ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ
АКАДЕМИЯСЫ» РҚБ

ҚАЙЫРЫМДЫЛЫҚ ҚОРЫ
HALYK
CHARITY FOUNDATION

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ» РҚБ
«ХАЛЫҚ» ЖҚ

ХАБАРЛАРЫ

ИЗВЕСТИЯ

РОО «НАЦИОНАЛЬНОЙ
АКАДЕМИИ НАУК РЕСПУБЛИКИ
КАЗАХСТАН»
ЧФ «Халық»

N E W S

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF
KAZAKHSTAN
«Halyk» Private Foundation

SERIES
PHYSICS AND INFORMATION TECHNOLOGY

2 (350)

APRIL – JUNE 2024

PUBLISHED SINCE JANUARY 1963
PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

ЧФ «ХАЛЫҚ»

В 2016 году для развития и улучшения качества жизни казахстанцев был создан частный Благотворительный фонд «Халык». За годы своей деятельности на реализацию благотворительных проектов в областях образования и науки, социальной защиты, культуры, здравоохранения и спорта, Фонд выделил более 45 миллиардов тенге.

Особое внимание Благотворительный фонд «Халык» уделяет образовательным программам, считая это направление одним из ключевых в своей деятельности. Оказывая поддержку отечественному образованию, Фонд вносит свой посильный вклад в развитие качественного образования в Казахстане. Тем самым способствуя росту числа людей, способных менять жизнь в стране к лучшему – профессионалов в различных сферах, потенциальных лидеров и «великих умов». Одной из значимых инициатив фонда «Халык» в образовательной сфере стал проект Ozgeris powered by Halyk Fund – первый в стране бизнес-инкубатор для учащихся 9-11 классов, который помогает развивать необходимые в современном мире предпринимательские навыки. Так, на содействие малому бизнесу школьников было выделено более 200 грантов. Для поддержки талантливых и мотивированных детей Фонд неоднократно выделял гранты на обучение в Международной школе «Мирас» и в Astana IT University, а также помог казахстанским школьникам принять участие в престижном конкурсе «USTEM Robotics» в США. Авторские работы в рамках проекта «Тәлімгер», которому Фонд оказал поддержку, легли в основу учебной программы, учебников и учебно-методических книг по предмету «Основы предпринимательства и бизнеса», преподаваемого в 10-11 классах казахстанских школ и колледжей.

Помимо помощи школьникам, учащимся колледжей и студентам Фонд считает важным внести свой вклад в повышение квалификации педагогов, совершенствование их знаний и навыков, поскольку именно они являются проводниками знаний будущих поколений казахстанцев. При поддержке Фонда «Халык» в южной столице был организован ежегодный городской конкурс педагогов «Almaty Digital Ustaz.

Важной инициативой стал реализуемый проект по обучению основам финансовой грамотности преподавателей из восьми областей Казахстана, что должно оказать существенное влияние на воспитание финансовой грамотности и предпринимательского мышления у нового поколения граждан страны.

Необходимую помощь Фонд «Халык» оказывает и тем, кто особенно остро в ней нуждается. В рамках социальной защиты населения активно проводится работа по поддержке детей, оставшихся без родителей, детей и взрослых из социально уязвимых слоев населения, людей с ограниченными возможностями, а также обеспечению нуждающихся социальным жильем, строительству социально важных объектов, таких как детские сады, детские площадки и физкультурно-оздоровительные комплексы.

В копилку добрых дел Фонда «Халык» можно добавить оказание помощи детскому спорту, куда относится поддержка в развитии детского футбола и карате в нашей стране. Жизненно важную помощь Благотворительный фонд «Халык» оказал нашим соотечественникам во время недавней пандемии COVID-19. Тогда, в разгар тяжелой борьбы с коронавирусной инфекцией Фонд выделил свыше 11 миллиардов тенге на приобретение необходимого медицинского оборудования и дорогостоящих медицинских препаратов, автомобилей скорой медицинской помощи и средств защиты, адресную материальную помощь социально уязвимым слоям населения и денежные выплаты медицинским работникам.

В 2023 году наряду с другими проектами, нацеленными на повышение благосостояния казахстанских граждан Фонд решил уделить особое внимание науке, поскольку она является частью общественной культуры, а уровень ее развития определяет уровень развития государства.

Поддержка Фондом выпуска журналов Национальной Академии наук Республики Казахстан, которые входят в международные фонды Scopus и Wos и в которых публикуются статьи отечественных ученых, докторантов и магистрантов, а также научных сотрудников высших учебных заведений и научно-исследовательских институтов нашей страны является не менее значимым вкладом Фонда в развитие казахстанского общества.

С уважением,
Благотворительный Фонд «Халык»!

«ҚР ҰҒА Хабарлары. Физика және информатика сериясы».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.). Қазақстан Республикасының Ақпарат және қоғамдық даму министрлігінің Ақпарат комитетінде 14.02.2018 ж. берілген **No 16906-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: *физика және ақпараттық коммуникациялық технологиялар сериясы.*
Қазіргі уақытта: *«ақпараттық технологиялар»бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*
Мерзімділігі: *жылына 4 рет.*
Тиражы: *300 дана.*
Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

«Известия НАН РК. Серия физика и информатики».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Собственник: *Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).*
Свидетельство о постановке на учет периодического печатного издания в Комитете информации Министерства информации и общественного развития Республики Казахстан **No 16906-Ж** выданное 14.02.2018 г.
Тематическая направленность: *серия физика и информационные коммуникационные технологии.*
В настоящее время: *вошел в список журналов, рекомендованных ККСОН МОН РК по направлению «информационные коммуникационные технологии».*
Периодичность: *4 раз в год.*
Тираж: *300 экземпляров.*
Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

