритмов интеллектуального анализа данных с целью повышения эффективности и точности.

Наивная байесовская сеть: существует множество случаев, когда существуют статистические зависимости или причинно-следственные связи между системными переменными. Иногда бывает трудно точно выразить вероятностные отношения между этими переменными. Другими словами, прежнее знание о системе состоит просто в том, что некоторые переменные могут быть подвержены влиянию других. Чтобы воспользоваться этой структурной связью между случайными величинами задачи, можно использовать вероятностную графовую модель, называемую наивными Байсианскими сетями (NB). Эта модель дает ответ на такие вопросы, как если бы было дано несколько наблюдаемых событий, то какова вероятность того или иного вида атаки. Это можно сделать, используя формулу для условной вероятности. Структура NB обычно представлена направленным ациклическим графом (DAG), где каждый узел представляет одну из системных переменных, а каждое звено кодирует влияние одного узла на другой. При сравнении дерева решений и байсианских методов, хотя точность дерева решений намного выше, но вычислительное время байсианской сети невелико. Следовательно, когда набор данных очень велик, будет эффективно использовать NB-модели.

Генетический алгоритм*:* он был введен в области вычислительной биологии. Эти алгоритмы относятся к более широкому классу эволюционных алгоритмов (ЭА). Они генерируют решения оптимизационных задач с использованием методов, вдохновленных естественной эволюцией, таких как наследование, отбор, мутация и скрещивание. С тех пор они были применены в различных областях с очень многообещающими результатами. При обнаружении вторжений генетический алгоритм (ГА) применяется для получения набора правил классификации из данных аудита сети. Система поддержки и доверия используется в качестве функции пригодности для оценки качества каждого правила. Важными свойствами га являются его устойчивость к шуму и способность к самообучению. Преимущества методов га, описанных в случае обнаружения аномалий, заключаются в высокой частоте обнаружения атак и более низкой частоте ложноположительных результатов.

Нейронные сети: это совокупность взаимосвязанных узлов, предназначенных для имитации функционирования человеческого мозга. Каждый узел имеет взвешенное соединение с несколькими другими узлами в соседних слоях. Отдельные узлы принимают входные данные, полученные от Соединенных узлов, и используют веса вместе с простой функцией для вычисления выходных значений. Нейронные сети могут быть построены для контролируемого или неконтролируемого обучения . Пользователь указывает

количество скрытых слоев, а также количество узлов внутри определенного скрытого слоя. В зависимости от приложения выходной слой нейронной сети может содержать один или несколько узлов. Многослойные нейронные сети восприятия (MLP) были очень успешны в различных приложениях и давали более точные результаты, чем другие существующие вычислительные модели обучения. Они способны аппроксимировать с произвольной точностью любую непрерывную функцию до тех пор, пока содержат достаточное количество скрытых единиц. Это означает, что такие модели могут формировать любую границу решения о классификации в пространстве признаков и, таким образом, действовать как нелинейная дискриминантная функция.

Машина опорных векторов: это набор связанных контролируемых методов обучения, используемых для классификации и регрессии. Машина вектора поддержки (SVM) широко применяется в области распознавания образов. Он также используется для системы обнаружения вторжений. Один класс SVM основан на одном наборе примеров, принадлежащих к определенному классу, и никаких отрицательных примеров, а не на использовании положительного и отрицательного примера.

1.4 Анализ возможностей облачной среды AZURE по моделированию методов машинного обучения

Служба «Машинное обучение Microsoft Azure» предоставляет разработчикам и специалистам по обработке и анализу данных все средства, необходимые для рабочих процессов машинного обучения. Она поддерживает как методику Code First, так и подход с минимальной потребностью в создании кода.

«Машинное обучение Microsoft Azure» можно использовать для машинного обучения любого рода — от классического машинного обучения до глубокого обучения, контролируемого и неконтролируемого обучения. Можно писать код Python или R, используя пакет SDK, или варианты без кода или с минимальным созданием кода, например в студии, также можете создавать, изучать и отслеживать модели машинного обучения и глубокого обучения в рабочей области.

Типичное машинное обучение в Azure выполняется пошагово:

Шаг 1. Сбор и подготовка данных. После определения источников данных доступные данные компилируются. Тип используемых данных поможет определить, какие алгоритмы машинного обучения вы можете применять. При проверке данных обнаруживаются аномалии, разрабатывается структура и устраняются проблемы с целостностью данных

Шаг 2. Обучение модели. Подготовленные данные делятся на две группы: набор для обучения и набор для проверки. Набор для обучения — это большая часть данных, с помощью которых модели машинного обучения настраиваются с максимальной точностью.

Шаг 3. Проверка модели. При выборе конечной модели данных

производительность и точность оценивается с помощью набора для проверки.

Шаг 4. Интерпретация результатов. Полученные данные изучаются, чтобы получить аналитические сведения, сформировать выводы и спрогнозировать результаты.

Служба «Машинное обучение Microsoft Azure» предоставляет разработчикам и специалистам по обработке и анализу данных все средства, необходимые для рабочих процессов машинного обучения, в том числе:

Конструктор Машинного обучения Azure. Перетащите модули, чтобы создать эксперименты, а затем разверните конвейеры.

Записные книжки Jupyter. Используйте наши примеры записных книжек или создайте свои записные книжки, чтобы использовать для машинного обучения наши примеры для пакета SDK для Python.

Скрипты R или записные книжки, в которых используется пакет SDK для R для написания собственного кода, или модули R в конструкторе.

Акселератор решений для многих моделей (предварительная версия) основан на службе Машинного обучения Azure и позволяет обучать, использовать и обслуживать сотни и даже тысячи моделей машинного обучения.

Расширение машинного обучения для пользователей Visual Studio Code. Интерфейс командной строки для машинного обучения.

Платформы с открытым кодом, например Python, PyTorch, T ensorFlow, scikit-learn и многие другие.

Обучение с подкреплением с помощью Ray RLlib.

Вы можете даже использовать MLflow для мониторинга метрик и развертывания моделей или Kubeflow для создания конвейеров сквозных рабочих процессов.

Студия Машинного обучения Azure — это веб-портал в службе "Машинное обучение Azure" для обучения моделей, развертывания и управления активами с написанием минимального количества кода или без него. Для удобства работы студия интегрируется с пакетом SDK для Машинного обучения Azure.

Конструктор Машинного обучения Azure используется для обучения и развертывания моделей машинного обучения без написания кода в виде визуального перетаскивания объектов на холст рабочей области (рис.1.2).

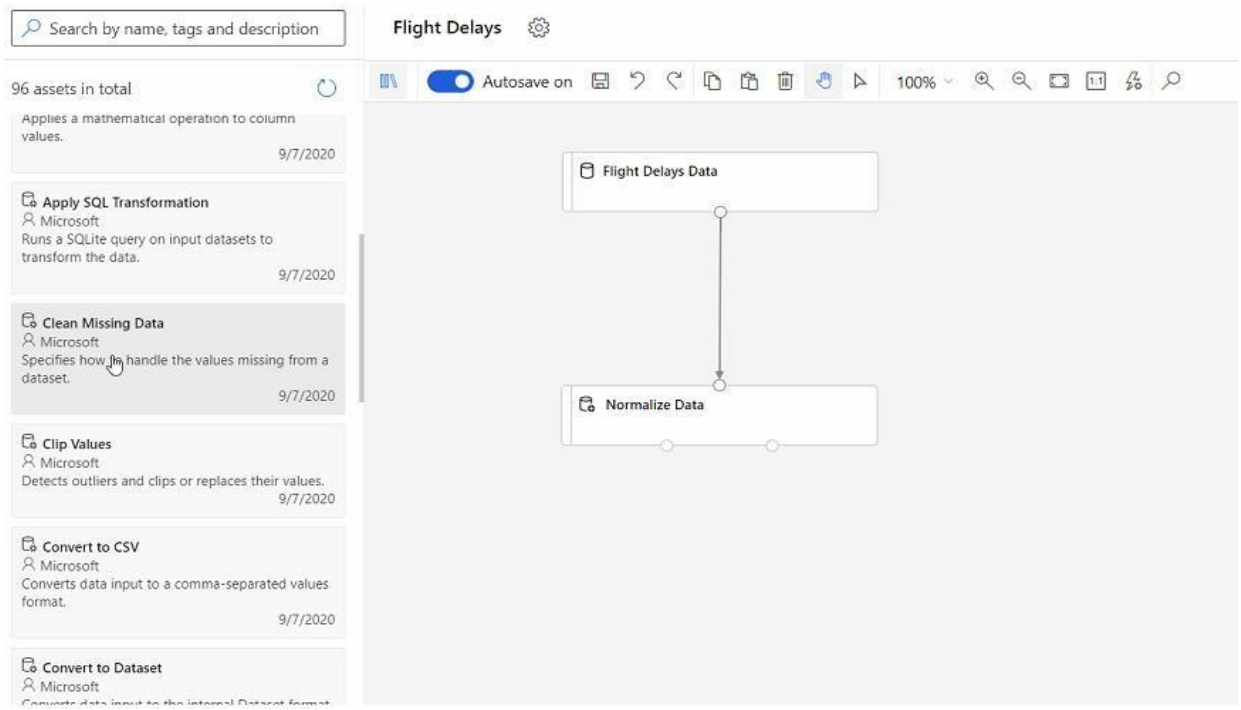

Рисунок 1.2 – Пример работы в Конструкторе Машинного обучения Azure

В составе Конструктора Машинного обучения Azure имеются возможности производить классификацию, кластеризацию и настраивать упрощенную нейронную сеть.

