обучение, обещают значительно ускорить анализ сложных потоков данных. Системы, использующие методы машинного обучения, становятся всё более автономными. Нейроморфные процессоры, имитирующие работу человеческого мозга, позволят создавать устройства, которые смогут анализировать потоковые данные на аппаратном уровне. Это обеспечит минимальную задержку обработки и снижение энергозатрат.

Заключение. Искусственный интеллект и машинное обучение стали неотъемлемой частью анализа больших данных, особенно в задачах, требующих обработки потоков информации в реальном времени. Эти технологии позволяют быстро и точно выявлять аномалии, тренды и паттерны. Повышать производительность систем и снижать затраты. Создавать новые решения для сложных задач в таких областях, как финансы, здравоохранение, интернета вещей и безопасность. Однако остаются вызовы, связанные с высокими вычислительными требованиями, качеством данных и интерпретацией моделей. Тем не менее, дальнейшее развитие технологий, таких как квантовые вычисления и нейроморфные системы, открывает огромные перспективы для более эффективного использования искусственного интеллекта и машинного обучение.

ЛИТЕРАТУРА

1. Goodfellow I., Bengio Y., Courville A. Deep Learning. – MIT Press, 2016.

2. Chollet F. Deep Learning with Python. – Manning Publications, – 2021.

3. McKinsey & Company: "Big Data and AI: Future Trends", 2023.

4. Apache Kafka Documentation: – URL: https://kafka.apache.org/.

5. Apache Flink Documentation: – URL: https://flink.apache.org/.

УДК 004.9

Т.А. Раченко, доц.; А.В. Пеков, маг.
(ТГУ, г. Тольятти, Россия)

ИСПОЛЬЗОВАНИЕ КОМБИНИРОВАННЫХ КРИПТОГРАФИЧЕСКИХ СИСТЕМ В КОРПОРАТИВНЫХ СИСТЕМАХ ХРАНЕНИЯ ДАННЫХ

Проблема безопасности данных в корпоративных системах хранения представляет собой одну из наиболее острых тем в области информационных технологий. В условиях, когда объем обрабатываемых и хранимых данных постоянно растет, компании сталкиваются с

риском утечки конфиденциальной информации, угрозами со стороны киберпреступников и внутренняя угроза несанкционированного доступа сотрудников. Недостаточная защита данных может привести не только к финансовым потерям, но и к репутационным рискам, что ставит под сомнение доверие клиентов и партнеров.

Кроме того, корпоративные системы хранения часто используют облачные технологии, что добавляет новый уровень сложности в вопросах безопасности. Сложные системы хранения, которые интегрируют облачные и локальные решения, создают уязвимости, если адекватная защита и мониторинг не обеспечены. Актуальной задачей становится не только защита информации от внешних угроз, но и внедрение методов контроля доступа, шифрования и хранения данных.

Необходимость внедрения криптографических систем в корпоративные хранилища данных обусловлена растущими угрозами кибербезопасности и увеличением числа нарушений конфиденциальности. Шифрование данных создает дополнительный уровень защиты, предотвращая несанкционированный доступ и минимизируя риски утечки информации. Этот подход также поддерживает соответствие требованиям стандартов безопасности и защиты данных.

Для обеспечения высокого уровня безопасности и защиты данных в криптосистемах используется комплексно-комбинированный подход к шифрованию данных. Такие системы шифрования используют гибридные методы шифрования, достигая высокого уровня безопасности данных за счет интеграции симметричных и асимметричных алгоритмов. В такой системе данные сначала шифруются симметричным ключевым шифрованием, что обеспечивает скорость обработки, а затем ключ, используемый для этого шифрования, шифруется с помощью асимметричного алгоритма. Это сочетание позволяет эффективно использовать преимущества обоих видов шифрования, обеспечивая как безопасность, так и производительность. В качестве гибридных методов шифрования используются алгоритмы AES и RSA.

AES (Advanced Encryption Standard) – это симметричный алгоритм шифрования, который работает с фиксированным размером блока в 128 бит и поддерживает ключи длиной 128, 192 и 256 бит [0]. AES является одним из самых распространенных алгоритмов для защиты данных благодаря своей скорости и высокой устойчивости к атакам. Он использует несколько раундов выполнения операций замены, перестановки и математических преобразований, чтобы эффективно зашифровать и расшифровать данные. За счет симметричного ключа, тот же ключ используется как для шифрования, так и для расшифрования, что делает алгоритм особенно быстрым.

