ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE REPUBLIC OF KAZAKHSTAN

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

2024 (18) 2

сәуір – маусым

ISSN 2708–2032 (print)
ISSN 2708–2040 (online)

Халықаралық ақпараттық және коммуникациялық технологиялар журналы
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Меншіктенуші: «Халықаралық ақпараттық технологиялар университеті» АҚ (Алматы қ.).
Қазақстан Республикасы Ақпарат және әлеуметтік даму министрлігінің Ақпарат комитетінде – **20.02.2020** жылы берілген.
№ KZ82VPY00020475 мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: ақпараттық технологиялар, әлеуметтік-экономикалық жүйелерді дамытудағы цифрлық технологиялар, ақпараттық қауіпсіздік және коммуникациялық технологияларға арналған.
Мерзімділігі: жылына 4 рет.
Тиражы: 100 дана
Редакцияның мекенжайы: 050040, Алматы қ-сы, Манас к-сі, 34/1, 709-кабинет, тел: +7 (727) 244-51-09.
E-mail: ijict@iitu.edu.kz Журнал сайты: https://journal.iitu.edu.kz

Международный журнал информационных и коммуникационных технологий
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Собственник: АО «Международный университет информационных технологий» (г. Алматы).
Свидетельство о постановке на учет периодического печатного издания в Министерство информации и общественного развития Республики Казахстан **№ KZ82VPY00020475,** выданное от **20.02.2020 г.**
Тематическая направленность: информационные технологии, информационная безопасность и коммуникационные технологии, цифровые технологии в развитии социо-экономических систем**.**
Периодичность: 4 раза в год.
Тираж: 100 экземпляров.
Адрес редакции: 050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09.
E-mail: ijict@iitu.edu.kz Сайт журнала: https://journal.iitu.edu.kz

---

«International Journal of Information and Communication Technologies»
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Owner: International Information Technology University JSC (Almaty).
The certificate of registration of a periodical printed publication in the Ministry of Information and Social Development of the Republic of Kazakhstan, Information Committee No. KZ82VPY00020475, issued on 20.02.2020.
Thematic focus: information technology, digital technologies in the development of socio-economic systems, information security and communication technologies
Periodicity: 4 times a year.
Circulation: 100 copies.
Editorial address: 050040. Manas st. 34/1, Almaty. +7 (727) 244-51-09. E-mail: ijict@iitu.edu.kz
Journal website: https://journal.iitu.edu.kz

МАЗМҰНЫ

ӘЛЕУМЕТТІК-ЭКОНОМИКАЛЫҚ ЖҮЙЕЛЕРДІ ДАМЫТУДАҒЫ ЦИФРЛЫҚ ТЕХНОЛОГИЯЛАР

АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР

СОДЕРЖАНИЕ

ЦИФРОВЫЕ ТЕХНОЛОГИИ В РАЗВИТИИ СОЦИО-ЭКОНОМИЧЕСКИХ СИСТЕМ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

CONTENTS

DIGITAL TECHNOLOGIES IN THE DEVELOPMENT OF SOCIO-ECONOMIC SYSTEMS

INFORMATION TECHNOLOGY

АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

INFORMATION TECHNOLOGY

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 5. Is. 2. Number 18 (2024). Pp. 70–83
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2024.18.2.007

HARNESSING ARTIFICIAL INTELLIGENCE FOR ADVANCED THREAT DETECTION IN NETWORK INFRASTRUCTURES

G. Alin*, A. Konsbayev, N. Abdikaparov
E-mail: g.alin@iitu.edu.kz

Alin Galymzada — Department of Cybersecurity International Information Technology University, Almaty Kazakhstan
E-mail: g.alin@iitu.edu.kz
Konsbayev Almas — Department of Cybersecurity International Information Technology University, Almaty Kazakhstan
E-mail: 38454@iitu.edu.kz
Abdikaparov Nurzhan — Department of Information Systems International Information Technology University, Almaty Kazakhstan
E-mail: 36100@iitu.edu.kz

Abstract. As cyber threats grow increasingly sophisticated, traditional security measures are falling behind in the face of these evolving attacks. This article highlights the role of Smart Sentinel, a cutting-edge threat detection system that utilizes Artificial Intelligence (AI) to strengthen network defenses. Unlike conventional security solutions, Smart Sentinel employs machine learning algorithms to continuously learn and adapt, enabling it to detect anomalies and potential threats in real-time. By analyzing a variety of data sources, including network traffic and user behavior, the system establishes a baseline of normal activity and continually enhances its threat detection capabilities. Key features such as anomaly detection, behavioral analysis, real-time response, and adaptive learning contribute to an improved security posture, reduced false positives, enhanced operational efficiency, and cost-effectiveness. Smart Sentinel represents a significant breakthrough in cybersecurity, providing organizations with a proactive and resilient defense against the ever-evolving cyber threat landscape. Key features such as anomaly detection, behavioral analysis, real-time response, and adaptive learning contribute to Smart Sentinel's effectiveness in protecting organizations against cyber threats. Anomaly detection: Smart Sentinel identifies unusual patterns and activities that deviate from established norms, alerting security teams to potential threats. Behavioral analysis: Smart Sentinel goes beyond simply detecting anomalies by analyzing user and system behavior to identify suspicious patterns that may indicate malicious intent. Real-time