Студия Машинного обучения Azure — это веб-портал в службе "Машинное обучение Azure" для обучения моделей, развертывания и управления активами с написанием минимального количества кода или без него. Для удобства работы студия интегрируется с пакетом SDK для Машинного обучения Azure.

Конструктор Машинного обучения Azure используется для обучения и развертывания моделей машинного обучения без написания кода в виде визуального перетаскивания объектов на холст рабочей области (рис.1.2).

1.5. Постановка задачи на исследование

Проведенный анализ показал, что для решения проблем безопасности в СС необходимо использование методов искусственного интеллекта (ИИ), в частности методов машинного обучения. В информационной безопасности ИИ – это программное обеспечение, способное интерпретировать состояние среды, распознавать происходящие в ней события и самостоятельно принимать необходимые меры. ИИ особенно хорошо справляется с распознаванием закономерностей и аномалий, поэтому может быть прекрасным инструментом обнаружения угроз.

Выявление аномалий в СС можно описать следующим обобщенным алгоритмом:

- Определение входных данных для алгоритма (в большинстве случаев

это сетевой трафик или некоторая метаинформация о нем).

- Обработка входных данных (это может быть глубокая инспекция пакетов или вычисление каких-то количественных или качественных характеристик трафика).
- Применение метода обнаружения аномалий (полностью автономного или, опирающегося на фиксированный набор правил или оценку внешним экспертом).
- Выявление аномалии по количественным или качественным характеристикам.

В качестве метода обнаружения аномалий будем использовать методы классификации (с применением различных алгоритмов машинного обучения и математической статистики).

Классификация, в общем случае, призвана определить для наблюдаемого состояния защищаемой системы является ли оно нормальным или аномалией (на основе данных, полученных на предыдущем шаге). Классификация может анализировать как мгновенное состояние системы, таки использовать сведения о предыдущих наблюдаемых состояниях системы (например, методом рекуррентной нейронной сети).

Классификацию будем проводить с использованием Конструктора Машинного обучения Azure.

Таким образом, необходимо построить общую модель с методами классификации в Конструкторе Машинного обучения Azure, обучить ее на исходных данных, оценить качество выявления аномалий и сравнить различные методы классификации между собой.

2 РАЗРАБОТКА МЕТОДОВ КЛАССИФИКАЦИИ СТУДИИ МАШИННОГО ОБУЧЕНИЯ MICROSOFT AZURE ДЛЯ РЕШЕНИЯ ЗАДАЧИ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

2.1 Разработка архитектуры решения по созданию технологии обнаружения аномалий средствами машинного обучения AZURE.

Студия машинного обучения – это инструмент, поддерживающий функцию перетаскивания объектов и предназначенный для создания, тестирования и развертывания решений для прогнозного анализа. Она позволяет создание, тестирование развертывание моделей машинного обучения. Студия (классическая) публикует модели как веб – службы , которые можно использовать в пользовательских приложениях. Для разработки модели прогнозной аналитики обычно используются данные из одного или нескольких источников. Для получения набора результатов эти данные преобразуются и анализируются с помощью различных операций и статистических функций подготовленная и эффективная модель.

Студия машинного обучения предоставляет интерактивную визуальную рабочую область, которая упрощает создание, тестирование и выполнение итераций модели прогнозной аналитики.

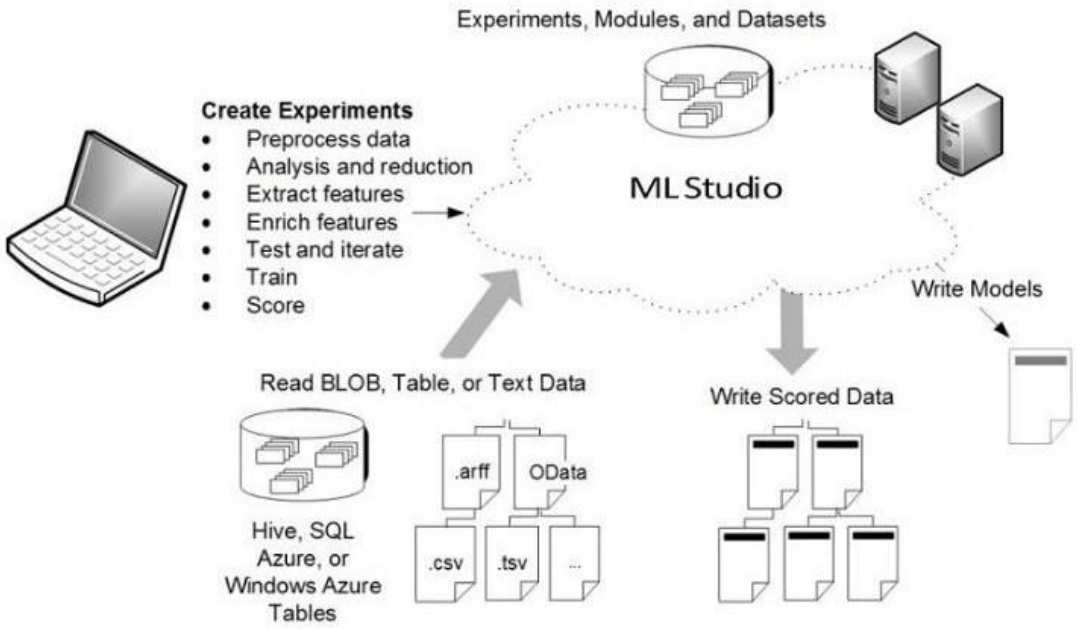

Рисунок 2.1 – Схема работы студии машинного обучения Azure

Она предоставляет возможность в режиме конструктора перетаскивать наборы данных и модули анализа на интерактивное полотно и связывать их вместе, чтобы создать эксперимент, который затем выполняется в Студии машинного обучения (классической). Для выполнения итераций в макете модели нужно отредактировать эксперимент, при необходимости сохранить копию и выполнить его снова. Когда модель будет готова, учебный эксперимент можно превратить в прогнозный, а затем опубликовать его как

веб-службу, чтобы модель стала доступна другим пользователям. При этом не нужно быть специалистом по программированию. Выполняется визуальное соединение наборов данных и модулей, чтобы создать модель прогнозной аналитики.

Эксперимент состоит из наборов данных, предоставляющих данные для модулей аналитики, которые соединяются друг с другом для создания модели прогнозной аналитики. В частности, правильный эксперимент имеет следующие характеристики:

1. В эксперименте по крайней мере один набор данных и один модуль.
2. Наборы данных могут быть связаны только с модулями.
3. Модули могут быть связаны либо с наборами данных, или с другимимодулями.
4. Все входящие порты для модулей должны иметь связь с потокомданных.
5. Все необходимые параметры для каждого модуля должны быть установлены.
6. Эксперимент можно создать с нуля или на основе существующегоэксперимента в качестве шаблона.

Набор данных – это данные, отправленные в Студию машинного обучения (классическую) для использования в процессе моделирования. В студию машинного обучения (классическую) включено несколько наборов данных, чтобы с ними можно было экспериментировать. Кроме того, можно отправлять дополнительные наборы данных по мере необходимости.

Модуль — это алгоритм, который можно выполнять с данными. ВСтудии машинного обучения (классической) есть ряд модулей, начиная с функций ввода данных для процессов обучения, оценки и проверки. Примеры модулей:

– вычисления элементарной статистики – выполняет элементарные статистические вычисления, такие как получение математического ожидания, среднеквадратического отклонения и др;
– классификация – дает набор модулей с методами классификации;
– модель оценки выполняет оценку обученной модели классификации или регрессии.

При создании эксперимента можно выбрать модули из списка, расположенного на холсте слева.

Модуль может иметь ряд параметров, которые можно использовать для настройки внутренних алгоритмов модуля. При выборе модуля на полотне его параметры отображаются на панели «Свойства» в правой части полотна. Подстройка модели осуществляется изменением параметров в этой области.

После подготовки модели прогнозной аналитики можно развернуть ее как веб-службу непосредственно из студии машинного обучения (классической).