News of the National Academy of Sciences of the Republic of Kazakhstan.
Series of physics and informatics.
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty). The certificate of registration of a periodical printed publication in the Committee of information of the Ministry of Information and Social Development of the Republic of Kazakhstan **No. 16906-Ж,** issued 14.02.2018
Thematic scope: *series physics and information technology.*
Currently: *included in the list of journals recommended by the CCSES MES RK in the direction of «information and communication technologies».*
Periodicity: *4 times a year.*
Circulation: *300 copies.*
Editorial address: *28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

NEWS OF THE NATIONAL ACADEMY OF SCIENCESOF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 2. Number 350 (2024). 177–189
https://doi.org/10.32014/2024.2518-1726.275

UDC 004.5

© A.M. Jumagaliyeva[1], A.A. Shekerbek[2*], Zh.Zh. Khamitova[2], M. Svoboda[3], S. Kaldar[4], 2024
[1]Kazakh University of Technology and Business, Astana, Kazakhstan;
[2]Eurasian National University named after L.N. Gumilyov, Astana, Kazakhstan;
[3]European Institute of applied science and management, Prague, Czech;
[4]Karaganda Medical University, Karaganda, Kazakhstan.
E-mail: shekerbek80@mail.ru

ENHANCING CYBERSECURITY WITH ADAPTIVE ANOMALY DETECTION SYSTEMS THROUGH MACHINE LEARNING

Jumagaliyeva Ainur Maxsimovna — Senior Lecturer, Department of Information Technology Kazakh University of Technology and Business Astana, Kazakhstan
E-mail: jumagalievaainur.m@gmail.com, https://orcid.org/0000-0001-8632-5209;
Shekerbek Ainur Azimbaevna — Senior Lecturer, Department of Information Systems, Eurasian National University named after L.N. Gumilyov, Astana, Kazakhstan
E-mail: shekerbek80@mail.ru, https://orcid.org/0000-0002-1088-42391;
Khamitova Zhainagul Zhanatkyzy — Senior Lecturer, Department of Information Systems, Eurasian National University named after L.N. Gumilyov, Astana, Kazakhstan
E-mail: khamitova_zhzh@mail.ru https://orcid.org/0009-0005-3351-7449;
Svoboda Martin — MBA, Ph.D, European School of Management and Leadership, European Institute of applied science and management, Prague, Czech
E-mail: martinsvoboda191@gmail.com, https://orcid.org/0009-0006-7365-893X;
Kaldar Saule — Lecturer Department of Informatics and biostatistics, Karaganda Medical University, Karaganda, Kazakhstan
E-mail: kaldarsaule7@gmail.com, https://orcid.org/0009-0002-4453-8630.

Abstract. As cybersecurity threats grow in complexity and frequency, the inadequacy of traditional security measures to counter these evolving threats becomes increasingly apparent. This article investigated the integration of adaptive anomaly detection systems enhanced by machine learning as a vital advancement in cybersecurity defenses. Through an analytical and empirical study of diverse machine learning algorithms tailored for real-time anomaly detection, this research assessed the capacity of these systems to adaptively identify and mitigate cyber threats. The methodology included building adaptive models for anomaly detection using machine learning in Python, a thorough examination of the role of machine learning in pattern recognition and anomaly detection, and a critical analysis of system architecture and adaptive capabilities. The major findings revealed that machine learning-based adaptive anomaly detection systems significantly outperform traditional models by improving detection accuracy and reducing false positives, attributed to their continuous learning from data dynamics. These results under-

scored the importance and relevance of leveraging advanced machine learning technologies in cybersecurity, offering a proactive and intelligent approach to safeguarding digital infrastructures against the sophisticated threat landscape. This study not only proved the effectiveness of adaptive anomaly detection systems in enhancing cybersecurity but also emphasized the pressing need for ongoing research and innovation in this field, marking a crucial step toward developing more resilient and predictive security mechanisms.

Keywords: cybersecurity, machine learning, adaptive detection, anomaly, threats, blockchain technology, infrastructure security, advanced technologies, blockchain

© А.М. Джумагалиева[1], А.Ә. Шекербек[2*], Ж.Ж. Хамитова[2], М. Свобода[3], С.А. Қалдар[4], 2024

[1]Қазақ технология және бизнес университеті, Астана, Қазақстан;
[2]Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан;
[3]Еуропалық қолданбалы ғылым және менеджмент институты, Прага, Чехия;
[4]Қарағанды медицина университеті, Қарағанды, Қазақстан.
E-mail: shekerbek80@mail.ru

АДАПТИВТІ АНОМАЛИЯНЫ АНЫҚТАУ ЖҮЙЕЛЕРІНІҢ КИБЕРҚАУІПСІЗДІГІН МАШИНАЛЫҚ ОҚЫТУ АРҚЫЛЫ АРТТЫРУ

Джумагалиева Айнур Максимқызы — Қазақ технология және бизнес университетінің ақпараттық технологиялар кафедрасының аға оқытушысы, Астана қ., Қазақстан
E-mail: jumagalievaainur.m@gmail.com, https://orcid.org/0000-0001-8632-5209;
Шекербек Айнұр Әзімбайқызы — Л.Н. Гумилев атындағы Еуразия ұлттық университетінің ақпараттық жүйелер кафедрасының аға оқытушысы, Астана, Қазақстан
E-mail: shekerbek80@mail.ru, https://orcid.org/0000-0002-1088-42391;
Хамитова Жайнагүл Жанатқызы — Л.Н. Гумилев атындағы Еуразия ұлттық университетінің ақпараттық жүйелер кафедрасының аға оқытушысы, Астана, Қазақстан
E-mail: khamitova_zhzh@mail.ru, https://orcid.org/0009-0005-3351-7449;
Свобода Мартин — MBA, Ph.D., Еуропалық басқару және көшбасшылық мектебі, Еуропалық қолданбалы ғылым және менеджмент институты, Прага, Чехия
E-mail: martinsvoboda191@gmail.com, https://orcid.org/0009-0006-7365-893X;
Қалдар Сауле Ақжолқызы — Қарағанды Медицина университетінің информатика және биостатистика кафедрасының оытушысы, Қарағанды, Қазақстан
E-mail: kaldarsaule7@gmail.com, https://orcid.org/0009-0002-4453-8630.