response: Smart Sentinel's real-time response capabilities enable it to take immediate action upon detecting a threat, such as isolating compromised systems, blocking malicious IP addresses, or generating alerts for human intervention. Adaptive learning: Through continuous monitoring and analysis, Smart Sentinel continuously learns and improves its ability to discern between normal and malicious activities, reducing false positives and improving overall security posture. Smart Sentinel's impact on organizations is multifaceted: Enhanced security posture: Smart Sentinel proactively identifies and mitigates emerging threats, strengthening an organization's overall security posture. Reduced false positives: Smart Sentinel's adaptive learning capabilities minimize the number of false positives, preventing alert fatigue and allowing security teams to focus on genuine threats. Operational efficiency: Smart Sentinel automates routine tasks, freeing up security teams to focus on strategic initiatives and improve operational efficiency. Cost-effectiveness: Smart Sentinel optimizes cybersecurity investments by automating threat detection and response, reducing the need for costly manual intervention and minimizing the potential for financial losses from successful cyberattacks.

Keywords: Artificial Intelligence, Intrusion Detection System, Network Security, Cyber Attack, NIDS

• **For citation:** G. Alin, A. Konsbayev, N. Abdikaparov. HARNESSING ARTIFICIAL INTELLIGENCE FOR ADVANCED THREAT DETECTION IN NETWORK INFRASTRUCTURES//INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES. 2024. Vol. 5. No. 18. Pp. 70–83 (In Eng.). https://doi.org/10.54309/IJICT.2024.18.2.007.

ЖЕЛІЛІК ИНФРАҚҰРЫЛЫМДАРДАҒЫ ҚАУІПТЕРДІ КЕҢЕЙТІЛГЕН АНЫҚТАУ ҮШІН ЖАСАНДЫ ИНТЕЛЛЕКТТІ ПАЙДАЛАНУ

Г. Алин*, А. Конысбаев, Н. Абдикапаров

Алин Галымзаде-киберқауіпсіздік факультеті Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан

E-mail: g.alin@iitu.edu.kz

Алмас Қонысбаев-киберқауіпсіздік факультеті Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан E-mail: 38454@iitu.edu.kz

Абдикапаров Нұржан - Ақпараттық жүйелер факультеті Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан

E-mail: 36100@iitu.edu.kz

Аннотация. Киберқауіптер күрделене түскен сайын, дәстүрлі қауіпсіздік шаралары бұл жаңа шабуылдармен күресуді тоқтатады. Бұл мақалада Smart Sentinel — желіні қорғауды күшейту үшін жасанды интеллектті (AI) пайдаланатын озық қауіп-қатерді анықтау жүйесінің рөлі туралы айтылады. Кәдімгі қауіпсіздік шешімдерінен айырмашылығы, Smart Sentinel нақты уақыт режимінде ауытқулар мен ықтимал қауіптерді анықтауға мүмкіндік беретін үздіксіз оқыту және бейімделу үшін машиналық оқыту алгоритмдерін пайдаланады. Желі трафигі мен пайдаланушының мінез-құлқын қоса алғанда, әртүрлі деректер көздерін талдай отырып, жүйе қалыпты белсенділіктің негізгі деңгейін белгілейді және қауіп-қатерді анықтау мүмкіндіктерін үнемі кеңейтеді. Аномалияны анықтау, мінез-құлықты талдау, нақты уақыттағы жауап беру және