Будем разрабатывать модель классификации с помощью конструктора. Конструктор — это средство перетаскивания, которое позволяет создавать модели машинного обучения без единой строки кода. Основными этапами создания модели с помощью конструктора являются следующие:

– создание рабочей области Azure;
– создание конвейера;

– импорт данных;
– подготовка данных;
– обучение модели машинного обучения;
– оценка модели машинного обучения;
– развертывания модели в виде конечного продукта прогнозирования в реальном времени.

Этап 1. Создание рабочей области. Для применения конструктора сначала нужна рабочая область Машинного обучения Azure. Рабочая область
– это ресурс верхнего уровня для Машинного обучения Azure, который обеспечивает централизованное расположение для работы со всеми артефактами, созданными в Машинном обучении Azure .

Этап 2. Создание конвейера. Конвейеры Машинного обучения Azure объединяют несколько этапов машинного обучения и обработки данных в одном ресурсе. Конвейеры позволяют организовывать, администрировать и повторно использовать сложные рабочие процессы машинного обучения с несколькими проектами и пользователями.

Применив Easy-to-use prebuilt modules (Удобные готовые модули), в верхней части полотна выбираем имя конвейера по умолчанию Pipeline-Created-on и переименовываем его.

Устанавливаем целевой объект вычислений по умолчанию. Конвейер выполняется с целевым объектом вычислений, который является вычислительным ресурсом, подключенным к рабочей области. После создания целевого объекта вычислений его можно повторно использовать приследующих запусках. Для всего конвейера можно задать Целевой объект вычислений по умолчанию, что позволит каждому модулю использовать одини тот же целевой объект вычислений по умолчанию. Однако, целевые объектывычислений можно задать конкретно для каждого модуля. Для этого необходимо выполнить следующие действия:

1. Рядом с именем конвейера выбираем значок «Шестеренки» в верхней части холста, чтобы открыть область «Параметры».
2. В области «Параметры» справа от полотна выбираем целевой объект вычислений. Конструктор может выполнять учебные эксперименты только с целевыми объектами вычислительной среды и вычислительных операций

Машинного обучения Azure, а другие целевые объекты вычислений не показываются.

3. Выбираем или создаем имя вычислительного ресурса и нажимаем «Сохранить». Создание вычислительного ресурса занимает около пяти минут. После создания ресурса его можно повторно использовать, что экономитвремя при последующих запусках.

Таким образом, среда готова для работы с конструктором.

2.2 Анализ исходных данных и их предварительная обработка

Для обучения и тестирования модели будем использовать KDD Cup Data set. Это набор данных, который используется при тестировании инструментов для интеллектуального анализа данных. Эта база данных содержит стандартный набор данных для аудита, который включает широкий спектр вторжений, смоделированных в реальной сетевой среде.

Программное обеспечение для обнаружения сетевых вторжений защищает компьютерную сеть от неавторизованных пользователей, включая, возможно, инсайдеров. Задача обучения детектора вторжений состоит в том, чтобы построить прогностическую модель (то есть классификатор), способную различать «плохие» соединения, называемые вторжениями или атаками, и «хорошие» нормальные соединения.

Необработанные обучающие данные составляли около четырех гигабайт сжатых двоичных данных дампа TCP за семь недель сетевого трафика. Это было обработано примерно в пять миллионов записей о подключении. Точно так же за две недели тестовых данных было получено около двух миллионов записей о соединениях.

Соединение — это последовательность пакетов TCP, которые начинаются и заканчиваются в определенные моменты времени, между которыми данные передаются от исходного IP-адреса к целевому IP-адресу по некоторому четко определенному протоколу. Каждое соединение помечается как обычное или как атака с одним конкретным типом атаки. Каждая запись о подключении состоит примерно из 100 байт.

Атаки делятся на четыре основные категории:

- Denial of Service (DOS): отказ в обслуживании, например, синхронный флуд;
- Remote to Local (R2L): несанкционированный доступ с удаленной машины, например, угадывание пароля;
- User to Root (U2R): несанкционированный доступ к привилегиям локального суперпользователя (root), например, различные атаки на переполнение буфера;
- Probe (зондирование): наблюдение и другое зондирование, например сканирование портов.

Важно отметить, что тестовые данные не имеют того же распределения вероятностей, что и обучающие данные, и включают определенные типы атак, которых нет в обучающих данных. Это делает задачу более реалистичной. Некоторые эксперты по вторжению полагают, что большинство новых атак являются вариантами известных атак, и «сигнатуры» известных атак может быть достаточно для обнаружения новых вариантов. Наборы данных содержат в общей сложности 24 обучающих типа атак, с дополнительными 14 типами только в тестовых данных

Полученные характеристики

Stolfo et al. определены функции более высокого уровня, которые помогают отличать обычные соединения от атак. Есть несколько категорий производных функций.

Функции «того же хоста» проверяют только соединения за последние две секунды, которые имеют тот же целевой хост, что и текущее соединение,и вычисляют статистику, относящуюся к поведению протокола, сервису и т.д.

Аналогичные функции «той же службы» проверяют только соединения за последние две секунды, которые имеют ту же службу, что и текущее соединение.

Функции «Один и тот же хост» и «та же служба» вместе называются функциями трафика, зависящего от времени, в записях о подключении.

Некоторые зондирующие атаки сканируют хосты (или порты) с использованием гораздо большего временного интервала, чем две секунды, например, один раз в минуту. Таким образом, записи о подключениях также были отсортированы по целевому хосту, а функции были созданы с использованием окна из 100 подключений к одному и тому же хосту вместо временного окна. Это дает набор так называемых характеристик трафика на основе хоста.

В отличие от большинства DOS и зондирующих атак, похоже, нет последовательных шаблонов, которые часто встречаются в записях об атаках R2L и U2R. Это связано с тем, что DOS и зондирующие атаки включают множество подключений к некоторым хостам за очень короткий период времени, но атаки R2L и U2R встроены в части данных пакетов и обычно включают только одно соединение.

Полезные алгоритмы для автоматического анализа неструктурированных данных в пакетах - открытый вопрос исследования. Stolfo et al. использовали знания предметной области для добавления функций, которые выявляют подозрительное поведение в частях данных, например количество неудачных попыток входа в систему. Эти функции называются функциями контента.

Полный список функций, определенных для записей о подключении, приведен в трех таблицах ниже.

Набор данных представляет собой таблицу, имеющую 43 столбцов и 125973 строки.

Столбцы обозначают:

Таблица 2.1 – Основные характеристики отдельных TCP-соединений.

Название функции	Описание	Тип
Duration	длина (количество секунд)соединения	непрерывный
Protocol_type	тип протокола, например tcp, udp и т.д.	дискретный

Service	сетевой сервис в пункте назначения,например http, telnet и т. д.	дискретный
src_bytes	количество байтов данных от источника до места назначения	непрерывный
dst_bytes	количество байтов данных от местаназначения до источника	непрерывный
Flag	нормальный или ошибочный статуссоединения	дискретный
Land	1, если соединение осуществляется от / к одному и тому же хосту / порту; 0иначе	дискретный
wrong_ fragment	количество `` неправильных "фрагментов	непрерывный
Urgent	количество срочных пакетов	непрерывный

Таблица 2.2 – Функции контента в рамках соединения, предложенные знанием предметной области.

Название функции	Описание	Тип
Hot	количество `` горячих "индикаторов	непрерывный
num_failed_logins	количество неудачных попыток входа в систему	непрерывный
logged_in	1 при успешном входе всистему; 0 иначе	дискретный
num_compromised	количество `` скомпрометированных " условий	непрерывный
root_shell	1, если получена корневаяоболочка; 0 иначе	дискретный
su_attempted	1 при попытке выполнения команды `` su root "; 0 иначе	дискретный
num_root	количество `` корневых "доступов	непрерывный
num_file_creations	количество операций созданияфайлов	непрерывный
num_shells	количество приглашенийоболочки	непрерывный

num_access_files	количество операций над файлами контроля доступа	непрерывный
num_outbound_cmds	количество исходящих командв сеансе ftp	непрерывный
is_hot_login	1, если логин входит в `` горячий '' список; 0 иначе	дискретный
is_guest_login	1, если логин являетсягостевым; 0 иначе	дискретный

Таблица 2.3 – Характеристики трафика, рассчитанные с использованием двухсекундного временного окна.

Название функции	Описание	Тип
Count	количество подключений к томуже хосту, что и текущее подключение, за последние две секунды	непрерывный
	Примечание. Следующие функции относятся к этим соединениям с одними тем же хостом.	
serror_rate	% соединений с ошибками SYN	непрерывный
rerror_rate	% соединений с ошибками REJ	непрерывный
same_srv_rate	% подключений к одному сервису	непрерывный
diff_srv_rate	% подключений к разнымсервисам	непрерывный
srv_count	количество подключений к той жеслужбе, что и текущее подключение, за последние две секунды	непрерывный
	Примечание. Следующие функции относятся к этим соединениям с однимсервисом.	
srv_serror_rate	% соединений с ошибками SYN	непрерывный
srv_rerror_rate	% соединений с ошибками REJ	непрерывный
srv_diff_host_rate	% подключений к разным хостам	непрерывный

Есть два набор данных: network_intrusion_detection – будем использовать для обучения и network_intrusion_detection_test – будем использовать для тестирования.