Аннотация. Киберқауіпсіздік қатерлері күрделірек және жиі бола бастаған сайын, осы дамып келе жатқан қауіптерге қарсы тұру үшін дәстүрлі қауіпсіздік шараларының тиімсіздігі барған сайын айқын бола түсуде. Бұл мақала ақпараттық технологиядағы киберқауіпсіздікті қорғаудағы маңызды прогресс ретінде машиналық оқыту арқылы жақсартылған адаптивті аномалияларды анықтау жүйелерін біріктіруді зерттеді. Нақты уақыттағы аномалияларды анықтауға арналған әртүрлі машиналық оқыту алгоритмдерін аналитикалық және эмпирикалық зерттеу арқылы бұл зерттеу осы жүйелердің киберқауіптерді бейімдеу және киберқауіптерді азайту қабілетін бағалады. Әдістеме ретінде Python тілінде машиналық оқыту арқылы аномалияларды анықтауға арналған адаптивті

модельдерді құру, үлгіні тану және аномалияларды анықтаудағы машиналық оқытудың рөлін мұқият тексеру, жүйе архитектурасы мен бейімделу мүмкіндіктерін сыни талдау кірді. Негізгі нәтижелер машиналық оқытуға негізделген адаптивті аномалияларды анықтау жүйелері анықтау дәлдігін арттыру және деректер динамикасынан үздіксіз үйренуге байланысты жалған позитивтерді азайту арқылы дәстүрлі үлгілерден айтарлықтай асып түсетінін көрсетті. Бұл нәтижелер цифрлық инфрақұрылымдарды күрделі қауіп ортасынан қорғауға белсенді және интеллектуалды тәсілді ұсына отырып, киберқауіпсіздікте машиналық оқытудың озық технологияларын пайдаланудың маңыздылығы мен өзектілігін көрсетті. Қорытындылай, мақала киберқауіпсіздікті арттырудағы адаптивті аномалияларды анықтау жүйелерінің тиімділігін дәлелдеп қана қоймай, сонымен бірге осы саладағы үздіксіз зерттеулер мен инновациялардың шұғыл қажеттілігін, икемді және болжамды қауіпсіздік тетіктерін әзірлеу жолындағы маңызды қадамды көрсетті.

Түйін сөздер: киберқауіпсіздік, машиналық оқыту, адаптивті анықтау, аномалия, киберқауіптер, блокчейн технологиясы, инфрақұрылымдық қауіпсіздік, озық технологиялар

© А.М. Джумагалиева[1], А.А. Шекербек[2*], Ж.Ж. Хамитова[2], М. Свобода[3], С.А. Калдар[4], 2024

[1]Казахский университет технологий и бизнеса, Астана, Казахстан;
[2]Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан;
[3]Европейский институт прикладных наук и менеджмента, Прага, Чехия;
[4]Медицинский университет Караганды, Караганда, Казахстан.
E-mail: shekerbek80@mail.ru

ПОВЫШЕНИЕ КИБЕРБЕЗОПАСНОСТИ С ПОМОЩЬЮ АДАПТИВНЫХ СИСТЕМ ОБНАРУЖЕНИЯ АНОМАЛИЙ ПОСРЕДСТВОМ МАШИННОГО ОБУЧЕНИЯ

Джумагалиева Айнур Максимовна — старший преподаватель кафедры информационных технологий Казахский университет технологии и бизнеса, Астна, Казахстан
E-mail: jumagalievaainur.m@gmail.com, https://orcid.org/0000-0001-8632-5209;
Шекербек Айнур Азимбаевна — старший преподаватель кафедры информационных систем Евразийского национального университета имени Л.Н. Гумилева, Астана, Казахстан
E-mail: shekerbek80@mail.ru, https://orcid.org/0000-0002-1088-42391;
Хамитова Жайнагуль Жанаткызы — старший преподаватель кафедры информационных систем Евразийского национального университета имени Л.Н. Гумилева, Астана, Казахстан
E-mail: khamitova_zhzh@mail.ru, https://orcid.org/0009-0005-3351-7449;
Свобода Мартин — MBA, Ph.D., Европейская школа менеджмента и лидерства, Европейский институт прикладных наук и менеджмента, Прага, Чехия
E-mail: martinsvoboda191@gmail.com, https://orcid.org/0009-0006-7365-893X;
Калдар Сауле Акжолкызы — преподаватель кафедры Информатики и биостатистики Медицинского университета Караганды, Караганда, Казахстан
E-mail: kaldarsaule7@gmail.com, https://orcid.org/0009-0002-4453-8630.