RSA (Rivest-Shamir-Adleman) – это асимметричный алгоритм шифрования, который зависит от сложности разложения больших простых чисел. В отличие от AES, RSA использует пару ключей: открытый и закрытый. Открытый ключ используется для шифрования данных, а закрытый – для их расшифровки [0].

Помимо этого, эффективным вариантом комбинированных систем шифрования является использование алгоритмов хеширования и сжатия данных в процессе шифрования. Прежде чем данные будут зашифрованы, они могут быть сначала сжаты, что делает процесс шифрования более эффективным, уменьшает объем обрабатываемой информации и ускоряет ее передачу. Хеширование также вводится на этапе аутентификации, когда создается уникальный хеш для каждого блока данных, что позволяет гарантировать целостность информации и защитить ее от изменения.

Наиболее подходящим алгоритмом хеширования является SHA-256. Данный алгоритм широко используется в различных приложениях безопасности. Его особенностями является работа в одном направлении и фиксированный размер результирующего блока.

Главной проблемой использования комбинированной криптографической системы является скорость обработки входного потока данных. При таком подходе каждому очередному потоку данных необходимо будет пройти несколько трудоёмких алгоритмов шифрования и хеширования. Для повышения скорости вычислительных процессов необходимо использовать параллельные технологии.

Следовательно, внедрение параллельных технологий в комбинированные криптографические системы хранения данных позволит значительно ускорить алгоритмы шифрования за счет одновременной обработки нескольких потоков данных, что особенно полезно в условиях больших объемов трафика или при работе с большими файлами.

Кроме того, использование параллельных методов повышает устойчивость систем к потенциальным атакам, как по времени, так и по ресурсам, обеспечивая дополнительные уровни безопасности [0].

Таким образом, внедрение комбинированных криптографических систем в корпоративные системы хранения данных позволяет повысить надёжность их работы, а также безопасность и целостность данных, соблюдая требования стандартов безопасности и защиты в управлении информации.

ЛИТЕРАТУРА

1. Бурькова, Е.В. Модели и алгоритмы защиты информационной системы персональных данных : учебное пособие / Е.В. Бурькова, А.А. Рычкова. – Оренбург : ОГУ, 2023. – 141 с. – URL:

https://e.lanbook.com/book/422789 (дата обращения: 24.12.2024).

2. Антоненко, С.В. Исследование совместного использования алгоритмов сжатия и шифрования данных / С.В. Антоненко, Р.Д. Сим // Человек. Общество. Инклюзия (Приложение). – 2023. – № S1-1. – С. 110–113.

3. Косимова Маржона Шакиржон Кизи. Параллельные и распределённые алгоритмы // EJMTCS. – 2024. – № 6. – URL: https://cyberleninka.ru/article/n/parallelnye-i-raspredelyonnye-algoritmy (дата обращения: 17.12.2024).

УДК 004.942

И.Н. Пожаркова, проф.
(ФГБОУ ВО СПСА ГПС МЧС России, г. Железногорск, Россия)

ПРОГНОЗИРОВАНИЕ ТРАЕКТОРИИ СВОБОДНОЙ СТРУИ НА ОСНОВЕ MLP И KAN МОДЕЛЕЙ

В работах [1, 2] предложена методика разработки нейросетевых моделей для расчета параметров свободных жидкостных струй значительных геометрических размеров, одной из прикладных областей применения которых является ликвидация и ограничение распространения пожара, защита строительных конструкций от теплового излучения, охлаждение технологического оборудования, в т.ч. наружных установок. Для организации гибкого реагирования на различные сценарии развития пожара подобные струи воды или пены формируются и направляются пожарными роботами – автоматическими устройствами, в состав которых входит рабочий орган (лафетный ствол), устройство программного управления и другие элементы [3].

Из-за возмущающих воздействий (например, ветровых нагрузок) на открытых пространствах траектория струи может отклоняться от прогнозируемой. В этом случае система управления роботизированной установкой пожаротушения (СУ РУП) в режиме реального времени должна автоматически выдавать сигнал пожарным роботам для корректировки положения рабочего органа в пространстве.

Таким образом, является актуальным создание программного модуля на основе нейросетевой модели, осуществляющего в реальном времени расчет координат траектории струи с учетом возмущающих воздействий и текущих рабочих параметров пожарного робота. При этом данный расчет должен быть реализуемым на существующей элементной базе СУ РУП.