Для загрузки и предварительной обработки данных воспользуемся модулями Конструктора:

Import Data - загружает данные из внешних источников в сети; из различных форм облачного хранилища в Azure, таких как таблицы, большие двоичные объекты и базы данных SQL.

Edit Medadata - редактирует метаданные, связанные со столбцами в наборе данных.

Convert to Indicator Values - преобразует категориальные значения в столбцах в значения индикаторов. Настройки модуля для работы с нашим набором данных представлены на рис.2.2а.

Select Columns in Dataset- выбирает столбцы для включения или исключения из набора данных в операции. Настройки модуля для работы представлены на рисунке 2.2 б.

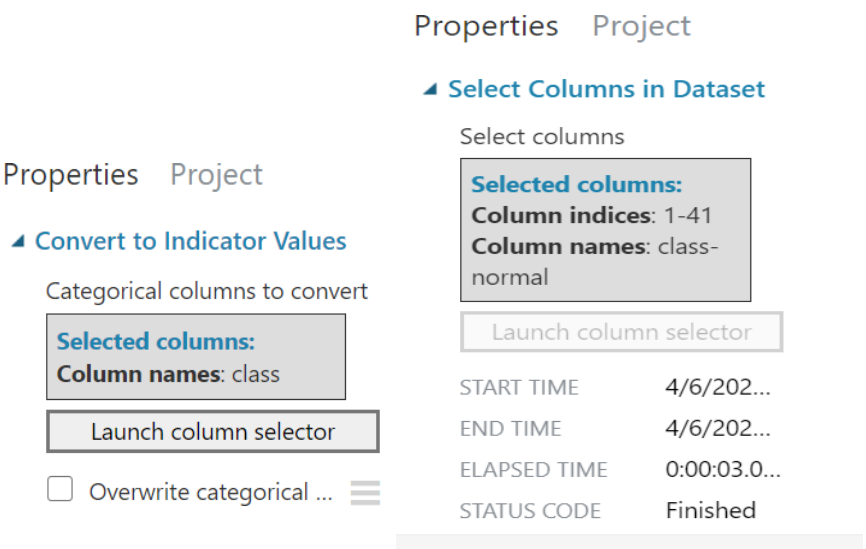

Рисунок 2.2 – Настройки модулей а) Convert to Indicator Values; б) Select Columns in Dataset

В результате модель в рабочем поле после загрузки данных будет выглядеть, как показано на рис. 2.3.

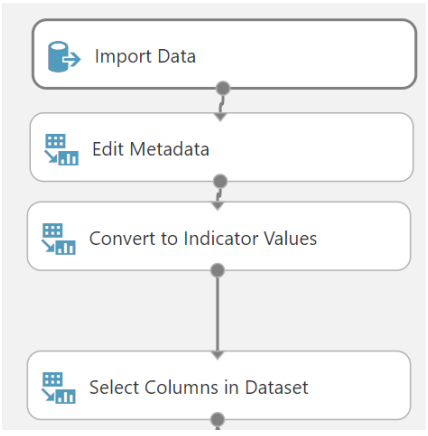

Рисунок 2.3 – Модель загрузки и предварительной обработки данных

Общий вид загруженных данных можно визуализировать (рис.2.4)

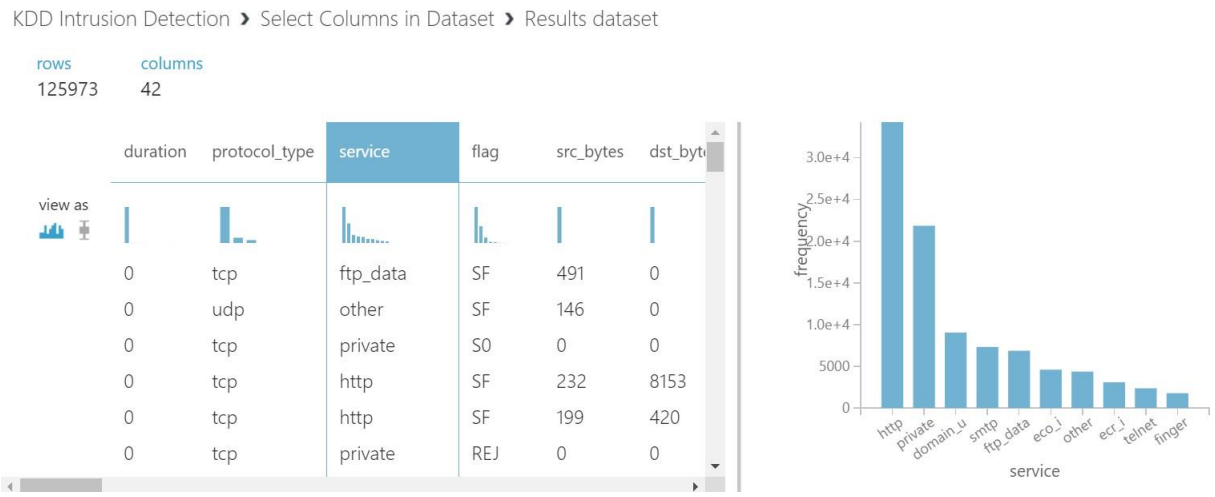

Рисунок 2.4 – Визуализация загруженных и обработанных данныхТаким образом, данные подготовлены для проведения обучения.

2.3 Разработка и обучение модели

Конструктор Машинного обучения Azure имеет целый ряд модулей двухклассовой классификации, которые могут быть использованы для определения аномалий.

Будем задействовать модули:

Двухклассовый усредняющий персептрон (Two-Class Averaged Perceptron) - Создает усредненную модель бинарной классификации персептроном.

Two-Class Bayes Point Machine - Создает модель двоичной классификации байесовской точечной машины.

Two-Class Boosted Decision Tree - Создает двоичный классификатор с использованием алгоритма усиленного дерева решений.

Two-Class Decision Forest - Создает двухклассовую модель классификации с использованием алгоритма леса решений.

Two-Class Support Vector Machine - Создает модель двоичной классификации с использованием алгоритма машины опорных векторов.

Каждый из этих модулей должен быть обучен и необходимо также оценить качество выявления аномалий.

Обучение модели осуществляется с помощью модуля Train Model (обучение модели). Перемещаем его на полотно эксперимента. Соединяем выходы модулей классификации с левым входом модуля Train Model (Обучение модели) (например, как показано на рис.2.5), а затем подсоединяемвыход (левый порт) модуля Split Data (Разделение данных) к правому входу модуля Train Model (Обучение модели).

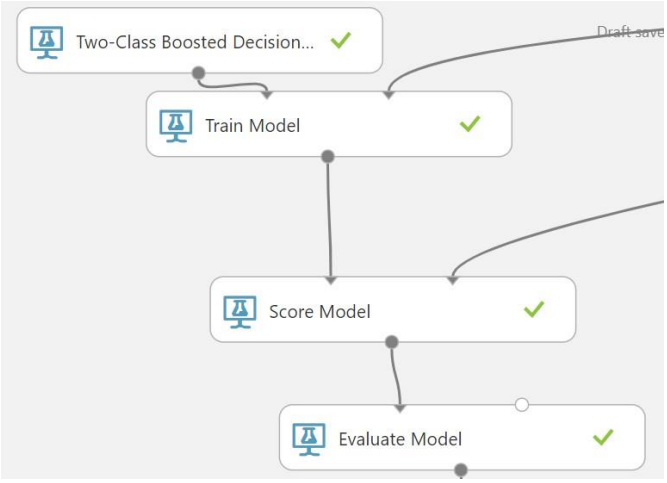

Рисунок 2.5 – Пример подключения модуля Обучения модели и разделения данных

Модуль Evaluate Model оценивает результаты классификации со стандартными метриками.

Поскольку мы хотим исследовать несколько методов, то целесообразно использовать еще некоторые методы для объединения информации:

Execute R Script - Выполняет сценарий R из эксперимента Студии машинного обучения Azure (классический). Общий вид модуля Execute R Script представлен на рис.2.6. Код сценария для модуля Execute R Script представлен на листинге рис. 2.6.