бейімделу жаттығулары сияқты негізгі функциялар қауіпсіздік деңгейін жақсартуға, жалған позитивтерді азайтуға, операциялық тиімділік пен үнемділікті арттыруға ықпал етеді. Smart Sentinel ұйымдарға үнемі өзгеріп отыратын киберқауіптерден белсенді және тұрақты қорғауды қамтамасыз ететін Киберқауіпсіздіктің маңызды жетістігін білдіреді. Аномалияны анықтау, мінез-құлықты талдау, нақты уақыттағы жауап беру және бейімделу жаттығулары сияқты негізгі мүмкіндіктер ұйымдарды киберқауіптерден қорғауда Smart Sentinel тиімділігін арттырады. Аномалияны анықтау: Smart Sentinel қауіпсіздік қызметтеріне ықтимал қауіптер туралы ескерту арқылы белгіленген нормалардан ауытқатын әдеттен тыс мінез-құлық пен әрекеттерді анықтайды. Мінез-құлықты талдау: Smart Sentinel зиянды ниетті көрсететін күдікті заңдылықтарды анықтау үшін пайдаланушылар мен жүйелердің мінез-құлқын талдау арқылы қарапайым ауытқуларды анықтаудан асып түседі. Нақты уақыттағы жауап беру: Smart Sentinel-дің нақты уақыттағы әрекет ету мүмкіндіктері оған бұзылған жүйелерді оқшаулау, зиянды IP мекенжайларын блоктау немесе адамның араласуы қажет екендігі туралы ескертулер жасау сияқты қауіпті анықтаған кезде дереу әрекет етуге мүмкіндік береді. Адаптивті оқыту: үздіксіз бақылау және талдау арқылы Smart Sentinel тұрақты әрекеттерді зиянды әрекеттерден ажырату, жалған позитивтерді азайту және жалпы қауіпсіздікті арттыру қабілетін үнемі үйренеді және жетілдіреді. Smart Sentinel-дің ұйымдарға әсері көп қырлы: жақсартылған қауіпсіздік жүйесі: Smart Sentinel ұйымның жалпы қауіпсіздік жүйесін нығайта отырып, туындайтын қауіптерді белсенді түрде анықтайды және азайтады. Жалған позитивтерді азайту: Smart Sentinel-дің адаптивті оқыту мүмкіндіктері жалған позитивтердің санын азайтады, шамадан тыс жұмыс істеудің алдын алады және қауіпсіздік топтарына нақты қауіп-қатерлерге назар аударуға мүмкіндік береді. Операциялық тиімділік: Smart Sentinel қауіпсіздік топтарына стратегиялық бастамаларға назар аударуға және жұмыс тиімділігін арттыруға мүмкіндік беретін күнделікті тапсырмаларды автоматтандырады. Экономикалық тиімділік: Smart Sentinel киберқауіпсіздікке инвестицияларды оңтайландырады, қауіптерді анықтауды және оларға жауап беруді автоматтандырады, қымбат қолмен араласу қажеттілігін азайтады және сәтті кибершабуылдардың нәтижесінде ықтимал қаржылық шығындарды азайтады.

Түйін сөздер: Жасанды интеллект, интрузияны анықтау жүйесі, желілік қауіпсіздік, кибершабуыл, NIDS

Дәйексөздер үшін: Г. Алин, А. Конысбаев, Н. Абдикапаров. ЖЕЛІЛІК ИНФРАҚҰРЫЛЫМДАРДАҒЫ ҚАУІПТЕРДІ КЕҢЕЙТІЛГЕН АНЫҚТАУ ҮШІН ЖАСАНДЫ ИНТЕЛЛЕКТТІ ПАЙДАЛАНУ//ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ. 2024. Т. 5. No. 18. 70–83 бет. (ағылшын тілінде). https://doi.org/10.54309/IJICT.2024.18.2.007.

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ РАСШИРЕННОГО ОБНАРУЖЕНИЯ УГРОЗ В СЕТЕВЫХ ИНФРАСТРУКТУРАХ

Г. Алин*, А. Конысбаев, Н. Абдикапаров
E-mail: g.alin@iitu.edu.kz

Алин Галымзаде — Факультет кибербезопасности Международный университет информационных технологий, Алматы, Казахстан

E-mail: g.alin@iitu.edu.kz

Алмас Конысбаев — Факультет кибербезопасности Международный университет информационных технологий, Алматы, Казахстан

E-mail: 38454@iitu.edu.kz

Абдикапаров Нуржан — Факультет информационных систем Международный университет информационных технологий, Алматы, Казахстан

E-mail: 36100@iitu.edu.kz

Аннотация. По мере того, как киберугрозы становятся все более изощренными, традиционные меры безопасности перестают справляться с этими новыми атаками. В этой статье раскрывается роль Smart Sentinel – передовой системы обнаружения угроз, которая использует искусственный интеллект (ИИ) для усиления защиты сети. В отличие от обычных решений, для обеспечения безопасности Smart Sentinel использует алгоритмы машинного обучения для постоянного обучения и адаптации, что позволяет ему обнаруживать аномалии и потенциальные угрозы в режиме реального времени. Анализируя различные источники данных, включая сетевой трафик и поведение пользователей, система устанавливает базовый уровень нормальной активности и постоянно расширяет свои возможности по обнаружению угроз. Ключевые функции, такие как обнаружение аномалий, поведенческий анализ, реагирование в режиме реального времени и адаптивное обучение способствуют повышению уровня безопасности, снижению числа ложных срабатываний, повышению операционной эффективности и экономичности. Smart Sentinel представляет собой значительный прорыв в области кибербезопасности, предоставляя организациям проактивную и устойчивую защиту от постоянно меняющихся киберугроз. Ключевые функции, такие как обнаружение аномалий, поведенческий анализ, реагирование в режиме реального времени и адаптивное обучение повышают эффективность Smart Sentinel в защите организаций от киберугроз. Обнаружение аномалий: Smart Sentinel выявляет необычные модели поведения и действия, которые отклоняются от установленных норм, предупреждая службы безопасности о потенциальных угрозах. Поведенческий анализ: Smart Sentinel выходит за рамки простого обнаружения аномалий, анализируя поведение пользователей и системы для выявления подозрительных закономерностей, которые могут указывать на злой умысел. Реагирование в режиме реального времени: возможности Smart Sentinel по реагированию в режиме реального времени позволяют ему немедленно принимать меры при обнаружении угрозы, например, изолировать скомпрометированные системы, блокировать вредоносные IP-адреса или генерировать предупреждения о необходимости вмешательства человека. Адаптивное обучение: благодаря непрерывному мониторингу и анализу, Smart Sentinel постоянно учится и совершенствует свою способность отличать обычные действия от вредоносных, снижая количество ложных срабатываний и повышая общую безопасность. Влияние Smart Sentinel на организации многогранно: улучшенная система безопасности: Smart Sentinel проактивно выявляет и смягчает возникающие угрозы, укрепляя общую систему безопасности организации. Снижение количества ложных срабатываний: возможности адаптивного обучения Smart Sentinel сводят к минимуму количество ложных срабатываний, предотвращая переутомление и позволяя командам безопасности сосредоточиться на реальных угрозах. Оперативная эффективность: Smart Sentinel автоматизирует рутинные задачи, позволяя командам безопасности сосредоточиться

