ПРОБЛЕМНО-ОРИЕНТИРОВАННАЯ СИСТЕМА МОНИТОРИНГА И РЕАГИРОВАНИЯ НА МНОГОВЕКТОРНЫЕ АТАКИ В ДЕЦЕНТРАЛИЗОВАННОЙ СРЕДЕ ИНТЕРНЕТА ВЕЩЕЙ

Тебуева Ф. Б.[1], Петренко В. И.[2], Сатыбалдина Д. Ж.[3], Огур М. Г.[4], Гусева Т. М.[5]

DOI: 10.21681/2311-3456-2025-6-69-80

Цель исследования: *повышение эффективности мониторинга и реагирования на многовекторные атаки в децентрализованной среде Интернета вещей за счёт интеграции федеративного обучения, глубоких автоэнкодеров и распределённого реестра IOTA. Приоритеты включают точное обнаружение атак, минимизацию ложных срабатываний, снижение времени реакции и сохранение конфиденциальности данных.*

Метод исследования: *разработана проблемно-ориентированная система, объединяющая локальный мониторинг на IoT-узлах с автоэнкодерами для выявления аномалий, федеративное обучение с алгоритмом FedAvg для коллективного обновления моделей, а также децентрализованное распространение оповещений через распределённый реестр IOTA. Система реализует защищённый обмен модельными параметрами, цифровую подпись сообщений и асинхронное реагирование через сеть публикации/подписки.*

Результат исследования: *экспериментальные исследования на реальных данных N-BaIoT с имитацией многовекторных атак показали высокую точность обнаружения (около 95%), достижение F1-меры свыше 94%, при уровне ложных срабатываний около 4%. Время реакции системы не превышало 5 секунд, что существенно улучшает оперативность противодействия атакам. Федеративное обучение обеспечило устойчивое повышение качества модели с учётом распределённости и гетерогенности данных. Архитектура доказала масштабируемость, отказоустойчивость и способность эффективно выявлять комплексные угрозы на разных уровнях системы.*

Практическая ценность *решения заключается в возможности его внедрения в промышленных IoT, умных городах и медицинских сетях для повышения кибербезопасности с сохранением приватности и снижением нагрузок на сеть.*

Научная новизна *состоит в комплексном синтезе федеративного обучения, глубоких автоэнкодеров и технологии распределённых реестров для эффективного мониторинга многовекторных атак в децентрализованных IoT-средах. Предложенный подход сочетает преимущества распределённого обучения и блокчейн-механизмов для достижения высокой адаптивности, точности и безопасности в условиях быстрорастущих и разнообразных IoT-инфраструктур.*

Вклад авторов: *Тебуева Ф. Б. предложила концепцию и общую структуру исследования, сформулировала ключевые гипотезы и руководила проведением экспериментов; Петренко В. И. разработал математическую модель системы, предложил алгоритмы федеративного обучения и участвовал в создании архитектуры комплексной системы мониторинга и реагирования; Сатыбалдина Д. Ж. отвечала за методологию глубокого обучения, в частности, разработку и оптимизацию моделей автоэнкодеров для обнаружения аномалий; Огур М. Г. провёл экспериментальное моделирование, подготовил набор данных и осуществлял сбор и анализ экспериментальных результатов; Гусева Т. М. занималась реализацией механизмов взаимодействия компонентов системы через распределённый реестр IOTA, а также подготовкой текстовой части исследования и оформлением публикации.*

Ключевые слова: *Интернет вещей; многовекторные атаки; обнаружение вторжений; федеративное обучение; автоэнкодер; IOTA; блокчейн; аномалия; мониторинг безопасности.*

Введение

Интернет вещей (Internet of Things, IoT) с его интеллектуальными приложениями и услугами, в настоящее время охватил ключевые области в нашей повседневной жизни, включая промышленность, медицину, сельское хозяйство / сельское хозяйство, умные города, умные дома, интеллектуальный транспорт, интеллектуальные автономные транспортные средства, роботов и модульных роботов (например, беспилотные летательные аппараты, беспилотные наземные транспортные средства и беспилотные подводные аппараты) [1]. Ограниченность вычислительных ресурсов устройств и их

1 Тебуева Фариза Биляловна, доктор физико-математических наук, доцент, профессор кафедры вычислительной математики и кибернетики, ФГАОУ ВО «Северо-Кавказский федеральный университет». г. Ставрополь, Россия. ORCID: https://orcid.org/0000-0002-7373-4692. E-mail: fariza.teb@gmail.com

2 Петренко Вячеслав Иванович, кандидат технических наук, доцент, заведующий кафедрой организации и технологии защиты информации, ФГАОУ ВО «Северо-Кавказский федеральный университет». г. Ставрополь, Россия. https://orcid.org/0000-0003-4293-7013. E-mail: vipetrenko@ncfu.ru

3 Сатыбалдина Дина Жагыпаровна, кандидат физико-математических наук, директор НИИ Информационной безопасности и криптологии, НАО «Евразийский национальный университет имени Л. Н. Гумилева». г. Астана, Республика Казахстан. https://orcid.org/0000-0003-0291-4685. E-mail: satybaldina_dzh@enu.kz

4 Огур Максим Геннадьевич, старший преподаватель кафедры вычислительной математики и кибернетики, ФГАОУ ВО «Северо-Кавказский федеральный университет». г. Ставрополь, Россия. https://orcid.org/0000-0002-2387-0901. E-mail: ogur26@gmail.com

5 Гусева Татьяна Михайловна, ассистент кафедры организации и технологии защиты информации, ФГАОУ ВО «Северо-Кавказский федеральный университет». г. Ставрополь, Россия. E-mail: tatyana.petrova.96@bk.ru

распределённый характер формируют новые уязвимости, угрожающие конфиденциальности, целостности и доступности данных [2]. Традиционные централизованные методы кибербезопасности часто оказываются неэффективными в условиях распределённой архитектуры IoT и жёстких ограничений по энергопотреблению и вычислительной мощности [3]. Как следствие, фиксируется увеличение числа успешных атак на IoT-инфраструктуры [4]. Особую опасность представляют многовекторные атаки, в которых злоумышленники комбинируют различные методы воздействия (например, одновременное проведение DDoS-атаки и внедрение вредоносного кода) [5]. Подобные скоординированные воздействия сложно обнаружить и нейтрализовать, поскольку они затрагивают различные уровни системы (сетевой, прикладной, данных) и могут маскировать друг друга [6]. Это обусловливает необходимость разработки комплексных систем мониторинга безопасности, способных в реальном времени выявлять аномалии разнородной природы.

Ключевым инструментом защиты IoT-сетей являются системы обнаружения вторжений (IDS). Наиболее перспективными представляются IDS, идентифицирующие отклонения от нормального профиля работы устройств и сетевого трафика [7]. С ростом объёмов данных и усложнением угроз для анализа всё активнее применяются методы машинного обучения, в частности глубокого обучения [8]. Глубокие нейронные сети и автоэнкодеры демонстрируют высокую точность выявления ранее неизвестных атак за счёт обнаружения скрытых паттернов аномального поведения [9]. Например, в работе [10] с помощью глубокого автоэнкодера достигнуто высокоточное обнаружение ботнет-атак на IoT-устройства. Однако большинство современных IDS для IoT основаны на централизованном сборе и анализе данных: информация с устройств передаётся на сервер, где обучается общая модель классификации трафика. Такой подход имеет два существенных недостатка: (1) угрозу конфиденциальности и утечек данных из-за централизованного хранения и передачи чувствительной информации; (2) высокую нагрузку на сеть и задержки, что критично для ресурсоограниченных распределённых сред IoT [11].