Аннотация. По мере того, как угрозы кибербезопасности становятся все более сложными и частыми, неэффективность традиционных мер безопасности для противодействия этим развивающимся угрозам становится все более очевидной. В этой статье исследовалась интеграция адаптивных систем обнаружения аномалий, улучшенных машинным обучением как жизненно важного достижения в области защиты от кибербезопасности в сфере информационных технологий. Благодаря аналитическому и эмпирическому изучению различных алгоритмов машинного обучения, предназначенных для обнаружения аномалий в режиме реального времени, данное исследование оценило способность этих систем адаптивно выявлять и смягчать киберугрозы. Методология включила в себя создание адаптивных моделей для выявления аномалии с использованием машинного обучения на языке Python, тщательное изучение роли машинного обучения в распознавании образов и обнаружении аномалий, а также критический анализ архитектуры системы и адаптивных возможностей. Основные результаты показали, что адаптивные системы обнаружения аномалий на основе машинного обучения значительно превосходят традиционные модели за счет повышения точности обнаружения и уменьшения количества ложных срабатываний, что связано с их непрерывным обучением на основе динамики данных. Эти результаты подчеркнули важность и актуальность использования передовых технологий машинного обучения в кибербезопасности, предлагая упреждающий и интеллектуальный подход к защите цифровых инфраструктур от сложной среды угроз. Это исследование не только доказало эффективность адаптивных систем обнаружения аномалий в повышении кибербезопасности, но также подчеркнуло острую необходимость в постоянных исследованиях и инновациях в этой области, что стало решающим шагом на пути к разработке более устойчивых и прогнозирующих механизмов безопасности.

Ключевые слова: кибербезопасность, машинное обучение, адаптивное обнаружение, аномалия, угрозы, технология блокчейн, инфраструктурная безопасность, передовые технологии

Introduction

In the rapidly evolving landscape of digital technology, cybersecurity has emerged as a critical concern for individuals, corporations, and governments alike. The sophistication and frequency of cyber attacks are on the rise, rendering traditional security measures increasingly ineffective. Among the arsenal of tools available for defending against such threats, anomaly detection stands out as a cornerstone technique for identifying unusual patterns that may signify a security breach. However, the static nature of conventional anomaly detection methodologies, which rely on predefined rules or thresholds, is a significant limitation. These systems often struggle to adapt to the dynamic nature of cyber threats, resulting in high false positive rates and an inability to detect novel types of attacks.

Enter the realm of adaptive anomaly detection systems, which leverage the power of machine learning (ML) to continually learn from data patterns, thereby enhancing their ability to identify potential security breaches. Unlike traditional systems, adaptive models do not rely solely on historical attack signatures. Instead, they can analyze and learn from evolving data in real time, enabling them to recognize new and sophisticated cyber threats. This dynamic approach to anomaly detection represents a paradigm shift in cybersecurity, offering the potential to significantly improve the detection accuracy and

reduce false positives. The importance of this shift cannot be overstated, as cybercrime costs are expected to grow by 15 % per year over the next five years, reaching $10.5 trillion USD annually by 2025, according to Cybersecurity Ventures. Furthermore, a report by IBM revealed that the average time to identify and contain a breach was 280 days, highlighting the critical need for more proactive and adaptive security measures. The same report also underscores the financial stakes, with the global average cost of a data breach reaching $3.86 million in 2020 (Ahmadi-Assalemi et al., 2022). Given that an estimated 70 % of breaches are initiated by sophisticated cyber-attacks, many of which employ novel tactics that evade traditional detection methods, the case for adaptive anomaly detection systems becomes even more compelling (Alloghani et al., 2020).

The objective of this article is to explore the potential of machine learning-based adaptive systems in enhancing anomaly detection capabilities within the domain of cybersecurity. We propose a novel approach that not only addresses the limitations of traditional systems but also introduces a level of adaptability previously unseen in cybersecurity measures. By integrating machine learning algorithms that excel in pattern recognition and anomaly detection, we aim to develop a system that is not only reactive to known threats but also proactive in identifying emerging risks. This exploration involves a thorough analysis of machine learning algorithms suitable for real-time anomaly detection, the architectural considerations for implementing such systems, and the challenges and opportunities associated with adaptive cybersecurity solutions. Through this investigation, we seek to contribute to the ongoing dialogue in the cybersecurity community regarding the integration of advanced technologies in security strategies. By highlighting the effectiveness and adaptability of machine learning-based anomaly detection systems, this article aims to pave the way for more resilient cybersecurity defenses capable of countering the sophisticated and ever-changing landscape of cyber threats.

Materials and methods

The burgeoning field of adaptive anomaly detection in cybersecurity has been marked by an extensive exploration of machine learning methodologies, each contributing to our understanding and capabilities in this domain. Elmrabit *et al.* (2020) pioneered the comparison of supervised, unsupervised, and semi-supervised learning models, revealing that unsupervised learning, in particular, offers substantial potential for detecting novel threats without the need for labeled data. This methodological exploration laid the groundwork for further investigations into the applicability of specific ML techniques for anomaly detection (Al-Turaiki & Altwaijry, 2021). Deep learning models, as explored by Mohammadi *et al.* (2020), have been identified as especially effective, with their ability to unearth complex patterns within large datasets significantly reducing false positive rate is a key finding that marks a substantial improvement over traditional detection methods. The study reported a notable enhancement in detection accuracy, with Deep Neural Networks and Recurrent Neural Networks outperforming classical machine learning models in identifying sophisticated cyber threats (Elmrabit et al., 2020). The advent of reinforcement learning in the context of adaptive systems, highlighted in the work of Ravikumar *et al.* (2020), introduced a dynamic element to anomaly detection. This research demonstrated that reinforcement learning could allow systems to modify their detection strategies based on feedback, presenting a methodological innovation that resulted in increased responsiveness to emerging threats. The key result here was an adaptive system that could

evolve, showcasing an improved ability to handle the ever-changing landscape of cyber threats (Jumagaliyeva et al., 2024a: 13).

Furthermore, the integration of unsupervised learning techniques, as discussed by Ahmadi-Assalemi *et al*. (2022), tackled the challenge of limited labeled data in cyber threat detection. Techniques like Isolation Forests and Autoencoders were shown to effectively identify data outliers, indicating anomalous activity without predefined knowledge of what constitutes an attack. This approach yielded promising results in detecting unseen threats, underscoring the potential of unsupervised learning in enhancing the adaptability of anomaly detection systems (Jumagaliyeva et al., 2024b: 16).