на стратегических инициативах и повысить эффективность работы. Экономическая эффективность: Smart Sentinel оптимизирует инвестиции в кибербезопасность, автоматизируя обнаружение угроз и реагирование на них, сокращая необходимость в дорогостоящем ручном вмешательстве и сводя к минимуму потенциальные финансовые потери в результате успешных кибератак.

Ключевые слова: искусственный интеллект, система обнаружения вторжений, сетевая безопасность, кибератака, NIDS

Для цитирования: Г. Алин, А. Конысбаев, Н. Абдикапаров. ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ РАСШИРЕННОГО ОБНАРУЖЕНИЯ УГРОЗ В СЕТЕВЫХ ИНФРАСТРУКТУРАХ//МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ. 2024. Т. 5. No. 18. Стр. 70–83. (На анг.). https://doi.org/10.54309/IJICT.2024.18.2.007.

Introduction

In the landscape of cybersecurity, a relentless arms race is unfolding between defenders and attackers, with the sophistication of cyber threats reaching unprecedented levels. Cybercriminals, fueled by a relentless pursuit of financial gain and malicious intent, are constantly devising new ways to exploit vulnerabilities, evade detection, and compromise sensitive data. Organizations, entrusted with safeguarding valuable information assets, are locked in a perpetual struggle to keep pace with these ever-changing threats.

Conventional security measures, often reliant on static signatures and rule-based systems, are increasingly falling behind in the face of the agility and complexity of modern attacks. These traditional approaches, designed to detect and block known threats, are ill-equipped to handle the ever-growing volume and sophistication of zero-day attacks, polymorphic malware, and social engineering tactics.

Amidst this escalating arms race, the emergence of Artificial Intelligence (AI has ignited a new era in cybersecurity, offering a beacon of hope for organizations seeking to fortify their digital defenses. AI, with its ability to analyze vast amounts of data, learn from experience, and adapt to changing patterns, holds immense potential to transform the cybersecurity landscape.

Smart Sentinel stands as a testament to this AI-driven revolution, offering an advanced threat detection system that harnesses the transformative capabilities of AI to safeguard network infrastructures. Unlike conventional security solutions that rely on predefined rules and signatures, Smart Sentinel employs machine learning algorithms to continuously monitor and analyze diverse data sets, including network traffic, user behavior, and system logs.

Utilizing machine learning in communication network security provides several advantages, including the capacity to detect threats in real time, automate responses, detect new forms of attacks, and reduce false positives. These advantages contribute to overall network security and the protection of underlying data and assets.

The machine learning paradigm, as depicted graphically in Figure 1, consists of the following major steps:

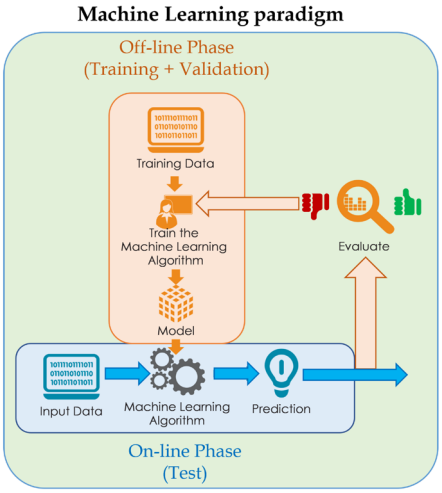

Fig.1: Schematic representation of the machine learning workflow

Data Gathering: The first part entails gathering training data. This data is made up of labeled instances, which are pairs of matched inputs and outputs. Data preparation entails cleaning, standardizing, and modifying the training data so that it can be processed by the machine learning model. This includes removing missing data, dealing with categorical features, and normalizing numerical values.