Федеративное обучение (Federated Learning, FL) позволяет решить эти проблемы путём переноса процесса обучения моделей на конечные устройства с последующей агрегацией локальных обновлений [12]. При использовании FL исходные данные не покидают устройство: каждый узел обучает локальную модель на своих данных, а на сервер передаются только обновления параметров (градиенты или веса модели). Сервер-агрегатор объединяет их (например, с помощью алгоритма FedAvg) для обновления глобальной модели, которая затем рассылается участникам [13]. Этот подход обеспечивает сохранение конфиденциальности данных и снижение сетевой нагрузки, позволяя использовать знания множества распределённых источников. FL уже применяется для IDS в IoT. В частности, в [14] разработана федеративная самообучающаяся IDS, адаптирующаяся к типу устройства, которая показала точность обнаружения атак ботнета Mirai на уровне 95,6 % с задержкой ~257 мс и минимальным количеством ложных срабатываний. Другие исследования также подтверждают, что федеративные IDS по точности сопоставимы с централизованными, обеспечивая при этом приватность данных. Так, в [15] показано, что совместное обучение простой нейронной сети на устройствах с использованием FedAvg даёт метрики (точность, полнота, F1-score), comparable с централизованной моделью при обнаружении атак, но без передачи исходных данных.

Параллельно растёт интерес к использованию технологий блокчейн и распределённых реестров для повышения надёжности систем безопасности IoT [16]. Традиционный блокчейн обеспечивает неизменяемость и отслеживаемость записей о событиях безопасности, позволяя узлам доверять зафиксированным в реестре предупреждениям об атаках [17]. Однако классические блокчейн-платформы (например, Ethereum) страдают от ограниченной масштабируемости, низкой скорости транзакций и высокой энергоёмкости алгоритмов консенсуса, что затрудняет их применение в IoT-сетях [18]. В связи с этим в последние годы появились альтернативные распределённые реестры, ориентированные на IoT. Один из наиболее перспективных вариантов – платформа IOTA, использующая направленный ациклический граф (Tangle) вместо традиционной цепочки блоков [19]. IOTA сохраняет ключевые свойства блокчейна (неизменяемость, прозрачность транзакций), но устраняет комиссионные сборы и обеспечивает высокую пропускную способность и быстродействие за счёт параллельной обработки операций [20]. Исследования показывают, что IOTA существенно превосходит традиционный блокчейн по масштабируемости и энергоэффективности, что делает её одним из немногих практичных решений для ресурсоограниченных IoT-устройств [21]. Авторы [22] в своём обзоре отмечают эволюцию IoT-экосистем от блокчейна к IOTA, подчёркивая её преимущества в контексте IoT-приложений.

Учитывая указанные тенденции, актуальной научной задачей является синтез федеративного обучения, интеллектуального аномального мониторинга и распределённого реестра в единую систему защиты

IoT. Отдельные компоненты уже продемонстрировали свою эффективность: автоэнкодеры обнаруживают сложные и малозаметные атаки [23], федеративное обучение обеспечивает адаптивность и приватность [24], а реестры на основе блокчейн-технологий повышают доверие между узлами и устойчивость к компрометации журналов событий [17]. Однако интеграция этих компонентов в комплексную систему мониторинга многовекторных атак исследована недостаточно. Существующие решения, как правило, фокусируются на одной из составляющих (например, только на распределённом обнаружении или только на регистрации событий в блокчейне) и не учитывают специфику многовекторных сценариев атак.

В последние годы активно внедряются новые методы обеспечения безопасности, направленные на противодействие современным киберугрозам в условиях быстрорастущей экосистемы IoT. К ним относятся принципы Zero Trust, интеллектуальные системы обнаружения и реагирования (EDR/XDR), а также применение искусственного интеллекта и машинного обучения для анализа и предотвращения атак [4]. Например, в [24] предложено объединить блокчейн с федеративным обучением для IDS в медицинских IoT-сетях, достигнув точности ~97–98 % на реальных наборах данных. Al Sadi и др. разработали систему P-IOTA, в которой сетевые контроллеры SDN выявляют DDoS-атаки и отправляют оповещения в реестр IOTA для глобального оповещения. Тем не менее, остаётся открытым вопрос проектирования единой проблемно-ориентированной системы, способной в реальном времени обнаруживать и нейтрализовать многовекторные атаки в IoT-среде за счёт совместного использования FL, методов глубокого обучения и распределённого реестра.

Целью настоящего исследования является повышение эффективности системы мониторинга и реагирования на многовекторные атаки в децентрализованной IoT-среде за счёт минимизации совокупной ошибки обнаружения атак и времени реакции на них.

1. Постановка задачи мониторинга и реагирования на многовекторные атаки в децентрализованной среде Интернета вещей

Особенностью предлагаемого подхода является использование федеративного обучения (FL), которое позволяет обучать модели обнаружения атак непосредственно на устройствах без передачи исходных данных, обеспечивая таким образом приватность информации и устойчивость системы к новым, неизвестным видам атак. В статье [25] предложена модель угроз информационной безопасности агентов в децентрализованной среде Интернета вещей, формализующая сценарии атак на информационную безопасность доверенного взаимодействия.

Введем обозначения переменных и параметров:

N – общее число IoT-узлов (участников FL);

$D_i = \{x_{i,1}, x_{i,2}, \ldots, x_{i,n_i}\}$ – набор локальных данных (трафик, события) на узле i;

w_i^t – локальные параметры модели (веса автоэнкодера) на узле i на t-м раунде FL;

w_{glob}^t – глобальные параметры модели после централизованного или агрегированного обновления на t-м раунде;

$f(\cdot; w)$ – функция автоэнкодера (модель обнаружения аномалий с параметрами w);

$L(x; w)$ – функция потерь (ошибка реконструкции) автоэнкодера;

α – доля (или вес) вклада каждого узла при глобальном обновлении (FedAvg);

θ_{alert} – порог аномальности, при превышении которого срабатывает тревога;

$y_{i,j} \in \{0,1\}$ – метка события в D_i: 1 – атака, 0 – норма;

τ – максимальное допустимое время для срабатывания и распространения предупреждения (констрейнт на быстродействие);

$S = \{s_1, s_2, \ldots, s_M\}$ – множество вариантов многовекторных атак, где каждая атака s_m представляет собой комбинацию нескольких векторов (например, DoS + спуфинг + перебор паролей и др.);

$D_i^{s_m}$ – локальный набор данных на узле i, относящийся к атаке s_m, либо нормальным состояниям;

$L^{s_m}(x; w)$ – функция потерь (ошибка реконструкции) автоэнкодера для данных, поражённых атакой s_m;

β_m – вес, отражающий критичность (приоритетность) обнаружения многовекторной атаки s_m;

$T_{detect}^{s_m}$, $T_{alert}^{s_m}$ — время обнаружения и оповещения для атаки s_m.

Целевая функция задачи имеет вид:

$$\min_{w_{glob}} \sum_{i=1}^{N} \frac{n_i}{\sum_k n_k} \left(\sum_{m=1}^{M} \beta_m \cdot L_i^{s_m}(w_{glob}) \right) + \\ + \lambda \cdot \sum_{m=1}^{M} \gamma_m \cdot (T_{detect}^{s_m} + T_{alert}^{s_m}), \quad (1)$$

где $L_i^{s_m}(w) = \frac{1}{|D_i^{s_m}|} \sum_{x \in D_i^{s_m}} L^{s_m}(x; w)$ – усреднённая функция потерь по данным под многовекторной атакой s_m; $\beta_m \geq 0$ – приоритет обнаружения отдельных многовекторных атак, чтобы уделить особое внимание наиболее критичным; $\gamma_m \geq 0$ – вес времени реакции для каждой атаки; $\lambda \geq 0$ – параметр балансировки между точностью обнаружения и скоростью реакции.