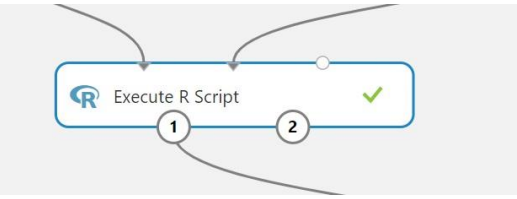

Рисунок 2.6 – Листинг Общий вид модуля Execute R Script

Add Rows - добавляет набор строк из входного набора данных в конец другого набора данных. Общий вид модуля Add Rows.

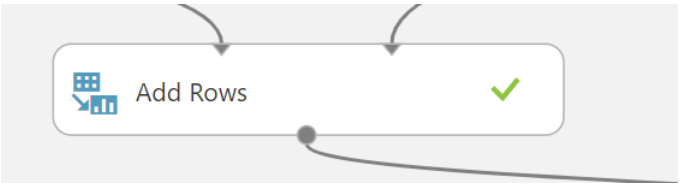

Рисунок 2.6 – Общий вид модуля Add Rows

Теперь необходимо проверить качество результатов. Выбираем модуль Evaluate Model (Анализ модели) и перетаскиваем его на холст эксперимента, а потом соединяем выход модуля Score Model (Оценка модели) с левым входом модуля Evaluate Model (Анализ модели).

Таким образом, окончательная схема модели для эксперимента выглядит так, как подано на рис.2.7.

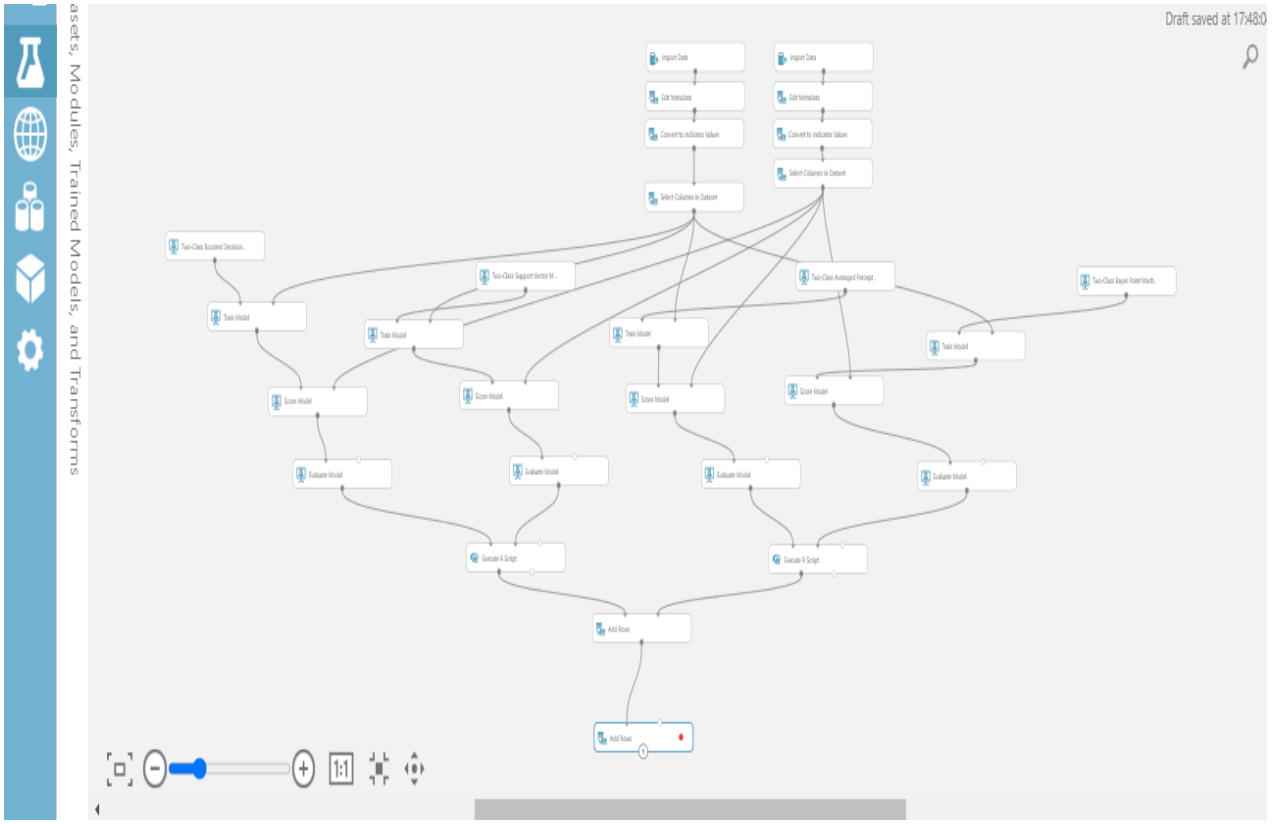

Рисунок 2.7 – Общий вид полной модели

Основными особенностями общей модели являются: использование двух dataset – один для обучения, а другой для оценки качества;объединение результатов с показателями качества поиска аномалий длятого, чтобы удобнее было производить сравнение.

3.ОЦЕНКА КАЧЕСТВА ОБУЧЕНИЯ И ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ КЛАССИФИКАЦИИ РАЗНЫМИ МЕТОДАМИ

3.1 Показатели качества классификации при обнаружении аномалий и вторжений

После создания модели необходимо оценить качество ее работы. Для оценки качества модели используется модуль Evaluate Model в Конструкторе Машинного обучения Azure. Этот модуль вычисляет набор метрик оценки, стандартных для двухклассовой классификации.

После проведения классификации возможно получение четырех видов результатов:

TP (от англ. True Positive – истинно положительный), TN (от англ. True Negative – истинно отрицательный),FP (от англ. False Positive – ложно положительный), FN (от англ. False Negative – ложно отрицательный).

Эти результаты можно представить в виде матрицы ошибок в таблице 2,где yy' – ответ алгоритма на объекте, а yy – истинная метка класса на этом объекте.

Таблица 3.1 – Матрица ошибок

	y=1	y=0
y'=1	True Positive (TP)	False Positive (FP)
y'=0	False Negative (FN)	True Negative (TN)

Матрица ошибок демонстрирует такие варианты, когда и прогнозируемое, и фактическое значение равно 1 (т.н. истинноположительные значения) в верхнем левом углу, а также варианты, когда и прогнозируемое, и фактическое значение равны 0 (истинноотрицательные значения) в нижнем правом углу. В других ячейках показаны варианты, когда прогнозируемые фактические значения отличаются (ложноположительные и ложноотрицательные значения). Ячейки в матрице могут быть окрашены таким образом, что чем больше вариантов представлено в ячейке, тем более интенсивным будет цвет. Таким образом, можно определить модель, которая формирует точные прогнозы для всех классов. Для этого нужно найти диагональ, проходящую по интенсивно окрашенным ячейкам от левого верхнего угла вправо (иными словами, в ячейках, где прогнозируемые значения соответствуют фактическим значениям).

Аккуратность (Accuracy) измеряет качество модели классификации как отношение истинных результатов к общему количеству случаев.

Точность (precision) показывает долю объектов, названных классификатором положительными и при этом действительно являющимися положительными (3.1):

$$precision = \frac{TP}{TP+FP} \quad (3.1)$$

Полнота (recall) показывает долю правильно помеченных (выявленных) положительных объектов среди всех объектов положительного класса (3.2):

$$recall = \frac{TP}{TP+FN} \quad (3.2)$$

Точность чувствительна к распределению данных, в то время как полнота – нет. Полнота не отражает, сколько объектов помечены как положительные неверно, а точность не дает никакой информации о том, сколько положительных объектов помечены неправильно.

F-мера (F-score, F_β) сочетает в себе вышеупомянутые две метрики – среднее гармоническое точности и полноты.

F-мера достигает максимума при полноте и точности, равным единице, и близка к нулю, если один из аргументов близок к нулю.