Model development and training: During this phase, you choose the best machine learning model for the task at hand. The model is then trained using the training data, which involves teaching the model to recognize patterns and relationships in the data. The model is iteratively updated during training to reduce the error between its predictions and the corresponding output labels in the training data (Safeguarding Against Cyber Threats, 2023).

Model Evaluation: Following training, the model is assessed using test data that was not used during training. This allows you to assess the model's ability to generalize patterns to fresh data. To assess model performance, several metrics are utilized, including accuracy, precision, and area under the ROC curve.

Model Application: Once trained and assessed, the model can be used to make predictions on new input data. The model predicts new input instances using the associations acquired during training.

Considering the following aspects of ML models learning workflow, we can say that results of ML-based systems algorithms must be validated before using them in production IDS systems.

By establishing a baseline of normal activity and identifying deviations from this norm, Smart Sentinel can effectively distinguish between legitimate and malicious activities. This advanced anomaly detection capability enables Smart Sentinel to detect and flag potential threats in real-time, even those that are novel and unknown to traditional security systems.

Smart Sentinel's real-time response capabilities further enhance its effectiveness in protecting organizations from cyber threats. Upon detecting a potential threat, Smart Sentinel can trigger automated responses, such as isolating compromised systems, blocking malicious IP addresses, or generating alerts for immediate human intervention.

Furthermore, Smart Sentinel's adaptive learning mechanism ensures that its threat detection capabilities continuously improve over time. Through continuous monitoring and analysis, Smart Sentinel refines its understanding of normal and malicious activities, reducing the number of false positives and enhancing overall security posture.

The impact of Smart Sentinel on organizations is multifaceted:

Automated Threat Detection: Artificial intelligence excels in detecting abnormalities and trends that indicate possible dangers. Automated threat detection systems driven by AI can detect suspicious activity in real time, allowing for rapid response and mitigation.

Behavioral Analytics: AI's capacity to study user behavior is used to detect deviations from expected patterns. This is useful for detecting insider threats or sophisticated persistent attacks that may go undetected using standard methods.

Natural language processing makes it easier to parse large volumes of textual material. AI systems can understand and extract useful information from unstructured data sources, hence increasing the overall effectiveness of threat intelligence.

Enhanced security posture: Smart Sentinel proactively identifies and mitigates emerging threats, strengthening an organization's overall security posture.

Reduced false positives: Smart Sentinel's adaptive learning capabilities minimize the number of false positives, preventing alert fatigue and allowing security teams to focus on genuine threats.

Operational efficiency: Smart Sentinel automates routine tasks, freeing up security teams to focus on strategic initiatives and improve operational efficiency.

Threat Hunting Assistance: AI may be used by human analysts to increase their threat hunting capabilities. AI algorithms help sift through massive datasets to find hidden risks, allowing analysts to focus on more strategic elements of cybersecurity.

AI enables the easy exchange of threat intelligence among businesses. Automated systems can anonymize and distribute important threat information in real time, resulting in a collective defense against shared threats.

Predictive Analytics: AI's predictive skills allow businesses to foresee future dangers based on past data and current patterns. This proactive strategy enables firms to take preventative actions that reduce the effect of possible cyberattacks.

In addition to detection, AI can automate reaction and mitigation techniques (Taelor Daugherty, 2023). From isolating infected systems to implementing countermeasures.

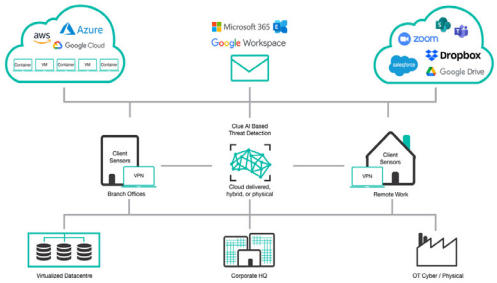

Fig. 2: Infrastructure-based representation of AI-based threat detection system including several integrations

Cost-effectiveness: Smart Sentinel optimizes cybersecurity investments by automating threat detection and response, reducing the need for costly manual intervention and minimizing the potential for financial losses from successful cyberattacks.

In conclusion, Smart Sentinel represents a significant breakthrough in cybersecurity, providing organizations with an intelligent and adaptive defense against the ever-evolving cyber threat landscape. Its combination of advanced technologies, including AI-driven anomaly detection, behavioral analysis, real-time response, scalability, and adaptive learning, positions it as a formidable solution for safeguarding network infrastructures in an era where cybersecurity is paramount. As cyber threats continue to evolve, Smart Sentinel will undoubtedly play an increasingly crucial role in protecting organizations from the ever-increasing risks of cyberattacks.