Задача имеет ограничения:

1. Ограничения приватности (Privacy-preserving):

$\forall i,j$: $D_i^{s_m} \cap D_j^{s_m} = \emptyset$, и $D_i^{s_m}$ не передаются вне узла, (2)

то есть исходные данные остаются локальными, передача происходит только агрегированных параметров моделей:

$$w_{glob}^{t+1} = \sum_{i=1}^{N} \alpha_i \, w_i^t, \; \sum_i \alpha_i = 1, \; \alpha_i \geq 0. \quad (3)$$

2. Ограничения вычислительных ресурсов узлов.

Параметры модели $f(\cdot; w_i^t)$ должны удовлетворять локальным ресурсным ограничениям:

$$C_{time}(f_i) \leq C_{time}^{max}, \; C_{memory}(f_i) \leq C_{memory}^{max}, \quad (4)$$

где $C_{time}(f_i)$ – время вычисления модели на устройстве i; $C_{memory}(f_i)$ – объём памяти, необходимый под модель; C_{time}^{max}, C_{memory}^{max} – максимальные допустимые значения, заданные техническими характеристиками устройств.

3. Ограничения на скорость обнаружения и реагирования.

Для каждого типа атаки s_m суммарное время обнаружения и оповещения должно удовлетворять:

$$T_{detect}^{s_m} + T_{alert}^{s_m} \leq T_{max}, \quad (5)$$

где $T_{detect}^{s_m}$ – время с момента начала атаки s_m до её обнаружения системой; $T_{alert}^{s_m}$ – время распространения предупреждения по сети IoT.

4. Ограничения на качество детекции для каждого типа многовекторной атаки.

Для обеспечения надёжного обнаружения многовекторных атак пороги тревог $\theta_{alert}^{s_m}$ должны поддерживать минимальные значения метрик:

■ минимальный уровень Recall (полнота):

$$Recall^{s_m} = \frac{TP^{s_m}}{TP^{s_m} + FN^{s_m}} \geq R_{min}^{s_m}, \quad (6)$$

■ максимальный уровень ложных срабатываний (False Positive Rate):

$$FPR^{s_m} = \frac{FP^{s_m}}{FP^{s_m} + TN^{s_m}} \leq FPR_{max}^{s_m}, \quad (7)$$

где TP^{s_m}, FN^{s_m}, FP^{s_m}, TN^{s_m} – соответственно истинно-положительные, ложные отрицательные, ложные положительные и истинно-отрицательные результаты для атаки s_m; $R_{min}^{s_m}$, $FPR_{max}^{s_m}$ – целевые минимальные/максимальные значения для метрик.

2. Используемые методы и технологии

2.1. Расширенный алгоритм федеративного обучения FedAvg

Федеративное усреднение с агрегацией импульса FedAvg является передовым методом, разработанным для повышения производительности систем обнаружения вторжений IoT. Этот метод расширяет традиционный подход федеративного усреднения, включая член импульса в процесс агрегации [2].

Федеративное обучение FedAvg обеспечивает плавную и быструю сходимость глобальной модели обнаружения вторжений, даже при наличии шумных или разнородных клиентских обновлений, значительно повышая точность и эффективность. Правило обновления выражается следующим образом:

$$\theta_t = \theta_{t-1} = \eta \times (\alpha \times \sum_i \nabla \mathrm{Loss}(\theta_i) + (1 - \alpha) \times \mathrm{PrevAggGrad}), \quad (8)$$

где θ_t – обновленные параметры глобальной модели в раунде t; θ_{t-1} – глобальные параметры модели из предыдущего раунда; η – скорость обучения, которая контролирует величину обновлений; α – параметр импульса, уравновешивающий влияние текущего градиента и прошлых суммарных градиентов; $\nabla \mathrm{Loss}(\theta_i)$ – локальный градиент функции потерь, вычисленный участвующим клиентом i; PrevAggGrad – агрегированный градиент из предыдущего раунда.

Эта формулировка расширяет стандартный алгоритм FedAvg, вводя член импульса $\nabla \mathrm{Loss}(\theta_i)$, который помогает уменьшить колебания и сгладить процесс оптимизации. Включение $(1 - \alpha) \times \mathrm{PrevAggGrad}$ гарантирует, что историческая информация о градиенте способствует глобальному обновлению, обеспечивая стабильность и более быструю сходимость, особенно в средах данных не независимых и одинаково распределенных.

Расширенный алгоритм федеративного обучения FedAvg описывает метод агрегации на стороне сервера с импульсом для FL. Алгоритм направлен на повышение сходимости и устойчивости путем включения импульса в агрегацию градиентов от участвующих сущностей. Этот параметр импульса улучшает способность ориентироваться в сложных ландшафтах оптимизации и эффективно распространять информацию между федеративными раундами обучения. Алгоритм начинается с инициализации глобальных параметров модели (θ_0), параметра импульса (α) и скорости обучения (η). Затем он выполняет несколько раундов федеративного обучения до достижения сходимости. В каждом раунде алгоритм инициализирует агрегированный градиент (AggGrad) нулем. Он собирает локальные параметры модели ((θ_i)) из каждой участвующей сущности и вычисляет локальный градиент ($Grad_i$) на основе градиента функции потерь ($\nabla \mathrm{Loss}(\theta_i)$). Эти локальные градиенты накапливаются для обновления агрегированного градиента (AggGrad).

Для применения импульса алгоритм обновляет агрегированный градиент, объединяя предыдущий агрегированный градиент (PrevAggGrad), взвешенный по $(1 - \alpha)$, с текущим агрегированным градиентом (AggGrad), взвешенным по α. Эта корректировка сохраняет историческую информацию из предыдущих раундов, помогая сгладить влияние зашумленных или флуктуирующих градиентов.

После агрегации глобальные параметры модели (θ_t) обновляются путем вычитания произведения скорости обучения (η) и агрегированного градиента (AggGrad) из предыдущих глобальных параметров

модели (θ_{t-1}). Обновлённые параметры затем распределяются обратно участвующим сущностям для следующего раунда обучения. На протяжении всей работы алгоритма PrevAggGrad сохраняет агрегированный градиент из предыдущего раунда для обеспечения непрерывности импульса. Этот итерационный процесс продолжается до тех пор, пока не будут выполнены критерии сходимости, что завершает обучение.

2.2. Глубокие автоэнкодеры

Глубокие автоэнкодеры обучаются восстанавливать входные данные, сжимая их в компактное представление (кодировку) и затем декодируя обратно. Основная идея заключается в том, что автоэнкодер хорошо восстанавливает нормальные данные, но плохо справляется с аномалиями, что позволяет выявлять отклонения на основе ошибки реконструкции.

Автоэнкодер состоит из двух частей:

1. Кодировщик (энкодер) – преобразует входные данные в скрытое представление меньшей размерности.
2. Декодировщик (декодер) – восстанавливает исходные данные из скрытого представления.

Обучение автоэнкодера проводится на нормальных данных, чтобы минимизировать ошибку восстановления. После обучения для новых данных вычисляется ошибка реконструкции: если она превышает заданный порог, событие считается аномальным. Это позволяет обнаруживать неизвестные атаки без необходимости их предварительного описания.

Функция кодирования (энкодер) представляет собой отображение

$$f_{\theta_e} : \mathbb{R}^d \longrightarrow \mathbb{R}^h, \tag{9}$$

где θ_e – параметры кодировщика, d – размерность входных данных, h – размерность скрытого представления ($h < d$).

Функция декодирования (декодер) представляет собой отображение

$$g_{\theta_d} : \mathbb{R}^h \longrightarrow \mathbb{R}^d, \tag{10}$$

где θ_d – параметры декодировщика.

Автоэнкодер обучается путем минимизации различия между исходными данными и восстановленными данными. Основное требование – точное воспроизведение исходных данных на выходе.