ROC-кривая или кривая ошибок – график, позволяющий оценить качество классификации (рис.3.1), который отображает соотношение между чувствительностью (TPR, True Positive Rate) алгоритма и долей из объектов отрицательного класса, которые алгоритм предсказал неверно (FPR, False Positive Rate) при варьировании порога решающего правила (3.4):

$$FPR = \frac{FP}{FP+TN} \quad (3.4)$$

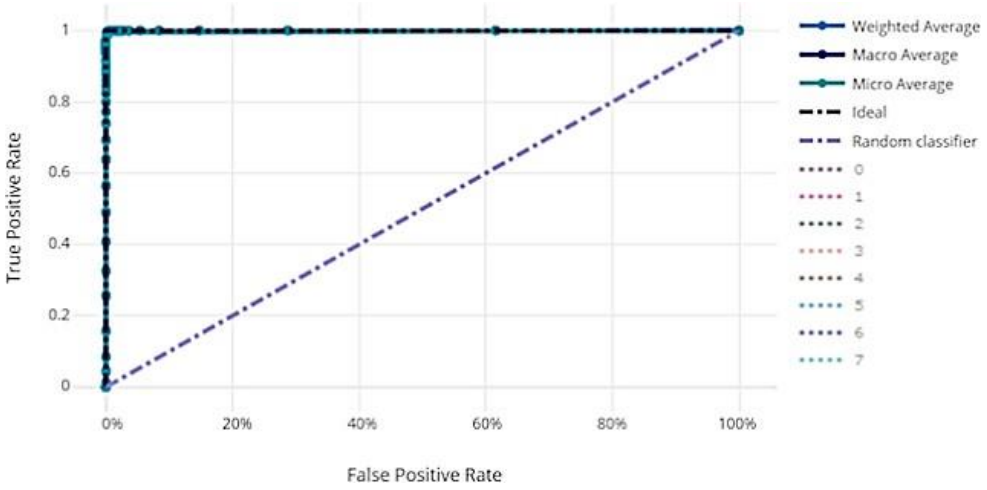

Рисунок 3.1 – Общий вид идеальной кривой ROC

Количественную интерпретацию ROC-кривой дает показатель AUC- ROC. В идеальном случае, когда классификатор не делает ошибок (FPR = 0, TPR = 1), получается площадь под кривой, равная 1; если классификатор

«гадает», то AUC-ROC будет стремиться к 0,5, так как классификатор будет выдавать одинаковое количество TP и FP. Площадь под кривой в этом случае показывает качество алгоритма (больше – лучше); кроме этого, важной является крутизна самой кривой (желательно максимизировать TPR, минимизируя FPR), а значит, она в идеале должна стремиться к точке (0,1).

Критерий AUC-ROC устойчив к несбалансированным классам и может быть интерпретирован как вероятность того, что случайно выбранный положительный объект будет ранжирован классификатором выше (будет иметь более высокую вероятность быть положительным), чем случайно выбранный отрицательный объект.

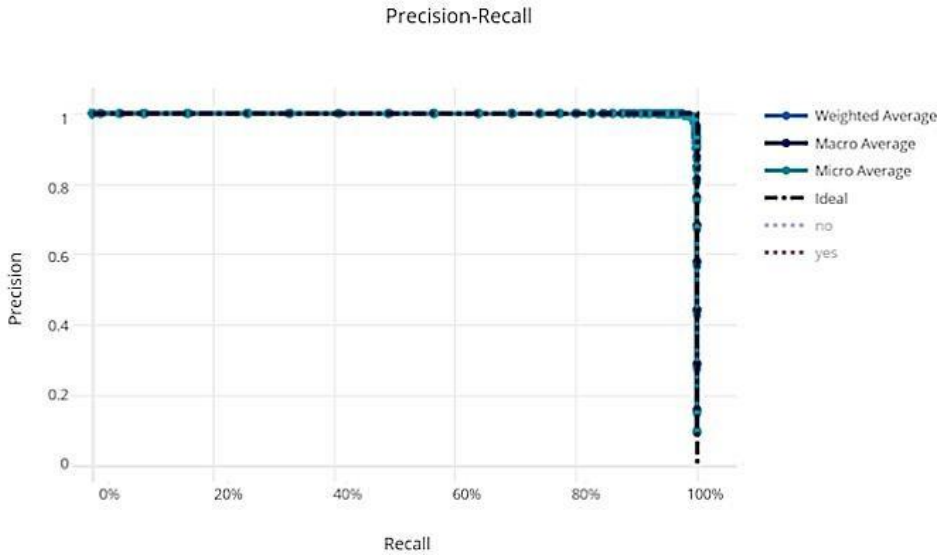

Рисунок 3.2 – Общий вид идеальной кривой PR

Помимо ROC-кривой существует PR-кривая (от англ. Precision-Recall Curve), показывающая отношение точности (3.1) от полноты (3.2). Соответственно, количественный показатель в данном случае такой же – площадь по кривой – AUC-PR (больше – лучше). В идеальном случае кривая должна стремиться к точке (1,1), где классификатор получает только истинно положительные результаты, без отрицательных. PR-анализ также применяетсяна несбалансированных данных (рис.3.2).

Значение средних потерь (Average log loss) — это единичная оценка, которая используется для выражения штрафа за неправильные результаты. Он рассчитывается как разница между двумя распределениями вероятностей - истинным и модельным.

Значение потерь обучения (Training log loss) — это единичная оценка, которая показывает преимущество классификатора над случайным предсказанием. Значение потерь обучения измеряет неопределенность вашей модели, сравнивая вероятности, которые она выводит, с известными значениями (истинность) в метках. Необходимо минимизировать Значение потерь обучения для модели в целом.

3.2 Исследование алгоритмов обнаружении аномалий и торжений

Основная идея этого исследования заключается в том, чтобы сравнить между собой показатели качества алгоритмов двухклассовой классификации Конструктора машинного обучения при решении задачи обнаружения аномалий и вторжений.

Исследования проведены на модели, разработанной в разделе 2 с использованием показателей, описанных в подразделе 3.1.

Общий вид эксперимента в Конструкторе Студии машинного обучения Azure показан на рис. 3.3.

Для оценки качества, запускаем эксперимент на выполнение. После выполнения всех модулей проверяем исходные данные модуля анализа. Чтобы проверить выходные данные модуля Evaluate Model (анализ модели), необходимо нажать порт вывода и выбрать элемент Visualize (Визуализировать).

Также можно:

- Сохранить результаты в виде набора данных для упрощения анализа с помощью других инструментов.

- Создать визуализации в интерфейсе Studio (классический).

Если вы подключите наборы данных к обоим входам Evaluate Model, результаты будут содержать метрики для обоих наборов данных или обеих моделей. Модель или данные, прикрепленные к левому порту, сначала представляются в отчете, за ними следуют метрики для набора данных или

модели, прикрепленные к правому порту.

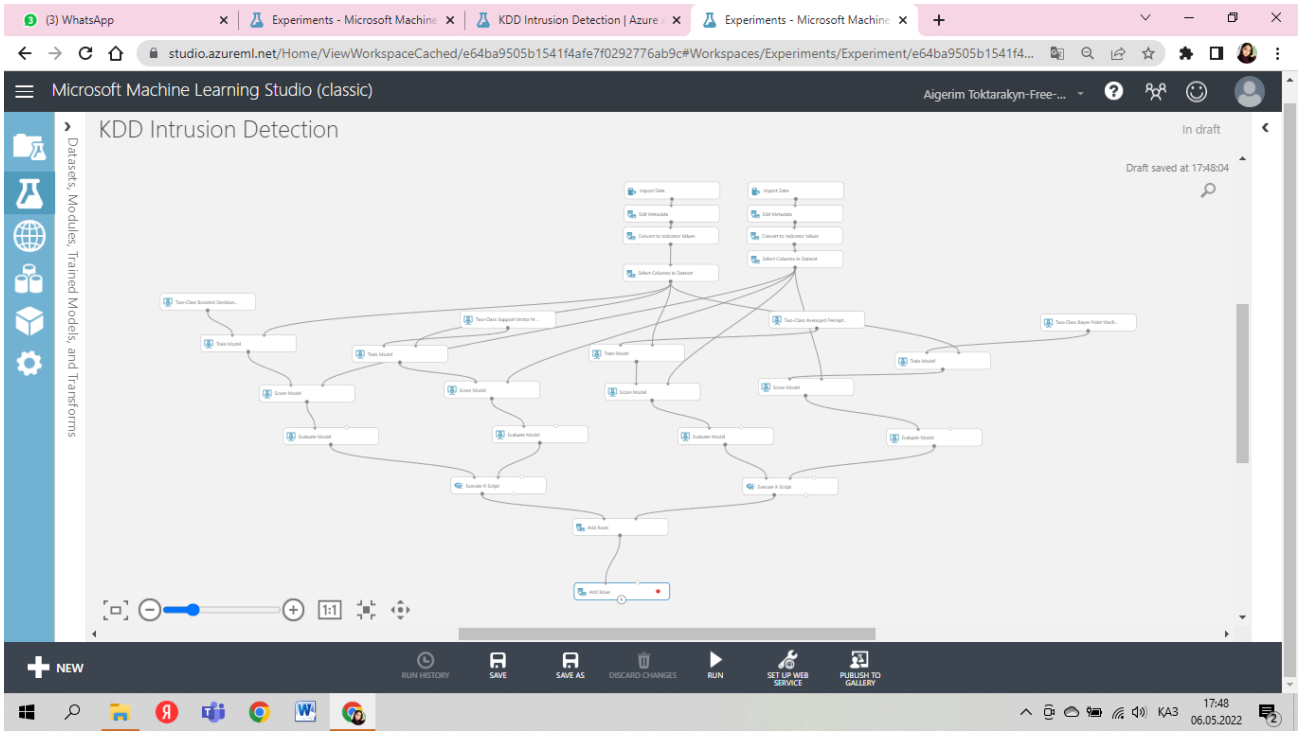

Рисунок 3.3 – Общий вид эксперимента в Конструкторе Студии машинного обучения Azure

Рассмотрим промежуточные результаты, полученные для Двоичного классификатора с использованием алгоритма усиленного дерева решений (Two-Class Boosted Decision Tree). На рис.3.4 показаны результаты оценки качества для этого алгоритма.