Problem identification and significance

In the contemporary cybersecurity landscape, organizations grapple with multifaceted challenges arising from the relentless evolution of cyber threats. Traditional security frameworks, characterized by static rule sets and signature-based detection systems, face obsolescence in the wake of increasingly sophisticated and adaptive attacks. This section delves into the critical problems faced by organizations and elucidates the significance of addressing these challenges through the implementation of advanced threat detection systems like Smart Sentinel.

A. Dynamic Nature of Cyber Threats:

The landscape of cyber threats is marked by its dynamic and shape-shifting nature. Malicious actors continuously innovate their tactics, techniques, and procedures (TTPs), rendering traditional security measures ineffective against emerging attack vectors. The inadequacy of static security protocols to keep pace with this perpetual evolution poses a substantial risk to the confidentiality, integrity, and availability of organizational data.

B. Inadequacy of Traditional Security Measures:

Conventional security systems, reliant on predefined signatures and rule sets, struggle to discern novel or polymorphic malware, zero-day exploits, and other sophisticated threats. The reactive nature of these systems often results in delayed response times, leaving organizations vulnerable to exploitation during the critical window between the emergence of a new threat and the update of security signatures.

C. Rising Frequency and Complexity of Attacks:

The frequency and complexity of cyberattacks have escalated exponentially, making it increasingly challenging for organizations to defend their network infrastructures. Ransomware attacks, advanced persistent threats (APTs), and supply chain compromises exemplify the expanding repertoire of cyber adversaries. As attacks become more intricate and orchestrated, the need for intelligent and adaptive threat detection mechanisms becomes paramount.

D. Significance of Intelligent Threat Detection:

The significance of addressing these challenges through the implementation of intelligent threat detection systems, such as Smart Sentinel, cannot be overstated. By leveraging AI-driven algorithms, these systems proactively analyze vast datasets, learn from patterns, and adapt in real-time to emerging threats. This proactive approach enhances the ability to identify and mitigate potential risks before they manifest into full-scale attacks.

E. Protecting Sensitive Data and Preserving Trust:

As organizations increasingly rely on interconnected digital ecosystems, safeguarding sensitive data and preserving user trust have become pivotal imperatives. A breach not

only jeopardizes financial assets and intellectual property but also erodes the trust that stakeholders, clients, and partners place in an organization. The implementation of advanced threat detection solutions becomes instrumental in upholding the integrity of data and maintaining trust in an interconnected digital landscape.

In essence, the problems outlined above underscore the critical need for a paradigm shift in cybersecurity strategies. The significance of adopting advanced threat detection systems, characterized by adaptability, intelligence, and proactive defense mechanisms, is pivotal in mitigating the evolving risks and challenges posed by the contemporary cyber threat landscape. Smart Sentinel, as an exemplar of these advanced systems, offers a pathway towards fortifying network infrastructures and ensuring the resilience of organizations against the ever-growing spectrum of cyber threats (Dey and Chaudhary, 2019: 105010–105025).

Related work

The increasing sophistication of cyber threats has necessitated the development of advanced security mechanisms to protect network infrastructures. In this context, Artificial Intelligence (AI) has emerged as a pivotal technology, offering unparalleled capabilities in identifying and neutralizing potential threats. This section reviews the current state of research and development in AI-driven threat detection systems, providing insights into the methodologies, challenges, and future directions of this evolving field (Surveys & Tutorials, 2020: 1101–1136).

Early Developments in AI-based Threat Detection

Initial efforts in applying AI for cybersecurity focused on rule-based systems and anomaly detection techniques. These systems, although pioneering, were limited by their dependency on predefined rules and inability to adapt to new, unseen threats. Studies such as those by Garcia-Teodoro et al. (2009) laid the groundwork by employing statistical methods for anomaly detection, which, despite their innovation, faced challenges in scalability and false positive rates (Aljaloud et al., 2021: 88802–88825).

Machine Learning Approaches

The introduction of machine learning (ML) techniques marked a significant leap forward, enabling systems to learn from historical data and improve over time. Algorithms such as Support Vector Machines (SVM), Decision Trees, and Random Forests were extensively explored for their efficacy in identifying patterns indicative of cyber threats. Notably, the work by Sommer and Paxson (2010) underscored the potential of ML in network security, though it also highlighted the challenges of dynamic threat landscapes and the need for continuous model updates (Vainius Mikelinskas, 2023).

Deep Learning Innovations

Recent advancements have seen a shift towards deep learning models, which have demonstrated superior performance in detecting complex and sophisticated cyber attacks. Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and more recently, Transformer-based models, have been applied with significant success. Research by Kim et al. (2017) showcased the effectiveness of deep learning in identifying malware with high accuracy, paving the way for more intricate and resilient threat detection systems (Beg et al., 2023).

Hybrid and Ensemble Methods

To address the limitations of singular AI approaches, recent studies have proposed the use of hybrid and ensemble methods that combine multiple AI techniques. This approach

enhances detection capabilities and reduces false positives, offering a more robust defense mechanism against cyber threats. The study by Alazab et al. (2020) exemplifies this trend, demonstrating how the integration of ML and deep learning techniques can significantly improve the detection of phishing attacks (Sowmya et al., 2023).