Обучение происходит по следующим этапам:

Этап 1. Ошибка реконструкции.

Для входного вектора x автоэнкодер вычисляет восстановленный выход:

$$\hat{x} = g_{\theta_d} f_{\theta_e}(x). \tag{11}$$

Ошибка реконструкции определяется как среднеквадратичное отклонение:

$$L(x;\Theta) = \|x - \hat{x}\|^2, \tag{12}$$

где $\Theta = \{\theta_e, \theta_d\}$ — параметры модели.

Этап 2. Обучение.

Автоэнкодер обучается на множестве нормальных данных $X_{\text{train}} = \{x^i_{\text{norm}}\}$ путем минимизации средней ошибки:

$$L(\Theta) = \frac{1}{|X_{\text{train}}|} \sum_{x \in X_{\text{train}}} \| x - g_{\theta_d}(f_{\theta_e}(x)) \|^2 . \tag{13}$$

Этап 3. Обнаружение аномалий.

Для нового входного вектора x_{new} вычисляется ошибка реконструкции $e_{x_{\text{new}}}$

$$e_{x_{\text{new}}} > \theta, \tag{14}$$

где θ – порог аномальности, событие помечается как аномальное. Порог θ выбирается так, чтобы вероятность ложных срабатываний α была минимальной $\Pr_{x \sim P_{\text{norm}}}(e(x) > \theta) = \alpha$.

3. Предлагаемая проблемно-ориентированная система

3.1. Алгоритм предлагаемой системы

Для решения поставленной задачи (1)–(7) разработан комбинированный метод, сочетающий распределённое обучение модели обнаружения аномалий и децентрализованное распространение оповещений. На рисунке 1 представлена общая схема предлагаемой системы. Она включает три основные процесса, происходящие непрерывно и параллельно: локальный мониторинг на узлах IoT, федеративное обновление модели обнаружения, децентрализованное оповещение и реагирование.

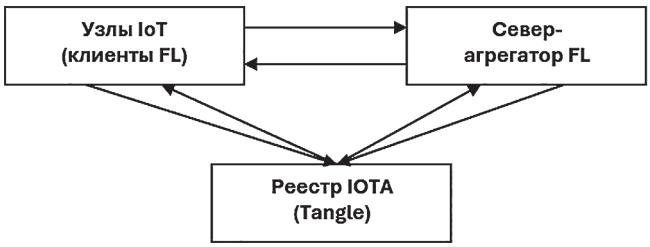

Рис. 1. Общая схема предлагаемой системы

1. Локальный мониторинг на узлах IoT.

Каждый узел (устройство) выполняет постоянный сбор данных о своём состоянии и трафике (например, сетевые потоки, системные логи, показания датчиков и пр.). Эти данные в режиме реального времени подаются на вход локальной модели обнаружения аномалий – лёгкого автоэнкодера, заранее обученного распознавать нормальное поведение устройства. Модель рассчитывает степень аномалии каждого наблюдения: если ошибка реконструкции превышает заданный порог θ, событие помечается

как потенциальная атака. Порог θ выбирается на основе статистики ошибок на обучающей выборке (например, θ соответствует квантилю 99-го процента ошибок на нормальных данных, чтобы обеспечить низкий уровень ложных срабатываний).

2. Федеративное обновление модели обнаружения.

Для адаптации к новым угрозам и изменениям в поведении устройств узлы периодически участвуют в обновлении модели автоэнкодера. Процесс координируется центральным агрегатором по следующему алгоритму:

1. Агрегатор рассылает актуальные веса глобальной модели W всем узлам.
2. Каждый узел проводит локальное обучение на новых данных, включая нормальные и аномальные сессии с пониженным весом.
3. Локальные веса W_i или градиенты ΔW_i передаются агрегатору.
4. Агрегатор усредняет полученные обновления.

Такой подход позволяет модели обучаться на распределённых данных всех устройств, повышая её обобщающую способность. Федеративное обучение сокращает объём передаваемых данных до параметров модели (несколько КБ вместо МБ исходных логов) и обеспечивает сохранение приватности, поскольку исходные данные не покидают устройства.

3. Децентрализованное оповещение и реагирование.

При срабатывании детектора аномалий узел формирует сигнал тревоги с идентификатором устройства, временной меткой, типом активности и хэшем подозрительных данных. Сигнал публикуется в распределённый реестр IOTA через транзакцию в Tangle, обеспечивая быстрое и безкомиссионное распространение. Подписанные узлы получают уведомление и применяют локальные меры: фильтрацию трафика, изоляцию устройств или оповещение администратора. Все события фиксируются в реестре, формируя неизменяемый журнал. Система устойчива к отказам: данные сохраняются в Tangle и не могут быть удалены злоумышленником.

Алгоритм работы предлагаемой системы имеет вид:

Алгоритм 1. Federated Anomaly Detection and Response in IoT

Вход: Порог аномалии θ (14), начальные веса модели W_0, интервал федеративных обновлений T.

Выход: Обновляемая глобальная модель обнаружения; транзакции-оповещения об атаках в реестре.

Этап 1. Инициализация:

- считывать новые данные x (пакет трафика, измерение и т.п.);
- вычислить $\hat{x} = AE(x)$ проходом через автоэнкодер;
- рассчитать ошибку $e = ||x - \hat{x}||^2$ (12), (14);
- если $e > \theta$: пометить событие как аномалию и перейти к шагу 3; иначе продолжить мониторинг.

Этап 2. Локальная реакция на аномалию (узел-детектор):

- сформировать сообщение об атаке m с детализацией (ID узла, время, признаки аномалии);
- отправить транзакцию в реестр IOTA с сообщением m (функция PublishToTangle(m));
- продолжить мониторинг (шаг 2).

Этап 3. Глобальное оповещение (каждый узел, асинхронно):

- при получении из реестра нового сообщения m об атаке: проверить подпись и целостность;
- выполнить преднастроенные меры: например, обновить локальные правила фильтрации, пометить соответствующие данные как вредоносные, уведомить администратора.

Этап 4. Федеративное обновление модели (агрегатор, каждые T времени):

- разослать текущее состояние модели $W^{(t)}$ на все узлы;
- для каждого узла i: обучить копию модели на локальных данных (например, за последние T интервала), получить обновлённые веса $W_i^{(t+1)}$; отправить их агрегатору;
- по получении всех (или большинства) обновлений вычислить новое глобальное состояние: $W^{(t+1)} = \frac{1}{\sum_i n_i} \sum_i n_i W_i^{(t+1)}$;
- установить $t\ (:=)\ t + 1$.

Этап 5. Обновление локальных моделей: По мере получения обновлённых глобальных весов $W^{(t+1)}$ узлы обновляют свои автоэнкодеры (начиная новый цикл мониторинга с улучшенной моделью).

Алгоритм обеспечивает цикличное улучшение модели и параллельное реагирование на инциденты. Фаза реагирования (этапы 3–4) выполняется асинхронно и значительно быстрее обучения: сигнал тревоги распространяется через IOTA с задержкой в секунды, тогда как обучение модели происходит в фоне с интервалом порядка часа. Это позволяет быстро локализовать и ограничить атаку до обновления глобальной модели.

3.2. Архитектура предлагаемой системы

Архитектура системы включает ключевые компоненты:

1. Узлы IoT – гетерогенные устройства с агентом безопасности, выполняющим сбор диагностических данных и локальный запуск автоэнкодера для обнаружения аномалий. При срабатывании генерируется оповещение. Узлы реализуют федеративное обучение, имеют защищённое хранилище ключей для подписания сообщений.

2. Центральный сервер-агрегатор – координатор федеративного обучения, хранящий глобальную модель и собирающий обновления. Размещается в облаке или на периферии. Обеспечена защита сервера, но система сохраняет базовую функциональность при его отказе. Сервер взаимодействует с IOTA, публикует глобальные сообщения и обновления.