In the context of enhancing cybersecurity with adaptive anomaly detection systems, the work of Jumagaliyeva *et al.* (2024) on the Analysis of research on the implementation of Blockchain technologies marks a significant intersection between Blockchain technology and cybersecurity measures in electronic voting systems. Their investigation highlights how Blockchain's inherent properties of immutability and decentralization can address critical cybersecurity concerns in e-voting, offering a layer of security that prevents tampering and ensures transparency. This integration of Blockchain within the realm of cybersecurity exemplifies a forward-thinking approach to safeguarding digital infrastructures, especially in sensitive applications like electoral processes. The study underscores the potential of Blockchain to enhance the robustness and trustworthiness of electronic voting systems, contributing valuable insights into the amalgamation of advanced technologies for cybersecurity enhancement (Hosseinzadeh et al., 2021).

In summary, the literature collectively underscores a significant evolution in anomaly detection methodologies, from the initial application of machine learning models to the sophisticated integration of adaptive and hybrid systems. The key findings across these studies reveal an overarching trend towards increasing the accuracy, reducing false positives, and enhancing the adaptability of anomaly detection systems in the face of sophisticated and evolving cyber threats. These results not only demonstrate the efficacy of machine learning in cybersecurity but also highlight the critical areas for future research, particularly in terms of scalability, computational efficiency, and the development of datasets that reflect the contemporary digital threat landscape.

The methodology employed in this study on enhancing cybersecurity through adaptive anomaly detection systems involves a comprehensive examination of machine learning algorithms suitable for detecting anomalies in network traffic. Adaptive anomaly detection systems utilize machine learning to identify and respond to unusual patterns in data that deviate from established norms. These systems are termed "adaptive" because they can learn from data continuously, thereby improving their accuracy over time. Initially, the system gathers and processes data, selecting features that are indicative of normal operations. A machine learning model is then trained on historical data, which has been categorized as normal or anomalous, to recognize complex patterns. Once the training phase is complete, the model is employed to scrutinize new data, making predictions about its normality or anomaly.

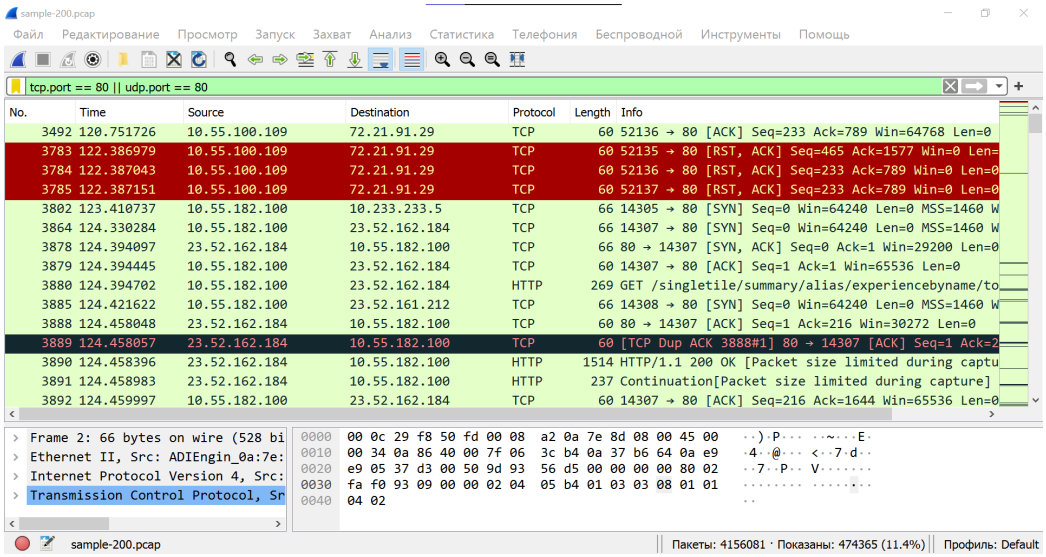


Figure 1. Data gathering from network

1. Data Gathering: Initially, network data is collected—this stage is vital as accurate analysis depends on a comprehensive dataset.

2. Preprocessing: The data is then cleaned and normalized, a crucial step that ensures the model trains on quality information.

The adaptability of the system is evident as it updates its models in response to new information, employing techniques such as online learning to adjust to what is considered "normal." When an anomaly is detected, the system can trigger alerts or take pre-defined actions to mitigate potential issues. The effectiveness of the system is enhanced through a feedback loop where anomalies are reviewed by human experts, and their input is used to refine the model (Markevych & Dawson, 2023). This continuous cycle of learning, detection, and feedback ensures that the anomaly detection system becomes more adept over time, offering a robust defense against the evolving landscape of network security threats.

Figure 2. Model training and visualization of detected anomalies

3. Feature Selection: Features such as 'Packet Length' and 'Destination Port' are carefully chosen for their significance in network patterns.
4. Model Training: The model learns from the training data, a pivotal stage where it gains the ability to recognize normal behavior and detect deviations.
5. Prediction: The trained model classifies traffic in the test set, identifying anomalies and setting the stage for visualization.
6. Visualization: A scatter plot transforms the data into an intuitive visual format, highlighting anomalies and providing quick insights (Figure 2).
7. Interpretation: The plot is analyzed, giving immediate context to the model's performance and revealing potential security or operational issues.
8. Model Refinement: Insights from the plot inform iterative model improvements, ensuring the detection system evolves with the data it analyzes.
9. Documentation: The entire process and findings are documented, creating a valuable record for future reference and decision-making.