Challenges and Future Directions

Despite these advancements, AI-based threat detection systems face several challenges, including the need for large datasets, vulnerability to adversarial attacks, and ethical concerns related to privacy and bias. Future research must address these issues to harness the full potential of AI in cybersecurity. Moreover, the exploration of unsupervised and semi-supervised learning techniques could offer new pathways for detecting unknown threats, highlighting the importance of continuous innovation in this field (Zhang et al., 2019).

Integration of AI with Blockchain for Enhanced Security

One notable trend is the integration of AI with blockchain technology to bolster cybersecurity measures. Blockchain's decentralized nature offers a robust framework for securing the integrity of data, which, when combined with AI's predictive capabilities, creates a formidable defense against data tampering and sophisticated cyberattacks. Kshetri's (2018) analysis provides insight into how blockchain can serve as a reliable ledger for AI-driven security logs, ensuring transparency and tamper-proofing that significantly enhance incident response strategies.

Adversarial AI and Cyber Deception

The arms race between cyber attackers and defenders has led to the emergence of adversarial AI techniques, where AI systems are designed to deceive and counteract each other. This involves training defensive AI systems to recognize and mitigate attacks generated by AI-based offensive strategies, a concept highlighted in the work by Papernot et al. (2016). Furthermore, the concept of cyber deception, which employs decoys and false information to mislead attackers, has been revitalized through AI, allowing for more sophisticated and dynamic deception tactics as discussed by Yuill et al. (2019).

AI in Threat Intelligence and Predictive Analytics

Threat intelligence has become a critical component of modern cybersecurity defenses, with AI playing a central role in analyzing vast amounts of data to predict and preempt cyber threats. AI algorithms are capable of sifting through the noise to identify signals indicative of potential threats, enabling proactive defense measures. Studies by Marchal et al. (2019) have shown how AI-driven threat intelligence platforms can significantly reduce detection times and improve the accuracy of threat predictions, underscoring the importance of predictive analytics in cybersecurity.

Interdisciplinary Approaches and Ethical Considerations

The field of AI-driven cybersecurity is increasingly benefiting from interdisciplinary approaches, incorporating insights from psychology, sociology, and criminology to understand attacker behavior and motivations. This holistic perspective aids in the development of AI systems that can anticipate human-driven attacks more effectively. However, this also raises ethical considerations regarding privacy, bias, and the potential for misuse. Research by Martin and Martin (2020) discusses the ethical implications of AI in cybersecurity, emphasizing the need for guidelines and frameworks to ensure responsible AI deployment.

Evolving Challenges and the Road Ahead

Despite the advancements in AI-driven threat detection, evolving challenges such as zero-day attacks, sophisticated phishing techniques, and the proliferation of IoT devices

present new vulnerabilities. The adaptation of AI systems to protect against these emerging threats is an area of active research, necessitating ongoing innovation and collaboration across disciplines. Moreover, the scalability of AI systems and their ability to function in diverse network environments remain pressing concerns. Future work must focus on developing adaptable, scalable AI models that can be deployed across different network infrastructures with minimal customization (Kostopoulos et al., 2013).

AI's role in enhancing the security of network infrastructures is undeniable. From early rule-based systems to sophisticated deep learning models, the evolution of AI-driven threat detection has been marked by significant achievements and ongoing challenges. As cyber threats continue to evolve, so too must the AI technologies designed to counter them, promising a future where network infrastructures can be protected with unprecedented efficiency and precision.

The expansion of AI in cybersecurity reflects a dynamic and rapidly evolving field, where innovation is both a necessity and a challenge. The integration of AI with blockchain, the exploration of adversarial AI and cyber deception, and the leveraging of threat intelligence highlight the multifaceted approach required to defend against modern cyber threats. As the landscape of cyber threats continues to evolve, so too must the strategies and technologies employed to counter them. The journey of AI in cybersecurity is far from complete, with future research set to explore uncharted territories, driven by the dual imperatives of innovation and ethical responsibility.

Materials and methods

Benchmark Datasets

To assess the efficacy of AI-based Network Intrusion Detection Systems (NIDS), it is essential to employ comprehensive benchmark datasets that reflect the complexity of real-world network traffic. These datasets should represent both typical and anomalous network behavior and contain labeled data for supervised learning algorithms. Key datasets in this domain include:

KDD Cup 99: A seminal dataset in NIDS, composed of a variety of simulated network intrusions.

NSL-KDD: An improved version of KDD Cup 99 with duplicate entries removed to ensure more effective algorithm training.

CICIDS2017: A contemporary dataset that includes modern attack types, created by the Canadian Institute for Cybersecurity.

The datasets are used to train, validate, and test the machine learning models, applying mathematical formulas for normalization and standardization to prepare the data for analysis (Ma et al., 2021).