3. Распределённый реестр IOTA – децентрализованная сеть для хранения и распространения сообщений об атаках без комиссий. Узлы IoT и сервер подключаются к сети по схеме публикация/подписка. Может использоваться публичный Tangle или выделенный кластер.

4. Администратор/аналитический центр – обеспечивает мониторинг, управление параметрами системы, доступ к истории атак. Не является обязательным, но важен для эксплуатации.

Взаимодействие построено по двум осям: обучение (узлы ↔ сервер-агрегатор) и реагирование (узлы ↔ узлы через реестр), что обеспечивает многоуровневую защиту от локального обнаружения до глобальной координации и оповещения.

Ключевыми процессами являются:

1. Обмен параметрами модели (FL) – агент на узле выступает клиентом FL, соединяется с сервером через защищённый канал (TLS). Протокол предусматривает аутентификацию клиентов и проверку подписей глобальной модели для предотвращения атак с подменой модели.

2. Публикация и получение оповещений (IOTA) – модуль Tangle Client отправляет зашифрованные сообщения об атаках в сеть IOTA с использованием общего тега («IoTSecAlert»). Подписанные узлы получают уведомления и инициируют локальные меры защиты, обеспечивая быструю реакцию на распространение угроз.

3. Хранилище и анализ данных – преимущественно онлайн-мониторинг с возможностью сбора агрегированных статистик и результатов обнаружения. Журнал транзакций IOTA служит неизменяемым хранилищем истории инцидентов. Сервер или администратор могут использовать данные для отчётности, дообучения и прогнозирования атак.

Ниже описан сценарий, иллюстрирующий работу системы при возникновении атаки:

0. Узлы A, B, C запущены, начальная модель автоэнкодера обучена. Обмен параметрами с сервером происходит каждые 30 минут.

1. Злоумышленник начинает многовекторную атаку на узел A — массированный трафик и эксплуатация уязвимости прошивки.

2. Узел A фиксирует аномалию: автоэнкодер (13) выдаёт высокую ошибку реконструкции (9), (10), (12). Генерирует и публикует сообщение об атаке в IOTA.

3. Узлы B и C получают уведомление, блокируют подозрительный IP по правилам брандмауэра, предотвращая распространение атаки.

4. Сервер-агрегатор регистрирует инцидент и при необходимости запускает внеочередной раунд федеративного обучения. Часто вмешательство не требуется — узлы уже отреагировали.

5. Атака продолжается, злоумышленник пытается заразить узел B, но трафик блокируется. Узел A частично изолирован.

6. Узел B обнаруживает аномалию другим вектором, публикует своё сообщение. Узлы A и C обновляют защитные меры. Вся сеть обменивается информацией, снижая эффект неожиданности атаки.

7. После инцидента участники запускают федеративное обучение на собранных данных, включая аномалии, повышая чувствительность модели. Обновлённая модель распространяется по узлам, замыкая цикл обучения.

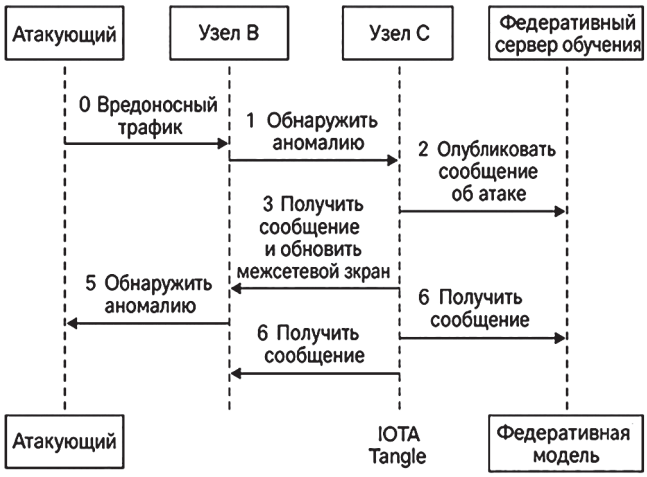

Рис. 2. Сценарий, иллюстрирующий работу системы при возникновении атаки

3.3. Метрики эффективности предложенной системы

Формально, качество обнаружения настраивается и оценивается следующими показателями. Обозначим: TP – число корректно обнаруженных атак (True Positives), FN – атак, которые система не обнаружила (False Negatives), FP – ложных тревог (False Positives), TN – корректных отрицаний (True Negatives).

1. Доля верно классифицированных ситуаций (атака / норма) среди всех

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}. \qquad (15)$$

При сильном дисбалансе (гораздо больше нормальных случаев) эта метрика не столь информативна, поэтому вводят дополнительные:

2. Точность прогноза атаки, характеризуюая надёжность срабатываний (сколько ложных тревог)

$$\text{Precision} = \frac{TP}{TP + FP}. \quad (16)$$

3. Полнота, чувствительность (доля обнаруженных атак)

$$\text{Recall} = \frac{TP}{TP + FN}. \quad (17)$$

4. F1-мера

$$\text{F1} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}. \quad (18)$$

5. Доля ложных тревог среди всех нормальных событий

$$\text{FPR} = \frac{FP}{FP + TN}. \quad (19)$$

4. Экспериментальные исследования

4.1. Экспериментальная установка и методология

Экспериментальная оценка системы мониторинга и реагирования проводилась в виртуальной IoT-среде с моделированием многовекторных атак. Для этого был использован специализированный стенд, включающий 9 виртуальных IoT-узлов различных типов устройств и сервер-агрегатор. Аппаратные ресурсы узлов соответствовали типовым характеристикам периферийных устройств, а сетевая инфраструктура воспроизводила параметры беспроводных IoT-сетей.

В качестве данных применён набор N-BaIoT, содержащий трафик девяти видов устройств в нормальном режиме и под воздействием атак. Из 115 признаков были отобраны 43 наиболее релевантных, а каждому узлу был назначен конкретный тип устройства для обеспечения гетерогенности поведения.

В эксперименте рассматривались два типа атак: классические одновекторные и синтезированные многовекторные с одновременным воздействием на несколько узлов. Для моделирования аутентификации добавлен признак количества неудачных попыток входа.

Перед тестированием проведена предварительная тренировка автоэнкодера на нормальных данных с установкой порога аномалий, обеспечивающего низкий уровень ложных срабатываний. Эксперимент длился 30 минут с периодическим обновлением глобальной модели в ходе шести раундов федеративного обучения.

Для сравнительного анализа применялись три конфигурации систем обнаружения: централизованная, федеративная и локальные модели. Во время эксперимента фиксировались ключевые показатели эффективности, включая точность и полноту обнаружения, время реагирования, а также нагрузку на сеть и вычислительные ресурсы. Использовались синтетические метки атак для обеспечения точности оценки.

4.2. Результаты эксперимента

Результаты экспериментов представлены в табл. 1 и на рис. 3, 4. Были сформированы результаты по следующим аспектам: качество обнаружения атак, эффективность реагирования, производительность и накладные расходы, а также влияние федеративного обучения.

Таблица 1.

Итоги обнаружения (среднее по узлам) по метрикам качества (16)–(19)

Подход	Precision, %	Recall, %	F1 score, %	FPR, %
Централизованный	95,8	95,1	95,5	1,2
Федеративный	94,7	94,0	94,3	3,9
Локальные	90,5	88,2	89,3	5,4

Экспериментальные исследования показали высокую эффективность предложенного подхода. Федеративный метод достиг F1-меры 94,3 %, близкой к централизованному решению (95,5 %) и значительно превосходящей изолированные локальные модели (89,3 %). Уровень ложных срабатываний в федеративной системе составил 3,9 %, что соответствует требованиям IoT. Полнота (recall) улучшена за счёт обобщения знаний о различных атаках в распределённой сети.

