Гаджиев Г.К. Разработка систем автоматического распознавания атак на основе технологии блокчейн // Международный журнал информационных технологий и энергоэффективности.– 2025. –Т. 10 № 4(54) с. 29–33

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

РАЗРАБОТКА СИСТЕМ АВТОМАТИЧЕСКОГО РАСПОЗНАВАНИЯ АТАК НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

Гаджиев Г.К.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: gugac134@gmail.com

Статья посвящена исследованию применения технологии блокчейн для разработки систем автоматического распознавания кибератак. Раскрываются проблемы традиционных подходов к обнаружению угроз, такие как централизованность, уязвимость к манипуляциям с данными и ограниченная масштабируемость. Рассматриваются преимущества внедрения блокчейна, включая неизменяемость данных, децентрализацию, прозрачность и отказоустойчивость, а также возможности интеграции с методами искусственного интеллекта для анализа и предотвращения атак. Особое внимание уделяется вызовам, связанным с масштабируемостью и скоростью работы блокчейн-сетей, а также перспективам их развития в гибридных архитектурах. Отмечается, что применение блокчейна в системах автоматического распознавания атак открывает новые горизонты для повышения их безопасности, прозрачности и эффективности.

Ключевые слова: Блокчейн, кибербезопасность, автоматическое распознавание атак, децентрализация, неизменяемость данных, искусственный интеллект, системы обнаружения вторжений, масштабируемость, безопасность данных, распределённые реестры.

DEVELOPMENT OF AUTOMATIC ATTACK RECOGNITION SYSTEMS BASED ON BLOCKCHAIN TECHNOLOGY

Gadzhiev G.K.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: gugac134@gmail.com

The article is devoted to the study of the use of blockchain technology for the development of automatic recognition systems for cyber attacks. The problems of traditional approaches to threat detection, such as centralization, vulnerability to data manipulation, and limited scalability, are revealed. The advantages of blockchain implementation are considered, including data immutability, decentralization, transparency and fault tolerance, as well as the possibility of integration with artificial intelligence methods for analyzing and preventing attacks. Particular attention is paid to the challenges associated with the scalability and speed of blockchain networks, as well as the prospects for their development in hybrid architectures. It is noted that the use of blockchain in automatic attack recognition systems opens up new horizons for improving their security, transparency and efficiency.

Keywords: Blockchain, cybersecurity, automatic attack recognition, decentralization, data immutability, artificial intelligence, intrusion detection systems, scalability, data security, distributed ledgers.

Введение

С ростом интенсивности кибератак и их усложнением традиционные механизмы защиты информации уже не всегда обеспечивают надёжную защиту данных и инфраструктуры.

Современные атаки все чаще используют передовые технологии, включая машинное обучение и автоматизацию, что значительно усложняет их обнаружение и предотвращение. В этой связи наибольшую актуальность приобретает разработка систем автоматического распознавания атак, которые способны не только обнаружить угрозу, но и оперативно предоставить информацию для её нейтрализации. Одной из инновационных технологий, которые могут усилить эффективность таких систем, является блокчейн. Блокчейн уже доказал свою надёжность в задачах сохранения данных, обеспечивая их неизменность, верификацию и прозрачность. Применение блокчейн-технологий в области кибербезопасности, особенно для автоматического распознавания атак, открывает новые возможности для создания децентрализованных и устойчивых к манипуляциям систем.

Традиционные системы обнаружения атак.

Традиционные системы обнаружения атак, в том числе основанные на сигнатурах и аномалиях, имеют ряд существенных недостатков. Во-первых, централизованность делает их уязвимыми к атакам на саму систему мониторинга, поскольку злоумышленник, получив доступ к центру управления сетью, может скрыть свои действия. Во-вторых, такие системы сильно зависят от скорости обновления баз данных об угрозах и редко обеспечивают оперативное взаимодействие между различными частями инфраструктуры компаний. Кроме того, масштабируемость традиционных систем также вызывает затруднения: по мере роста сетей и объёмов данных их производительность существенно падает. В этом контексте блокчейн предоставляет уникальное преимущество за счёт своей децентрализованной архитектуры, неизменяемости записей и возможности функционирования без необходимости в едином доверительном центре [1].

Одной из ключевых особенностей блокчейна, способствующих его применению для автоматического распознавания атак, является его способность хранить данные об аномалиях и подозрительных действиях в неизменяемой структуре. Каждая запись в блокчейне подтверждается с помощью криптографических алгоритмов, что позволяет исключить возможность её изменения или удаления задним числом. Это свойство особенно важно для накопления исторических данных об атаках, что впоследствии может быть использовано при обучении систем машинного обучения или анализе сложных угроз. Данные, хранящиеся в блокчейне, могут включать информацию о подозрительных IP-адресах, паттерны аномального поведения сетевого трафика или уникальные сигнатуры вредоносного ПО. Децентрализованный механизм хранения также гарантирует, что даже в случае компрометации одной из точек системы обмануть всю сеть будет практически невозможно, так как контроль данных остается распределённым между множеством узлов [2-3].

Блокчейн может быть интегрирован в систему обнаружения атак двумя ключевыми способами. Во-первых, он может функционировать как база данных для хранения событий безопасности (Security Events), что обеспечивает прозрачность их обработки и неизменяемость собранной информации. Например, данные о сетевых аномалиях и попытках атак, зафиксированные системой обнаружения, записываются сразу в распределённый реестр, что исключает вероятность их подмены. Во-вторых, блокчейн можно использовать для координации действий между различными компонентами системы. Например, на основе данных об обнаруженных угрозах узлы сети могут автоматически обновлять свои механизмы

защиты, не прибегая к обращению в централизованный сервер. Таким образом, блокчейн способствует созданию полностью автономных систем обнаружения и предотвращения атак.