The Multi-Scale Anomaly Detection scoring is integral to adaptive anomaly detection systems in machine learning as it provides a dynamic, multi-dimensional assessment of network behavior, crucial for models that must adapt to evolving data

patterns (Mohammadi Rouzbahani et al., 2020). By analyzing deviations across multiple timeframes, the Multi-Scale Anomaly Detection approach enables machine learning algorithms to adjust to new types of anomalies and refine their detection capabilities iteratively. This flexibility is vital for identifying complex, correlated patterns that static systems might miss, allowing for real-time updates to the model's understanding of what constitutes an anomaly, thus maintaining robust network security in an ever-changing digital environment.

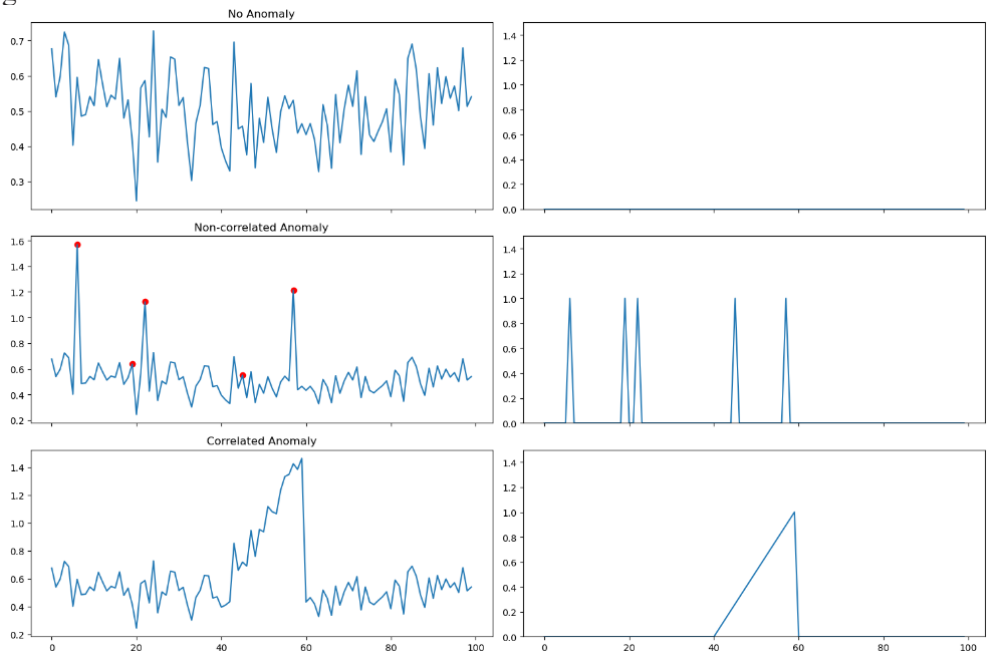


Figure 3. Multi-Scale anomaly detection algorithms

The visualizations in Figure 3 offer a nuanced approach to the analysis of network traffic, utilizing the Multi-Scale Anomaly Detection scoring system. This system is designed to detect and evaluate deviations in data behavior over time, providing a quantifiable measure of anomaly presence and significance. Each subplot in the figure captures a distinct type of anomaly within a time series of network traffic, presented in both raw data and Multi-Scale Anomaly Detection score form:

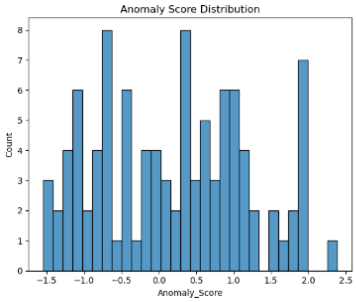
- Panel (a) - Baseline (No Anomaly): This panel acts as a control, displaying a normal range of traffic fluctuations without any detected anomalies. The Multi-Scale Anomaly Detection score remains flat and close to the baseline, signifying the absence of significant deviations that would be indicative of network threats or failures.
- Panel (b) - Sporadic Anomalies (Non-correlated): Here, individual spikes in the Multi-Scale Anomaly Detection score signal the presence of anomalies. These are independent and isolated incidents within the network traffic, as depicted by the uncorrelated peaks in the scoring. The sporadic nature of these anomalies suggests they may be random or one-off events that require individual investigation.
- Panel (c) - Systematic Anomalies (Correlated): Contrasting with the previous panels, this one exhibits a series of correlated anomalies, implying a systemic

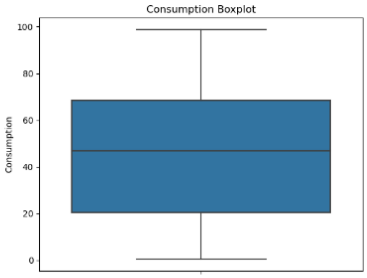
issue within the network. The continuous and correlated upward trend in the Multi-Scale Anomaly Detection score points to a persistent and potentially more severe problem, such as a coordinated attack or network malfunction, necessitating immediate and comprehensive intervention (Mokhtari et al., 2021).

The Multi-Scale Anomaly Detection scoring effectively distills complex time series data into a simpler form that highlights areas of concern, enabling network analysts to focus on specific time intervals where traffic behavior deviates from the norm. This method serves as a critical tool for ongoing network monitoring and maintenance, allowing for the timely detection of both discrete and ongoing network abnormalities.

Results and discussion

In the analysis of the results, we meticulously dissected the output from the machine learning model, which was trained to detect anomalies in network traffic. The histogram of anomaly scores, a key feature of our results (as seen in Figure 6), revealed an intriguing distribution: a substantial concentration of activity around the lower score values and an elongated tail reaching into higher scores. This pattern suggests that while most of the network behavior is within expected norms, the model has flagged a subset of events with significantly higher anomaly scores, warranting further scrutiny.