Среднее время обнаружения атаки – 1,8 с, доставка оповещений через реестр IOTA – 2,7 с, суммарное время реакции не превышает 4,5 с, что существенно быстрее развития атак. Объём передаваемых данных менее 1,2 МБ за 30 минут, загрузка процессора – 15–25 %, потребление памяти не превышает 50 МБ на узел.

В ходе федеративного обучения точность обнаружения повысилась с 92 % до 95 % к шестому раунду, что подтверждает адаптивность и эффективность коллективного обучения. Кривые Accuracy и Loss на рисунке 3 показывают, что федеративная модель приближается к централизованной по качеству, превышая локальные модели по точности восстановления.

Рисунок 4 иллюстрирует пример временной линии многовекторной атаки: показаны моменты срабатывания на узлах и доставки сигналов – как раз видно, что сигнал от узла A успел дойти до других до того, как их атаки начались, существенно снизив последствия.

Полученные результаты экспериментальных исследований свидетельствуют о достижении поставленных целей работы. Разработанная система

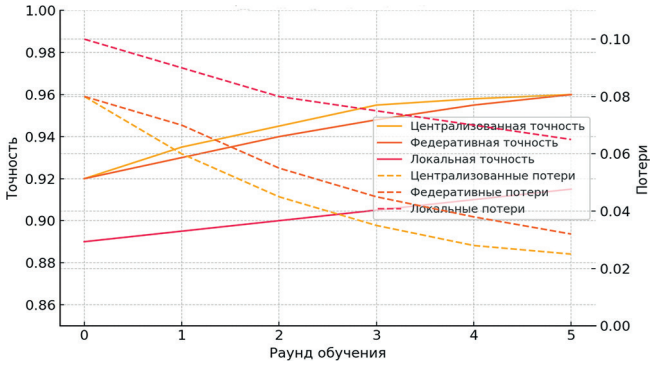

Рис. 3. Кривые изменения Accuracy (16) и Loss (ошибки реконструкции)

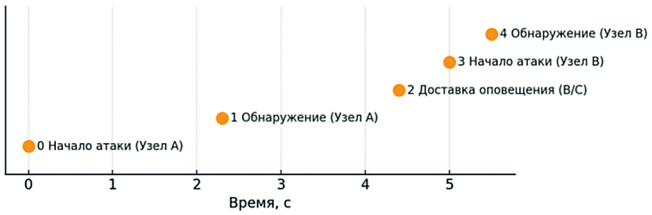

Рис. 4. Временная линия многовекторной атаки

продемонстрировала способность к эффективному обнаружению различных типов атак с показателем F1-меры, превышающим 94 %, при времени реакции менее 5 секунд. Важным достижением является приближение эффективности предложенного децентрализованного подхода к показателям централизованных систем при сохранении преимуществ распределённой архитектуры.

Несмотря на высокие показатели, достигнутые в контролируемых условиях, практическое внедрение системы требует решения ряда дополнительных задач. Реальный трафик IoT-устройств обладает повышенной зашумлённостью и вариативностью, что может вызвать рост числа ложных срабатываний. Для снижения этого влияния целесообразно применять адаптивные пороговые значения и совершенствовать модели обнаружения аномалий. Кроме того, вопросы безопасности самой системы требуют особого внимания. Цифровые подписи обеспечивают защиту от несанкционированного доступа, однако возможны атаки на модель обучения со стороны скомпрометированных устройств. Для решения этих проблем необходимы механизмы византийской отказоустойчивости и эффективные системы управления доверием.

Заключение

В работе предложена и исследована проблемно-ориентированная система мониторинга и реагирования на многовекторные атаки в децентрализованных IoT-средах. Разработанное решение интегрирует три ключевых компонента: федеративное обучение на основе алгоритма FedAvg, глубокие автоэнкодеры для обнаружения аномалий и распределенный реестр IOTA для координации реагирования. Такой комплексный подход позволяет одновременно решать проблемы распределенности данных, обнаружения неизвестных угроз и обеспечения доверия в отсутствие централизованных органов. Архитектура системы включает три уровня: устройства с локальными моделями обнаружения, сервер-агрегатор для координации обучения и распределенный реестр для обмена информацией об атаках. Представленная математическая модель формализует процессы обучения, обнаружения и реагирования, а также определяет критерии эффективности системы.

Экспериментальные исследования на наборе данных N-BaIoT подтвердили высокую эффективность предложенного подхода. Федеративная система продемонстрировала точность обнаружения атак на уровне 95 %, что сопоставимо с централизованными решениями. Показатель F1-меры улучшен на 5 процентных пунктов по сравнению с изолированными локальными системами. Время реакции системы не превышает 5 секунд, а ресурсные затраты соответствуют ограничениям IoT-устройств. Теоретическая значимость работы заключается в демонстрации возможности synergies технологий машинного обучения и распределенных реестров для безопасности IoT. Практическая ценность состоит в разработке архитектуры, применимой в промышленных IoT, умных городах и медицинских сетях.

Перспективные направления дальнейших исследований включают: расширение класса detectable атак, повышение устойчивости системы к targeted атакам, оптимизацию производительности для микроконтроллеров, а также интеграцию механизмов reinforcement learning для активного противодействия угрозам. Проведенное исследование подтверждает возможность создания эффективных распределенных систем безопасности для Интернета вещей, сочетающих высокую точность обнаружения с сохранением конфиденциальности данных и отказоустойчивостью.

Исследование выполнено при финансовой поддержке Российского научного фонда, проект №24-21-00481 по теме «Методы противодействия многовекторным атакам на децентрализованные системы Интернета вещей».