True Positive	False Negative	Accuracy	Precision	Threshold	AUC
9429	282	0.812	0.704	0.5	0.863
False Positive	True Negative	Recall	F1 Score		
3958	8875	0.971	0.816		
Positive Label	Negative Label				
1	0				

Рисунок 3.4 – Результаты оценки качества Двоичного классификатора с использованием алгоритма усиленного дерева решений

На рис.3.5 показана кривая ROC для алгоритма Двоичного классификатора с использованием алгоритма усиленного дерева решений.

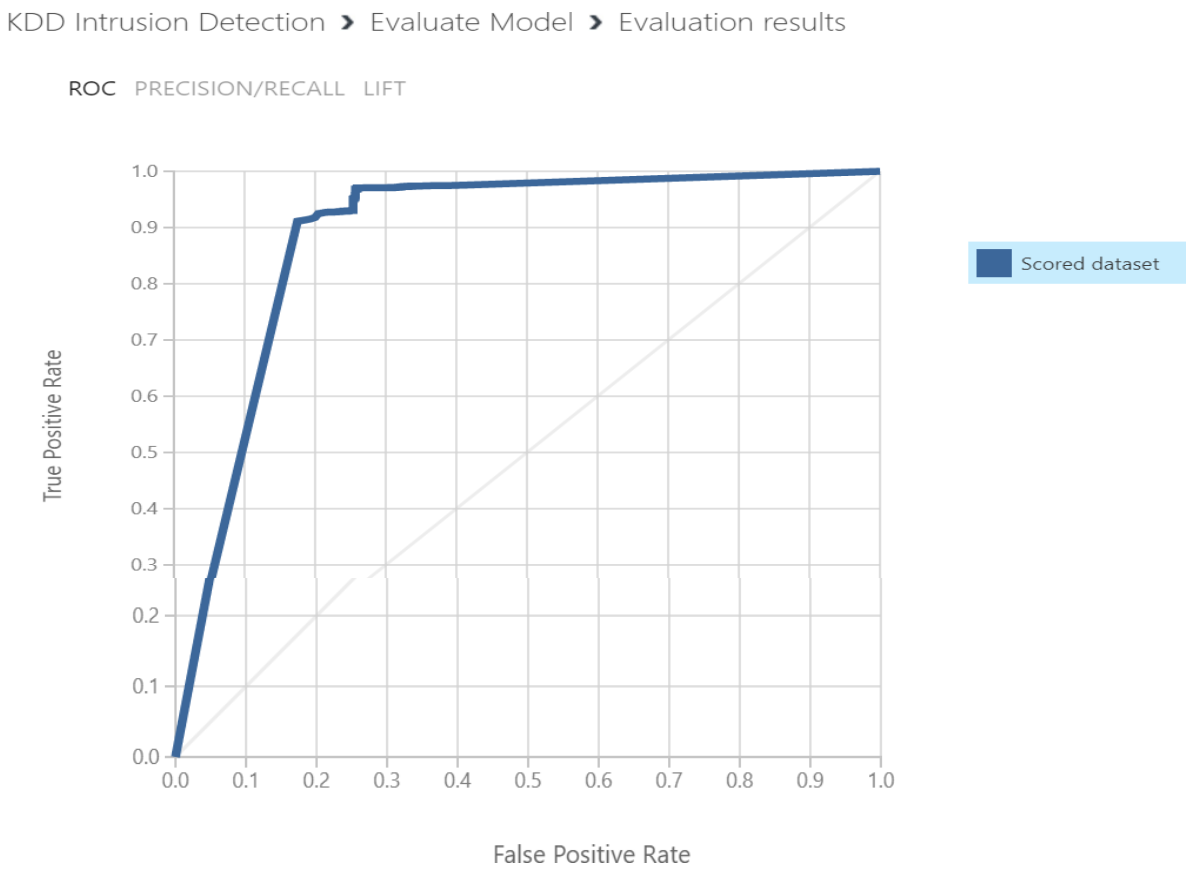

Рисунок 3.5 – Кривая ROC для алгоритма Двоичного классификатора с использованием алгоритма усиленного дерева решений

Обратите внимание на кривую ROC и на ползунок "Порог" на рис.3.5. Сопоставление двух метрик друг с другом для каждого возможного порогового значения в диапазоне между 0 и 1 формирует кривую ROC. Изменяя значения порога, можно подрегулировать и кривую ROC. В идеальной модели кривая уходит вверх слева по верхнему краю, охватывая всю область диаграммы. Чем больше область под кривой (может быть любымзначением от 0 до 1), тем выше производительность модели. Это показывает метрика AUC, которая приведена вместе с другими метриками на рис. 3.6.

Если метрика AUC для вашей модели имеет большее значение, чем значение для модели бинарной классификации (0,5), то в этом случае модель более эффективна, чем угадывание. Чем ближе AUC к 1 тем лучше модель распознает атаки и вторжения.

Для удобства сравнения качества алгоритмов результаты были сведены в единую таблицу (рисунок 3.6).

KDD Intrusion Detection › Add Rows › Results dataset

rows 10 columns 8

Algorithm	Accuracy	Precision	Recall	F.Score	AUC	Average.Log.Loss	Training.Log.Loss
Two-Class Boosted Decision Tree	0.811923	0.70434	0.970961	0.816434	0.954441	1.493383	-118.48189
Two-Class Support Vector Machine	0.735983	0.632368	0.924622	0.751066	0.90283	0.789937	-15.56772
Two-Class Averaged Perceptron	0.754303	0.651116	0.925548	0.764448	0.78888	1.232236	-80.276037
Two-Class Bayes Point Machine	0.753682	0.650434	0.925651	0.764013	0.794697	1.798601	-163.13518

Рисунок 3.6 - Обобщенная таблица оценки качества обнаружения аномалий различными алгоритмами

Анализ таблицы на рис. 3.6 показывает, что:

Все рассмотренные алгоритмы двухклассовой классификации обнаруживают аномалии и вторжения в большей или меньшей степени, однако выделить метод, который бы полностью справлялся с задачей нельзя.

Наилучшие свойства по обнаружению показал метод Двоичного классификатора с использованием алгоритма усиленного дерева решений (Two-Class Boosted Decision Tree).

Наихудшие свойства по обнаружению показал метод Двуклассовой логистической регрессии (Two-Class Logistic Regression).

ЗАКЛЮЧЕНИЕ

В дипломной работе выполнено исследование методов классификации Студии машинного обучения Microsoft Azure для решения задачи обнаружения вторжений.

Проведенный анализ показал, что тема работы по обеспечения безопасности СС является актуальной.

Анализ существующих методик обнаружения аномалий и вторжений выявил дополнительные возможности облачной среды Azure по моделированию методов машинного обучения.

Разработанная технология обнаружения аномалий и вторжений в СС использует методы машинного обучения, которые предоставляет Студия машинного обучения Azure.

Модель конвейера машинного обучения построена на основе методов классификации Конструктора машинного обучения Azure.

Оценка качества обучения и исследование эффективности классификации разными методами произведена с помощью показателей: аккуратность (accuracy), точность (precision), полнота (recall), F-меры, ROC-кривой.

Наилучшие результаты показал метод Двоичного классификатора с использованием алгоритма усиленного дерева решений (Two-Class Boosted Decision Tree).

В той или иной степени все рассмотренные алгоритмы двухклассовой классификации обнаруживают аномалии и вторжения, однако качество обнаружения оставляет желать лучшего.

Поэтому целесообразно использовать гибридные подходы, поскольку они могут обеспечить лучшие результаты и преодолевают недостаток одного подхода по сравнению с другим.