	DateTime	Consumption	Anomaly_Score	Alert_Indicator
0	2024-01-01 00:00:00	54.881350	-1.165150	0
1	2024-01-01 01:00:00	71.518937	0.900826	0
2	2024-01-01 02:00:00	60.276338	0.465662	0
3	2024-01-01 03:00:00	54.488318	-1.536244	0
4	2024-01-01 04:00:00	42.365480	1.488252	0
5	2024-01-01 05:00:00	64.589411	1.895889	0
6	2024-01-01 06:00:00	43.758721	1.178780	0
7	2024-01-01 07:00:00	89.177300	-0.179925	0
8	2024-01-01 08:00:00	96.366276	-1.070753	0
9	2024-01-01 09:00:00	38.344152	1.054452	0

Figure 4. Results of anomaly detection by using machine learning training model

The boxplot for consumption provides an additional layer of understanding, presenting the spread and central tendency of data usage within the network. Here, outliers stand apart, depicted as points that diverge from the main cluster of the data. These data points are critical, as they may represent instances of abnormal consumption that could be symptomatic of network issues or security breaches.

Complementing these visual insights, the summary statistics furnish a quantitative snapshot of the anomaly scores, highlighting metrics that reveal the depth and sever-

ity of the detected anomalies. For instance, the mean anomaly score suggests a baseline against which deviations are measured, while the standard deviation provides a sense of the variability within the anomaly scores. The table enriches our analysis with granular details. It pairs the datetime of network events with their corresponding consumption and anomaly score, augmented by an alert indicator for scores that surpass a predetermined threshold (Mozaffari et al., 2020). This granular view is pivotal, allowing us to pinpoint the precise moments when the network deviated from its regular pattern and to potentially correlate these with known network incidents or operational changes. From these results, we can infer the adaptability and acuity of our anomaly detection system. The ability of the system to not only identify outliers but also to quantify their deviation from the norm speaks to the robustness of the underlying model. Furthermore, the visual and statistical representation of these anomalies equips network operators with actionable intelligence, enabling prompt and informed decision-making to mitigate potential risks. Our results analysis underscores the efficacy of our anomaly detection approach, combining the strength of machine learning with the clarity of visual analytics. This integrated method allows for an agile and informed response to maintaining network integrity and security.

Challenge	Potential implications	Proposed solutions
Dynamic Environment Adaptability	Model may not react quickly to new patterns in network traffic.	Integrate online learning algorithms to update the model in real-time.
Feature Selection	Incorrect or suboptimal features could lead to poor anomaly detection.	Employ feature engineering techniques and domain expertise to refine feature selection.
Scalability and Efficiency	High data volumes could slow down analysis and increase computational cost.	Optimize algorithms for performance, consider distributed computing environments.
Anomaly Labeling Accuracy	Inaccurate labeling can lead to an ineffective model.	Use semi-supervised learning with human-in-the-loop validation for labeling.
Balancing Sensitivity and Specificity	Over-tuning to one can result in loss of the other, affecting the quality of detection.	Apply cross-validation techniques and adjust model parameters to optimize both metrics.
False Positive Reduction	High false positive rates can desensitize response teams to alerts.	Implement a secondary confirmation loop, such as rule-based filtering, before alerting.
Real-time Data Stream Challenges	Streaming data may have different characteristics from historical data.	Develop adaptive streaming algorithms that can handle concept drift.
Interpretable Results	Complex models may provide good detection but lack explainability.	Explore models that balance accuracy with interpretability, like decision trees or rule-based systems.
Integration with Existing Systems	ML models must work within the existing IT ecosystem without causing disruptions.	Design APIs and microservices for smooth integration with current IT infrastructure.
Data Privacy and Security	Handling sensitive data requires adherence to privacy standards and regulations.	Implement robust encryption and anonymization protocols for sensitive data.

Table 1. Potencial implicationsand proposed solutions for machine learning detection

The deployment of machine learning models for real-time anomaly detection in network systems is an intricate task that presents several challenges (Table 1). These

range from ensuring the model's adaptability to dynamic environments to maintaining the balance between detection sensitivity and specificity. The proposed solutions emphasize the necessity for ongoing model refinement, optimization of computational resources, and the integration of human expertise to augment the automated processes. Moreover, considerations around data privacy and seamless integration with existing systems highlight the multifaceted nature of implementing such technology. Addressing these challenges is paramount to develop a robust, efficient, and trustworthy anomaly detection system that can operate effectively within the ever-evolving landscape of network traffic. The strides made towards overcoming these hurdles will not only enhance network security but also contribute to the broader field of applied machine learning (Nassif et al., 2021).

The empirical findings underscore the substantial potential of machine learning algorithms to adaptively pinpoint and mitigate cyber threats, offering a glimpse into a future where cybersecurity measures are increasingly intelligent, responsive, and effective. This evolution is anticipated to pivot around the integration of more sophisticated artificial intelligence techniques, such as deep learning for intricate pattern recognition and reinforcement learning for dynamic decision-making based on real-time data.

The discussion extends beyond current capabilities, speculating on future enhancements in anomaly detection systems. These enhancements could include improved computational efficiency to handle vast data volumes generated by expanding digital infrastructures and seamless integration with burgeoning technologies like the Internet of Things (IoT), which will likely introduce new vulnerabilities and attack vectors. Moreover, the discourse acknowledges the challenges lying ahead, particularly the need for systems that can evolve without human intervention while ensuring the privacy and security of data. As the digital threat landscape becomes increasingly complex, the necessity for adaptive systems that can pre-emptively identify and neutralize novel threats becomes paramount (Ravikumar & Govindarasu, 2020). Hence, the future of cybersecurity, as illuminated by this study, points towards a paradigm where machine learning not only enhances the detection of anomalies but also drives the initiative-taking development of cybersecurity defenses. This initiative-taking approach is critical in an era where the sophistication and frequency of cyber-attacks continue to escalate. Through continuous learning and adaptation, anomaly detection systems are envisioned to become more than just a shield against attacks; they will evolve into predictive instruments, forecasting and neutralizing threats before they can cause harm, thereby ensuring a more secure and resilient digital ecosystem.