Литература

1. Yaacoub J.-P. A., Noura H. N., Salman O. Security of federated learning with IoT systems: issues, limitations, challenges, and solutions // Internet of Things and Cyber-Physical Systems. 2023. Vol. 3. P. 155–179. DOI: 10.1016/j.iotcps.2023.04.001.
2. Khraisat A., Alazab A., Jan T. Federated learning for intrusion detection in IoT environments: a privacy-preserving strategy // Discover Internet of Things. 2025. Vol. 5, № 1. Article 17 p. DOI: 10.1007/s43926-025-00169-7.
3. Olanrewaju-George B., Pranggono B. Federated learning-based intrusion detection system for the internet of things using unsupervised and supervised deep learning models // Cyber Security and Applications. 2025. Vol. 3, December. Article 100068. DOI: 10.1016/j.csa.2024.100068.
4. Karunamurthy A., Vijayan K., Kshirsagar P. R. et al. An optimal federated learning-based intrusion detection for IoT environment // Sci Rep. 2025. Vol. 15, Article 8696. DOI: 10.1038/s41598-025-93501-8.
5. Rampone G., Ivaniv T., Rampone S. A hybrid federated learning framework for privacy-preserving near-real-time intrusion detection in IoT environments // Electronics. 2025. Vol. 14, № 7. Article 1430. DOI: 10.3390/electronics14071430.
6. Meidan Y., Bohadana M., Mathov Y., Mirsky Y., Shabtai A., Breitenbacher D., Elovici Y. N-BaIoT – network-based detection of IoT botnet attacks using deep autoencoders // IEEE Pervasive Computing. 2018. Vol. 17, № 3. P. 12–22. DOI: 10.1109/MPRV.2018.03367731.
7. Anand R. V., Magesh G., Alagiri I. et al. Design of an improved model using federated learning and LSTM autoencoders for secure and transparent blockchain network transactions // Sci Rep. 2025. Vol. 15, Article 1615. DOI: 10.1038/s41598-024-83564-4.
8. Nguyen V.-D., Diro A., Chilamkurti N., Heyne W., Phan K. T. Novel blockchain-enabled federated learning scheme for IoT anomaly detection // IEEE Access. DOI: 10.1109/11070312.
9. Friha O., Ferrag M. A., Benbouzid M., Berghout T., Kantarci B., Choo K.-K. R. 2DF-IDS: decentralized and differentially private federated learning-based intrusion detection system for industrial IoT // Computers & Security. 2023. Vol. 127. Article 103097. DOI: 10.1016/j.cose.2023.103097.
10. Begum K., Mozumder M. A. I., Joo M., Kim H. BFLIDS: blockchain-driven federated learning for intrusion detection in IoMT networks // Sensors. 2024. Vol. 24, № 14. Article 4591. DOI: 10.3390/s24144591.
11. Yang E., Jeong S., Seo C. Harnessing feature pruning with optimal deep learning based DDoS cyberattack detection on IoT environment // Scientific Reports. 2025. Vol. 15. DOI: 10.1038/s41598-025-02152-2.
12. Saranya K., Valarmathi A. A multilayer deep autoencoder approach for cross layer IoT attack detection using deep learning algorithms // Scientific Reports. 2025. Vol. 15, Article 10246. DOI: 10.1038/s41598-025-93473-9.
13. Regan C., Nasajpour M., Parizi R. M., Pouriyeh S., Dehghantanha A., Choo K.-K. R. Federated IoT attack detection using decentralized edge data // Machine Learning with Applications. 2022. Vol. 8. Article 100263. DOI: 10.1016/j.mlwa.2022.100263.
14. Khan A. A., Waseem M., Alshamrani N., Alharbi M., Alhazmi A. S., Zohdy A. M., Alattas F. A., Al Ghamdi A. Learning-based methods for cyber attacks detection in IoT systems: a survey on methods, analysis, and future prospects // Electronics. 2022. Vol. 11, № 9. Article 1502. DOI: 10.3390/electronics11091502.
15. Ferrag M. A., Friha O., Maglaras L., Janicke H., Shu L. Security of federated learning with IoT systems: issues, limitations, challenges, and solutions // Internet of Things. 2023. T. 22. C. 100222. DOI: 10.1016/j.iot.2023.100222.
16. Alshaikhli M., Elfouly T., Elharrouss O., Mohamed A., Ottakath N. Evolution of internet of things from blockchain to IOTA: a survey // IEEE Access. 2022. Vol. 10. P. 844–866. DOI: 10.1109/ACCESS.2021.3138353.
17. Shalabi K., Abu Al-Haija Q., Al-Fayoumi M. A. A blockchain-based intrusion detection/prevention systems in IoT network: a systematic review // Procedia Computer Science. 2024. Vol. 236. P. 410–419. DOI: 10.1016/j.procs.2024.05.048.
18. Alharthi H., Alshehri S., Kalkatawi M. Revolutionizing IoT security: a blockchain and federated learning-based anomaly detection system // In: Proceedings of the 2024 7th Artificial Intelligence and Cloud Computing Conference (AICCC '24). 2024. P. 565–572. DOI: 10.1145/3719384.3719466.
19. Al Sadi A., Mazzocca C., Melis A., Montanari R., Prandini M., Romandini N. P-IOTA: a cloud-based geographically distributed threat alert system that leverages P4 and IOTA // Sensors. 2023. Vol. 23, № 6. Article 2955. DOI: 10.3390/s23062955.
20. Lazzarini R., Tianfield H., Charissis V. Federated learning for IoT intrusion detection // AI. 2023. Vol. 4. №. 3. P. 509–530. DOI: 10.3390/ai4030028.
21. Ferrag M. A., Friha O., Maglaras L., Janicke H., Shu L. On the performance of federated learning algorithms for IoT // IoT. 2023. T. 3, № 2. C. 273–284. DOI: 10.3390/iot3020016.
22. Alsaedi A., Moustafa N., Tari Z., Mahmood A., Anwar A. Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures // Journal of Information Security and Applications. 2021. Vol. 58. Article 102413. DOI: 10.1016/j.jisa.2021.102413.
23. Khan M. A., Waseem M., Alshamrani N., Alharbi M., Alhazmi A. S., Zohdy A. M., Alattas F. A., Al Ghamdi A. Security considerations for Internet of Things: a survey // SN Computer Science. 2020. Vol. 1, no. 4. Article 193. DOI: 10.1007/s42979-020-00201-3.
24. Ceccarelli M., Zecchini M., Brighente A., Conti M. GitHub – MMw-Unibo/FETA: enabling federated learning at the edge through the IOTA Tangle // Future Generation Computer Systems. 2024. P. 17–29. DOI: 10.1016/j.future.2023.10.014.
25. Тебуева Ф. Б., Рябцев С. С., Огур М. Г., Андреев И. А., Горяйнов С. А. Модель угроз информационной безопасности агентов в децентрализованной среде Интернета вещей, формализующая сценарии атак на информационную безопасность доверенного взаимодействия // Кузнечно-штамповочное производство. Обработка материалов давлением. 2024. № 11. С. 220–232.

PROBLEM-ORIENTED SYSTEM FOR MONITORING AND RESPONDING TO MULTIVECTOR ATTACKS IN A DECENTRALIZED INTERNET OF THINGS ENVIRONMENT

Tebueva F. B.[6], Petrenko V. I.[7], Satybaldina D. Zh.[8], Ogur M. G.[9], Guseva T. M.[10]

Keywords: *Internet of Things; multivector attacks; intrusion detection; federated learning; autoencoder; IOTA; blockchain; anomaly; security monitoring.*

Objective: *to enhance the effectiveness of monitoring and responding to multivector attacks in a decentralized Internet of Things (IoT) environment by integrating federated learning, deep autoencoders, and the distributed IOTA ledger. The priorities include accurate attack detection, minimizing false positives, reducing response time, and preserving data privacy.*

Method: *a problem-oriented system was developed, combining local monitoring on IoT nodes with autoencoders for anomaly detection, federated learning using the FedAvg algorithm for collective model updates, and decentralized alert dissemination via the distributed IOTA ledger. The system implements secure exchange of model parameters, digital message signing, and asynchronous response through a publish/subscribe network.*

Results: *experimental studies on the real N-BaIoT dataset simulating multivector attacks demonstrated high detection accuracy (approximately 95%), achieving an F1-score above 94%, with false positive rates around 4%. The system's response time did not exceed 5 seconds, significantly improving operational reaction to attacks. Federated learning provided steady improvement in model quality considering data distribution and heterogeneity. The architecture proved scalable, fault-tolerant, and capable of effectively detecting complex threats across multiple system levels.*

Practical value: *the solution is implementable in industrial IoT, smart cities, and medical networks to enhance cybersecurity while maintaining privacy and reducing network load.*

Scientific novelty: *the study presents a comprehensive synthesis of federated learning, deep autoencoders, and distributed ledger technology for effective monitoring of multivector attacks in decentralized IoT environments. The proposed approach combines the advantages of distributed learning and blockchain mechanisms to achieve high adaptability, accuracy, and security in rapidly growing and diverse IoT infrastructures.*