Автоматизация обнаружения атак с использованием блокчейн-технологий также активно поддерживается внедрением методов искусственного интеллекта. Современные алгоритмы анализа аномалий способны обнаруживать скрытые угрозы в реальном времени на основе огромного количества переменных данных. Однако для эффективного обучения таких алгоритмов необходимо большое количество качественных данных, которые не подвергались манипуляциям. Блокчейн в данном случае выполняет роль доверенной платформы, где хранятся "сырые" данные об атаках, доступные для анализа и обучения. Например, децентрализованные кибер-разведывательные платформы позволяют организациям делиться информацией о попытках атак, сохраняя анонимность и защищённость, а благодаря блокчейну гарантируется подлинность передаваемых данных.

Среди основных преимуществ применения блокчейн-технологии в системах автоматического распознавания атак выделяются неизменяемость данных, децентрализация, прозрачность деятельности и высокая отказоустойчивость. Неизменяемость данных обеспечивает точность анализа угроз, так как записи об угрозах нельзя удалить или модифицировать. Децентрализация устраняет необходимость в едином уязвимом центре управления, что делает систему устойчивой даже при компрометации отдельных узлов. Прозрачность позволяет организациям обмениваться данными об угрозах без необходимости устанавливать доверительные отношения между ними, а высокая отказоустойчивость обеспечивается тем, что для взлома системы злоумышленнику приходится одновременно атаковать множество узлов сети [4].

Однако, несмотря на эти преимущества, существуют и определённые вызовы, связанные с использованием блокчейна в системах обеспечения кибербезопасности. Первым из таких вызовов является проблема масштабируемости. Даже самые современные блокчейны, такие как Ethereum, всё ещё испытывают сложности с обработкой большого объёма транзакций при низкой пропускной способности, что ограничивает их применение в высоконагруженных кибербезопасных системах. Второй проблемой является задержка в работе сети: операции записи данных в блокчейн требуют времени для подтверждения, что может оказаться критичным фактором в средах, где требуется мгновенная реакция на атаки. Кроме того, несмотря на то что технология блокчейн обеспечивает неизменяемость данных, это также делает её уязвимой в случае, если вредоносные данные всё же были записаны в реестр, так как исправить ошибку становится практически невозможно.

С учётом текущих ограничений перспективы дальнейшего развития систем автоматического распознавания атак с использованием блокчейна связаны с внедрением гибридных архитектур и новых технологий [5]. Например, гибридные системы могут сочетать использование публичных блокчейнов для записи итоговых данных с применением частных распределённых реестров для быстрого реагирования на угрозы в реальном времени. Также активно развиваются решения второго уровня блокчейна, такие как свернутые цепочки и каналы обработки, которые могут значительно повысить скорость и производительность системы. Одновременно с этим продолжаются исследования в области интеграции блокчейн-сетей с технологиями интернета вещей (IoT) и искусственного интеллекта для разработки интеллектуальных адаптивных систем.

Заключение.

В заключение следует отметить, что развитие систем автоматического распознавания атак с использованием технологии блокчейн является перспективным направлением, способным поменять основные подходы к обеспечению кибербезопасности. Децентрализованность, надёжность и неизменяемость данных, предоставляемые блокчейн-технологиями, дают возможность создавать именно те системы защиты, которые способны противостоять современным видам атак, включая внедрение фальсифицированных данных и компрометацию узлов. Несмотря на сложные технологические вызовы, включая масштабируемость и задержки, дальнейшее развитие блокчейна и его адаптация к задачам автоматизации защиты помогут развивать новые стандарты в области кибербезопасности, делая системы обнаружения атак более быстрыми, надёжными и прозрачными.

Список литературы

1. Штеренберг, С. И. Компьютерные вирусы / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков. Том Часть 1. – Санкт-Петербург : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2015. –63с.– EDN CMMEML.
2. Катасонов А. И., Цветков А. Ю. Анализ механизмов разграничения доступа в системах специального назначения //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 563-568**.**
3. Суворов А. М., Цветков А. Ю. Исследование атак типа переполнение буфера в 64-х разрядных unix подобных операционных системах //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – С. 570-573**.**
4. Пестов И. Е. Методика разработки управляющего воздействия на инстансы облачной инфраструктуры //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – С. 72-76**.**
5. Казанцев А. А., Прохоров М. В., Худякова П. С. Обзор подходов к классификации текстов актуальными методами //Экономика и качество систем связи. – 2021. – №. 1 (19). – С. 57-67**.**

References

1. Shterenberg, S. I. Computer viruses / S. I. Shterenberg, A.V. Krasov, A. Y. Tsvetkov. Volume Part 1. – St. Petersburg : St. Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruevich, 2015. –63 p. - EDN CMMEML.
2. Katasonov A. I., Tsvetkov A. Yu. Analysis of access control mechanisms in special purpose systems //Actual problems of infotelec communications in science and education (APINO 2020). – 2020. – pp. 563-568.
3. Suvorov A.M., Tsvetkov A. Y. Investigation of buffer overflow attacks in 64-bit unix-like operating systems //Actual problems of infotelec communications in science and education (APINO 2018). – 2018. – pp. 570-573.
4. Pestov I. E. Methodology for developing control effects on cloud infrastructure instances //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. – 2020. – №. 4. – pp. 72-76.

5. Kazantsev A. A., Prokhorov M. V., Khudyakova P. S. Review of approaches to text classification by current methods //Economics and quality of communication systems. – 2021. – №. 1 (19). – pp. 57-67.