НАУЧНЫЙ ЖУРНАЛ
НАУКА И МИРОВОЗЗРЕНИЕ

УДК-004.056.5

ОЦЕНКА ЭФФЕКТИВНОСТИ МЕТОДА ЗАЩИТЫ ХРАНИЛИЩА ЗАДАНИЙ ДЛЯ РАСПРЕДЕЛЕННОЙ АСУ НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

Медведев Виктор Александрович
магистрант кафедры вычислительной техники и защиты информации,
Оренбургский государственный университет
РФ, г. Оренбург

Галимов Ринат Равильевич
научный руководитель, канд. техн. наук, доцент, Оренбургский государственный университет
РФ, г. Оренбург

Аннотация

Статья посвящена оценке эффективности применения технологии блокчейн для защиты хранилищ заданий в распределённых автоматизированных системах управления (АСУ). Рассматриваются различные аспекты использования блокчейн для обеспечения безопасности данных в условиях распределённой архитектуры, включая хранение, передачу и обработку заданий. Описание охватывает механизмы криптографической защиты, верификацию данных и предотвращение несанкционированного доступа. В статье также анализируются результаты применения предложенной модели в реальных условиях, а также сравнительный анализ с традиционными методами защиты данных в АСУ.

Ключевые слова: блокчейн, защита данных, распределённая АСУ, криптография, хранение данных, безопасность информации, распределённые системы.

1. Введение

В современных распределённых автоматизированных системах управления (АСУ) защита данных, особенно в отношении хранилищ заданий, играет ключевую роль в обеспечении их безопасности и целостности. Современные методы защиты, такие как традиционные системы шифрования и аутентификации, хотя и эффективны, но имеют свои ограничения, особенно в условиях высокой динамичности и масштабируемости распределённых систем. В последние годы одной из перспективных технологий для решения этой проблемы является блокчейн, который способен обеспечить надежную защиту данных с использованием криптографических методов и дистрибутивных протоколов.

2. Проблема и задачи защиты хранилищ заданий в распределённых АСУ

Распределённые АСУ, состоящие из множества узлов и облачных сервисов, требуют эффективных механизмов защиты данных, включая задачи по обеспечению конфиденциальности, целостности и доступности информации. Хранилища заданий, как часть этих систем, являются уязвимыми к различным типам атак, таким как несанкционированный доступ, изменение данных или утрата информации. Традиционные методы защиты, такие как централизованные базы данных или традиционные криптографические методы, могут быть недостаточны для обеспечения полной безопасности в таких системах.

В связи с этим важной задачей является разработка и внедрение нового метода защиты хранилищ заданий, который будет основываться на технологиях блокчейн, обеспечивая дистрибуцию и неизменность данных без централизованного контроля.

3. Метод защиты на основе технологии блокчейн

Технология блокчейн представляет собой распределённую базу данных, в которой информация сохраняется в виде блоков, каждый из которых связан с предыдущим, образуя цепочку. Такой подход гарантирует неизменность данных и делает их доступными только тем, кто имеет соответствующие права доступа. В контексте защиты хранилищ заданий для распределённой АСУ блокчейн может быть использован для обеспечения следующих ключевых аспектов:

3.1. Обеспечение целостности данных

Каждый блок в блокчейне содержит криптографическую подпись предыдущего блока, что гарантирует невозможность изменения данных без изменения всей цепочки. Это предотвращает несанкционированные изменения в хранилищах заданий, обеспечивая неизменность записей о выполненных или переданных заданиях.

3.2. Прозрачность и аудит

Технология блокчейн обеспечивает полную прозрачность всех операций с данными. Каждое изменение в хранилище заданий фиксируется в блоках и доступно для проверки любым уполномоченным пользователем. Это создаёт аудитируемую среду, где можно отслеживать всю историю изменений.

3.3. Децентрализация и отказоустойчивость

Использование блокчейн позволяет избежать централизованного контроля за хранилищем заданий. Каждый узел системы имеет доступ к полной копии данных, что делает систему более устойчивой к сбоям или атакам на центральный сервер. Кроме того, блокчейн-системы обеспечивают защиту от атак типа "отказ в обслуживании" (DoS) благодаря своей дистрибутивной природе.

3.4. Криптографическая защита

Для обеспечения безопасности передаваемых данных и их защиты от несанкционированного доступа используется криптография с открытым и закрытым ключами. Все записи в блокчейне могут быть зашифрованы, а доступ к данным предоставляется только авторизованным пользователям с соответствующими ключами.

4. Оценка эффективности метода

Для оценки эффективности применения блокчейн-технологий в защите хранилищ заданий был проведён ряд экспериментов и тестов в реальных условиях. Важными критериями эффективности являются:

4.1. Скорость обработки данных

Одним из важнейших параметров является скорость записи и извлечения данных из блокчейн-системы. В экспериментах было выявлено, что использование блокчейна может привести к небольшой задержке в процессе записи данных, однако это компенсируется высокой степенью безопасности и защиты от атак.

4.2. Безопасность

Использование блокчейна показало значительное улучшение в защите данных от атак. В частности, система продемонстрировала стойкость к типичным угрозам, таким как фальсификация данных и атаки на централизованные серверы.

4.3. Масштабируемость

Блокчейн-технология обладает хорошей масштабируемостью, позволяя эффективно работать с большими объемами данных в распределённых системах. Однако, с увеличением количества пользователей и узлов системы может возникнуть необходимость в оптимизации производительности блокчейн-структуры.

4.4. Стоимость

Хотя блокчейн-системы могут быть дороже в реализации по сравнению с традиционными методами защиты, их преимущества в обеспечении безопасности и децентрализации делают их более привлекательными для применения в распределённых АСУ.

5. Выводы

Метод защиты хранилищ заданий для распределённых АСУ на основе технологии блокчейн продемонстрировал свою эффективность в обеспечении целостности, безопасности и доступности данных.

Блокчейн предоставляет значительные преимущества по сравнению с традиционными методами, такими как централизованные базы данных или системы шифрования, обеспечивая децентрализацию и защиту от несанкционированных изменений данных. Тем не менее, существует необходимость в оптимизации скорости обработки данных и снижении стоимости реализации для более широкого внедрения технологии.

6. Литература

1. Nakamoto, S. "Bitcoin: A Peer-to-Peer Electronic Cash System." 2008.
2. Wood, G. "Ethereum: A Secure Decentralized Generalized Transaction Ledger." 2014.
3. Pilkington, M. "Blockchain Technology: Principles and Applications." 2016.
4. Tapscott, D., & Tapscott, A. "Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World." 2016.
5. Yermakov, M. A. "Blockchain: Principles, Technologies, Applications." 2020.