References

1. Yaacoub J.-P. A., Noura H. N., Salman O. Security of federated learning with IoT systems: issues, limitations, challenges, and solutions // Internet of Things and Cyber-Physical Systems. 2023. Vol. 3. P. 155–179. DOI: 10.1016/j.iotcps.2023.04.001.
2. Khraisat A., Alazab A., Jan T. Federated learning for intrusion detection in IoT environments: a privacy-preserving strategy // Discover Internet of Things. 2025. Vol. 5, № 1. Article 17 p. DOI: 10.1007/s43926-025-00169-7.
3. Olanrewaju-George B., Pranggono B. Federated learning-based intrusion detection system for the internet of things using unsupervised and supervised deep learning models // Cyber Security and Applications. 2025. Vol. 3, December. Article 100068. DOI: 10.1016/j.csa.2024.100068.
4. Karunamurthy A., Vijayan K., Kshirsagar P. R. et al. An optimal federated learning-based intrusion detection for IoT environment // Sci Rep. 2025. Vol. 15, Article 8696. DOI: 10.1038/s41598-025-93501-8.
5. Rampone G., Ivaniv T., Rampone S. A hybrid federated learning framework for privacy-preserving near-real-time intrusion detection in IoT environments // Electronics. 2025. Vol. 14, №7. Article 1430. DOI: 10.3390/electronics14071430.
6. Meidan Y., Bohadana M., Mathov Y., Mirsky Y., Shabtai A., Breitenbacher D., Elovici Y. N-BaIoT – network-based detection of IoT botnet attacks using deep autoencoders // IEEE Pervasive Computing. 2018. Vol. 17, № 3. P. 12–22. DOI: 10.1109/MPRV.2018.03367731.
7. Anand R. V., Magesh G., Alagiri I. et al. Design of an improved model using federated learning and LSTM autoencoders for secure and transparent blockchain network transactions // Sci Rep. 2025. Vol. 15, Article 1615. DOI: 10.1038/s41598-024-83564-4.
8. Nguyen V.-D., Diro A., Chilamkurti N., Heyne W., Phan K. T. Novel blockchain-enabled federated learning scheme for IoT anomaly detection // IEEE Access [электронный ресурс]. DOI: 10.1109/11070312. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=11070312 (дата обращения – 03.09.2025).
9. Friha O., Ferrag M. A., Benbouzid M., Berghout T., Kantarci B., Choo K.-K. R. 2DF-IDS: decentralized and differentially private federated learning-based intrusion detection system for industrial IoT // Computers & Security. 2023. Vol. 127. Article 103097. DOI: 10.1016/j.cose.2023.103097.
10. Begum K., Mozumder M. A. I., Joo M., Kim H. BFLIDS: blockchain-driven federated learning for intrusion detection in IoMT networks // Sensors. 2024. Vol. 24, № 14. Article 4591. DOI: 10.3390/s24144591.

6 Fariza B. Tebueva, Dr.Sc. of Physical and Mathematical Sciences, Associate Professor, Professor of the Department of Computational Mathematics and Cybernetics, North Caucasus Federal University. Stavropol, Russia. ORCID: https://orcid.org/0000-0002-7373-4692. E-mail: fariza.teb@gmail.com

7 Vyacheslav I. Petrenko, Ph.D. of Technical Sciences, Associate Professor, Head of the Department of Organization and Technology of Information Security, North Caucasus Federal University. Stavropol, Russia. https://orcid.org/0000-0003-4293-7013. E-mail: vipetrenko@ncfu.ru

8 Dina Z. Satybaldina, Ph.D. of Physical and Mathematical Sciences, Director of the Research Institute of Information Security and Cryptology, L.N. Gumilyov Eurasian National University, Astana, Republic of Kazakhstan. https://orcid.org/0000-0003-0291-4685. E-mail: satybaldina_dzh@enu.kz

9 Maxim G. Ogur, Senior Lecturer of the Department of Computational Mathematics and Cybernetics, North Caucasus Federal University, Stavropol, Russia. https://orcid.org/0000-0002-2387-0901. E-mail: ogur26@gmail.com

10 Tatyana M. Guseva, Assistant of the Department of Organization and Technology of Information Security, North Caucasus Federal University, Stavropol, Russia. E-mail: tatyana.petrova.96@bk.ru

11. Yang E., Jeong S., Seo C. Harnessing feature pruning with optimal deep learning-based DDoS cyberattack detection on IoT environment // Scientific Reports. 2025. Vol. 15. DOI: 10.1038/s41598-025-02152-2.
12. Saranya K., Valarmathi A. A multilayer deep autoencoder approach for cross layer IoT attack detection using deep learning algorithms // Scientific Reports. 2025. Vol. 15, Article 10246. DOI: 10.1038/s41598-025-93473-9.
13. Regan C., Nasajpour M., Parizi R. M., Pouriyeh S., Dehghantanha A., Choo K.-K. R. Federated IoT attack detection using decentralized edge data // Machine Learning with Applications. 2022. Vol. 8. Article 100263. DOI: 10.1016/j.mlwa.2022.100263.
14. Khan A. A., Waseem M., Alshamrani N., Alharbi M., Alhazmi A. S., Zohdy A. M., Alattas F. A., Al Ghamdi A. Learning-based methods for cyber attacks detection in IoT systems: a survey on methods, analysis, and future prospects // Electronics. 2022. Vol. 11, № 9. Article 1502. DOI: 10.3390/electronics11091502.
15. Ferrag M. A., Friha O., Maglaras L., Janicke H., Shu L. Security of federated learning with IoT systems: issues, limitations, challenges, and solutions // Internet of Things. 2023. T. 22. C. 100222. DOI: 10.1016/j.iot.2023.100222.
16. Alshaikhli M., Elfouly T., Elharrouss O., Mohamed A., Ottakath N. Evolution of internet of things from blockchain to IOTA: a survey // IEEE Access. 2022. Vol. 10. P. 844–866. DOI: 10.1109/ACCESS.2021.3138353.
17. Shalabi K., Abu Al-Haija Q., Al-Fayoumi M. A. A blockchain-based intrusion detection/prevention systems in IoT network: a systematic review // Procedia Computer Science. 2024. Vol. 236. P. 410–419. DOI: 10.1016/j.procs.2024.05.048.
18. Alharthi H., Alshehri S., Kalkatawi M. Revolutionizing IoT security: a blockchain and federated learning-based anomaly detection system // In: Proceedings of the 2024 7th Artificial Intelligence and Cloud Computing Conference (AICCC '24). 2024. P. 565–572. DOI: 10.1145/3719384.3719466.
19. Al Sadi A., Mazzocca C., Melis A., Montanari R., Prandini M., Romandini N. P-IOTA: a cloud-based geographically distributed threat alert system that leverages P4 and IOTA // Sensors. 2023. Vol. 23, № 6. Article 2955. DOI: 10.3390/s23062955.
20. Lazzarini R., Tianfield H., Charissis V. Federated learning for IoT intrusion detection // AI. 2023. Vol. 4. №. 3. P. 509–530. DOI: 10.3390/ai4030028.
21. Ferrag M. A., Friha O., Maglaras L., Janicke H., Shu L. On the performance of federated learning algorithms for IoT // IoT. 2023. T. 3, № 2. C. 273–284. DOI: 10.3390/iot3020016.
22. Alsaedi A., Moustafa N., Tari Z., Mahmood A., Anwar A. Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures // Journal of Information Security and Applications. 2021. Vol. 58. Article 102413. DOI: 10.1016/j.jisa.2021.102413.
23. Khan M. A., Waseem M., Alshamrani N., Alharbi M., Alhazmi A. S., Zohdy A. M., Alattas F. A., Al Ghamdi A. Security considerations for Internet of Things: a survey // SN Computer Science. 2020. Vol. 1, no. 4. Article 193. DOI: 10.1007/s42979-020-00201-3.
24. Ceccarelli M., Zecchini M., Brighente A., Conti M. GitHub – MMw-Unibo/FETA: enabling federated learning at the edge through the IOTA Tangle [электронный ресурс]. URL: https://github.com/MMw-Unibo/FETA (дата обращения – 03.09.2025).
25. Tebueva F. B., Ryabtsev S. S., Ogur M. G., Andreev I. A., Goryainov S. A. Information Security Threat Model for Agents in Decentralized Internet of Things Environment, Formalizing Attack Scenarios on Trusted Interaction Information Security // Kuznechno-shtampovochnoe proizvodstvo. Obrabotka materialov davleniem. 2024. No. 11. pp. 220–232. (in Russian).