В работе использованы методы визуального математического моделирования облачной среды Microsoft Azure, методы классификации машинного обучения, методы программирования.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. "Использование визуальных средств для создания моделей машинного обучения в Машинном обучении Azure" (https://docs.microsoft.com/ru-ru/learn/paths/create-no-code-predictive-models-azure-machine-learning/);
2. Статья "Применение методов машинного обучения в задачах обнаружения вторжения" С.С.ВОЛКОВ,И.И.КУРОЧКИН;
3. Статья " Обнаружение сетевого вторжения с помощью Наблюдателя за сетями Azure и средств с открытым исходным кодом"(https://docs.microsoft.com/ru-ru/azure/network-watcher/network-watcher-intrusion-detection-open-source-tools) ,
4. Статья "Как самому разработать систему обнаружения компьютерных атак на основе машинного обучения" (https://habr.com/ru/post/538296/) ,
5. Статья " РАЗРАБОТКА ПРОГРАММНОГО СЕРВИСА ДЛЯ АВТОМАТИЗАЦИИ ВЗАИМОДЕЙСТВИЯ ПО СЕТИ" Белов Н.В.,Мезенцева Е.М.
6. Статья “Azure Machine Learning Studio append rows to dataset”https://stackoverflow.com/questions/52055933/azure-machine-learning-studio-append-rows-to-dataset
7. Статья “ Cost-based Modeling and Evaluation for Data Mining With Application to Fraud and Intrusion Detection: Results from the JAM Project by Salvatore J. Stolfo, Wei Fan, Wenke Lee, Andreas Prodromidis, and Philip K. Chan.” https://kdd.ics.uci.edu/databases/kddcup99/task.html
8. Статья “Обнаружение аномалий и вторжений в космических сетях связи с использованием методов машинного обучения”
9. https://ml.azure.com/visualinterface/authoring/Normal/9f99e2e0-94e9-4c24-89e0-ec5a809804bd?wsid=/subscriptions/9b3e40d5-6308-42f8-a402-dc59a08d3925/resourcegroups/Klass/workspaces/AzureMachine01&tid=49cc33db-453b-4ada-aaee-63c5dcd64f9c
10. https://kdd.ics.uci.edu/databases/kddcup99/task.html
11. file:///C:/Users/tokta/Downloads/Intrusion%20Detection%20Framework%20using%20Correlation%20based%20Feature%20Selection%20over%20Cloud%20SANJEET%20CHOUDHARY.pdf
12. https://ict.az/uploads/konfrans/info_sec/RS02_DOS-ATTACKS-DETECTION-USING-AN-ENSEMBLE-OF-CLASSIFIERS.pdf

СПИСОК ИСПОЛЬЗОВАННЫХ СОКРАЩЕНИЙ

AUC Area Under Curve – (площадь под кривой) показатель качества классификации
DOS Disk Operating System – дисковая операционная система
KDD Knowledge Discovery in Databases — обнаружение знаний в базах данных
NL Network Layer - Сетевой уровень
ROC receiver operating characteristic - рабочая характеристика приёмника
TCP Transmission Control Protocol – протокол управления передачей
TL Transport Layder – Транспортный уровень
ИБ информационный безопасность
ИИ искусственный интеллект
СС системы связи
ЭВМ электронная вычислительная машина
SVM upport vector machine – метод опорных векторов

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
СӘТБАЕВ УНИВЕРСИТЕТІ

ОТЗЫВ

НАУЧНОГО РУКОВОДИТЕЛЯ

На дипломную работу

Тоқтарақын Айгерім Ержанқызы

5В074600 – Космическая техника и технологии

Тема: «Разработка оптимизации обнаружекния вторжений в сети связи с использованием студии машинного обучения Azure»

Студентом разработана технология обнаружения вторжений на основе возможностей Конструктора машинного обучения Azure. Проведено сравнение качества обнаружения алгоритмами классификации. Также, в работе демонстрируется, как методы, разработанные для обнаружения атак, могут быть обобщены и применены к важной области обнаружения вторжений в сетевые информационные системы.

Высокая практическая ценность исследования дополняется лаконичным изложением материала и удачно подобранными примерами, что должно вызвать наибольший интерес к работе у специалистов из сферы информационной безопасности. Дипломант показал, что умеет работать с программой и литературой.

Дипломная работа соответствует всем критериям высшего учебного заведения и научному направлению информационных систем безопасности,а дипломант, Тоқтарақын Айгерім Ержанқызы оценивается на 94 баллов и достоина степени бакалавра специальности 5В074600 «Космическая техника и технологии».

Научный руководитель
М.т.н.,лектор кафедры «ЭТиКТ»
Боранбаева А.Т.

«27» 05 2022 г.

РЕЦЕНЗИЯ
на дипломную работу Тоқтарақын А.Е.
на тему: «Разработка оптимизации обнаружения вторжений в сети связи с использованием студии машинного обучения Azure»

Целью дипломной работы Тоқтарақын А.Е. является исследование методов классификации Студии машинного обучения Microsoft Azure для решения задачи обнаружения аномалий и вторжений.

Под информационной безопасностью понимают защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры. Современное развитие мировой экономики характеризуется все большей зависимостью рынка от значительного объема информационных потоков. Таким образом, в рецензируемой дипломной работе рассматривается достаточно актуальная и интересная задача, связанная с защитой потоков данных и обеспечением информационной безопасности их обработки и передачи.

В данной дипломной работе выполнены работы по анализу методов обеспечения безопасности, по исследованию методов двухклассовой классификации Студии машинного обучения Microsoft Azure для решения задачи обнаружения вторжений в сети связи, по разработке и обучению модели машинного обучения на основе методов классификации, по разработке технологии обнаружения вторжений на основе возможностей Конструктора машинного обучения Azure, проведены работы по сравнению качества обнаружения алгоритмами классификации, работы по разработке рекомендации по применению технологии для обнаружения аномалий и вторжений.

Проведенные работы студентом позволят повысить информационную безопасность сетей связи от несанкционированных вторжений за счет применения разработанной технологии на основе возможностей облачной среды Microsoft Azure.

В целом дипломная работа выполнена на достаточно высоком уровне, соблюдены все требования к разработке информационных систем безопасности и к оформлению работы. В тексте работы наблюдаются стилистические ошибки, которые не влияют на качество выполненного проекта.

Учитывая вышесказанное, считаю, что дипломная работа заслуживает высокой оценки 92 баллов и рекомендуется к защите.

Заведующий лабораторией
разработки космических систем
ДТОО «Институт космической
техники и технологий» С.А. Елубаев

«25» 05 2022 г.

Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Тоқтарақын Айгерім Ержанқызы

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: Разработка оптимизации обнаружения вторжений в сети связи с использованием студии машинного обучения Azure

Научный руководитель: Ерлан Таштай

Коэффициент Подобия 1: 0.3

Коэффициент Подобия 2: 0

Микропробелы: 0

Знаки из здругих алфавитов: 1

Интервалы: 0

Белые Знаки: 0

После проверки Отчета Подобия было сделано следующее заключение:

☑ Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.

☐ Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.

☐ Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.

☐ Обоснование:

27.05.2021

Дата

Заведующий кафедрой

Университеттің жүйе администраторы мен Академиялық мәселелер департаменті директорының ұқсастық есебіне талдау хаттамасы

Жүйе администраторы мен Академиялық мәселелер департаментінің директоры көрсетілген еңбекке қатысты дайындалған Плагиаттың алдын алу және анықтау жүйесінің толық ұқсастық есебімен танысқанын мәлімдейді:

Автор: Тоқтарақын Айгерім Ержанқызы

Тақырыбы: Разработка оптимизации обнаружения вторжений в сети связи с использованием студии машинного обучения Azure

Жетекшісі: Ерлан Таштай

1-ұқсастық коэффициенті (30): 0.3

2-ұқсастық коэффициенті (5): 0

Дәйексөз (35): 2.1

Әріптерді ауыстыру: 1

Аралықтар: 0

Шағын кеңістіктер: 0

Ақ белгілер: 0

Ұқсастық есебін талдай отырып, Жүйе администраторы мен Академиялық мәселелер департаментінің директоры келесі шешімдерді мәлімдейді :

☑ Ғылыми еңбекте табылған ұқсастықтар плагиат болып есептелмейді. Осыған байланысты жұмыс өз бетінше жазылған болып санала отырып, қорғауға жіберіледі.

☐ Осы жұмыстағы ұқсастықтар плагиат болып есептелмейді, бірақ олардың шамадан тыс көптігі еңбектің құндылығына және автордың ғылыми жұмысты өзі жазғанына қатысты күмән тудырады. Осыған байланысты ұқсастықтарды шектеу мақсатында жұмыс қайта өңдеуге жіберілсін.

☐ Еңбекте анықталған ұқсастықтар жосықсыз және плагиаттың белгілері болып саналады немесе мәтіндері қасақана бұрмаланып плагиат белгілері жасырылған. Осыған байланысты жұмыс қорғауға жіберілмейді.

Негіздеме:

27.05.2021
Күні

Кафедра меңгерушісі

Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Тоқтарақын Айгерім Ержанқызы

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: Разработка оптимизации обнаружения вторжений в сети связи с использованием студии машинного обучения Azure

Научный руководитель: Ерлан Таштай

Коэффициент Подобия 1: 0.3

Коэффициент Подобия 2: 0

Микропробелы: 0

Знаки из здругих алфавитов: 1

Интервалы: 0

Белые Знаки: 0

После проверки Отчета Подобия было сделано следующее заключение:

☑ Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.

☐ Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.

☐ Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.

☐ Обоснование:

27.05.2021
Дата

Марженова К
проверяющий эксперт