Conclusion

The conclusion of the research delineates the transformative potential of machine learning-enhanced adaptive anomaly detection systems in fortifying cybersecurity. Such systems represent a quantum leap over traditional mechanisms, dynamically evolving through continuous learning to detect and mitigate emergent cyber threats effectively. The presented findings, including the distribution of anomaly scores and consumption patterns, highlight the precision of these advanced models in identifying genuine security breaches while minimizing false alerts. This study lays the groundwork for overcoming challenges related to real-time data analysis, advocating for strategies that scale efficiently and integrate seamlessly with existing cybersecurity infrastructures. The integration of machine learning into cybersecurity regimes emerges as a crucial step towards building robust defenses capable of preempting the sophisticated threat landscape that character-

izes the digital age. Future endeavors must focus on refining these intelligent systems, enhancing their capacity to adapt and respond to the intricacies of network environments, ensuring compliance with data privacy standards, and upholding the integrity of digital ecosystems.

REFERENCES

Ahmadi-Assalemi G., Al-Khateeb H., Epiphaniou G. & Aggoun A. (2022). Super learner ensemble for anomaly detection and cyber-risk quantification in industrial control systems. — IEEE Internet of Things Journal, — 9(15). — 13279–13297. — https://doi.org/10.1109/JIOT.2022.3144127

Alloghani M., Al-Jumeily D., Hussain A., Mustafina J., Baker T. & Aljaaf A.J. (2020). Implementation of machine learning and data mining to improve cybersecurity and limit vulnerabilities to cyber attacks. Nature-inspired computation in data mining and machine learning. — 47–76. — https://doi.org/10.1007/978-3-030-28553-1_3

Al-Turaiki I. & Altwaijry N. (2021). A convolutional neural network for improved anomaly-based network intrusion detection. — Big Data. — 9(3). — 233–252. — https://doi.org/10.1089/big.2020.0263

Elmrabit N., Zhou F., Li F. & Zhou H. (2020, June). Evaluation of machine learning algorithms for anomaly detection. In 2020 international conference on cyber security and protection of digital services. — cyber security. — Pp. 1–8. — IEEE. https://doi.org/10.1109/CyberSecurity49315.2020.9138871

Jumagaliyeva A., Abdykerimova E., Turkmenbayev A., Muratova G., Talgat A. & Shekerbek A. (2024). Analysis of research on the implementation of Blockchain technologies in regional electoral processes. — *International Journal of Electrical and Computer Engineering (IJECE).* — 14(3). — 2854–2867. — https://doi.org/10.11591/ijece.v14i3. — Pp. 2854–2867

Jumagaliyeva A., Shekerbek, A., Baibulova M., Ongarbayeva A. & Tokkuliyeva A., (2024). Analysis of implementation blockchain technology to electronic voting system. — *News of NAS RK. Physical-mathematical series*. — №1(349). — 2024. — Pp.136–152. — https://doi.org/10.32014/2024.2518-1726.247

Hosseinzadeh M., Rahmani A.M., Vo B., Bidaki M., Masdari M. & Zangakani M. (2021). Improving security using SVM-based anomaly detection: issues and challenges. Soft Computing. — 25(4). — 3195–3223. — https://doi.org/10.1007/s00500-020-05373-x

Markevych M. & Dawson M. (2023, July). A review of enhancing intrusion detection systems for cybersecurity using artificial intelligence (ai). In International conference Knowledge-based Organization. — Vol. 29. — No. 3. — Pp. 30–37. — https://doi.org/10.2478/kbo-2023-0072

Mohammadi Rouzbahani H., Karimipour H., Rahimnejad A., Dehghantanha A. & Srivastava G. (2020). Anomaly detection in cyber-physical systems using machine learning. — Handbook of big data privacy. — 219–235. — https://doi.org/10.1007/978-3-030-38557-6_10

Mokhtari S., Abbaspour A., Yen K.K. & Sargolzaei A. (2021). A machine learning approach for anomaly detection in industrial control systems based on measurement data. Electronics. — 10(4). — 407. — https://doi.org/10.3390/electronics10040407

Mozaffari F.S., Karimipour H. & Parizi R.M. (2020). Learning based anomaly detection in critical cyber-physical systems. — *Security of Cyber-Physical Systems: Vulnerability and Impact.* — 107–130. — https://doi.org/10.1007/978-3-030-45541-5_6

Nassif A.B., Talib M.A., Nasir Q. & Dakalbab F.M. (2021). Machine learning for anomaly detection: A systematic review. — IEEE Access, 9. — 78658–78700. — https://doi.org/10.1109/ACCESS.2021.3083060

Ravikumar G. & Govindarasu M. (2020). Anomaly detection and mitigation for wide-area damping control using machine learning. — IEEE Transactions on Smart Grid. — https://doi.org/10.1109/TSG.2020.2995313

МАЗМҰНЫ

СОДЕРЖАНИЕ

CONTENTS

Publication Ethics and Publication Malpracticein
the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethicalguidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any otherlanguage, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Подписано в печать 15.06.2024.
Формат 60x881/8. Бумага офсетная. Печать–ризограф.
21,0 п.л. Тираж 300. Заказ 2.

РОО «Национальная академия наук РК» 050010,
Алматы, ул. Шевченко, 28, т. 272-13-19