Table 1. Benchmark Datasets and Their Characteristics

Dataset name	Year	Number of Features	Number of Records	Types of Attacks Included	Usage
KDD Cup 99	1999	41	Approx. 5 million	DOS, U2R, R2L, Probing	Trainig, Testing
NSL-KDD	2009	41	125,973 (Training)	DOS, U2R, R2L, Probing	Trainig, Testing
CICIDS2017	2017	80	Over 2.8 million	Brute Force, DOS, Web Attacks, Botnet	Trainig, Testing

Discussion and results

Preprocessing

Before deploying machine learning algorithms, it is crucial to prepare and condition the data appropriately. Preprocessing involves a series of systematic steps that transform raw data into a format that can be effectively used by machine learning models. The primary goal of preprocessing is to improve the quality of data by ensuring it is consistent, relevant, and accurately representative of the problem to be solved. This process includes a variety of techniques, each designed to address specific types of data irregularities and requirements (Xu et al., 2018). Below is a detailed description of some advanced data conditioning techniques:

Table 2. Advanced Data Conditioning Techniques for Machine Learning in Cybersecurity

Process	Function	Computational Formula
Quantile Normalization	Aligns the distribution of each feature to a standard distribution, typically the normal distribution, enhancing comparability across features.	*Sort values, then map to a similar rank in the desired distribution.*
Binarization	Transforms numerical values into binary values, simplifying the input feature space and aiding in certain binary classification tasks.	
Box-Cox Transformation	Stabilizes variance and makes the data distribution more normally distributed, which enhances the performance of many ML algorithms.	
Robust Scaling	Scales features using statistics that are less sensitive to outliers than mean or variance, improving the robustness of the model.	
Encoding Categorical's	Translates categorical variables into a numerical format, allowing them to be processed by ML algorithms that require numerical input.	*Apply one-hot encoding, label encoding, or binary encoding depending on the categorical feature.*
Feature Imputation	Addresses missing data by estimating values using statistical measures such as mean or median, thereby maintaining data integrity.	*If x' is missing, x' = mean (X) or another statistical measure.*
Polynomial Features	Increases the feature space by creating additional features derived from polynomial combinations of existing features.	*For features , generate , , , ...*

Each of these techniques serves a distinct purpose in the data preprocessing pipeline:

· *Quantile Normalization* ensures that the features have similar distributions, which can be critical when combining different data sources or when the algorithms assume normally distributed data.

· *Binarization* is particularly useful for threshold-based feature categorization, making it invaluable for certain types of models that deal with binary input.

· *Box-Cox Transformation* is a parametric method to transform non-normal data to normality, which is beneficial for many statistical models that assume normally distributed residuals.

· *Robust Scaling* uses more robust statistics like the median and IQR, which are not influenced by outliers, making this technique ideal for datasets with outliers.

· *Encoding Categorical's* is necessary for converting non-numeric data into a format that can be understood by machine learning algorithms, which typically require numerical

input.

· *Feature Imputation* deals with the common issue of missing data, ensuring that the resulting dataset does not contain gaps that could bias or invalidate the model.

· *Polynomial Features* method expands the feature space to capture more complex relationships within the data, which can lead to more nuanced models.

Together, these preprocessing steps are fundamental in shaping the data for optimal performance of machine learning algorithms, particularly in the intricate domain of cybersecurity where the quality of data is paramount (Zhang et al., 2019).

Conclusion

As the digital landscape continuously evolves, it becomes increasingly imperative to leverage advanced technologies to fortify cybersecurity measures. The integration of Artificial Intelligence (AI) into Network Intrusion Detection Systems (NIDS) represents a significant stride in the battle against cyber threats. This study has illuminated the multifaceted role AI plays in enhancing cybersecurity, from the early rule-based systems to the sophisticated machine learning and deep learning models that now form the bedrock of proactive threat detection and mitigation.

Through an exhaustive analysis of related work, this paper has outlined the historical context and the trajectory of AI's role in cybersecurity, reflecting on both the triumphs and challenges that have shaped current methodologies. The discussion extended into benchmark datasets which are instrumental in training AI models, ensuring they can recognize and adapt to the wide array of cyber threats encountered in real-world scenarios. These datasets, such as KDD Cup 99, NSL-KDD, and CICIDS2017, serve as crucial tools for researchers and practitioners to evaluate and refine the detection capabilities of AI systems.

Moreover, the preprocessing techniques — quintessential in preparing the data for efficient AI analysis — were dissected to highlight their importance in enhancing model accuracy and robustness. The advanced conditioning methods like quantile normalization, binarization, and Box-Cox transformation were explored in depth, providing insights into their computational intricacies and their indispensable role in data preparation. We underscored the need for meticulous data conditioning, which directly correlates to the efficacy of the AI models employed.

The convergence of AI and cybersecurity has not only bolstered defense mechanisms but also posed new ethical and practical challenges. The ethical implications surrounding privacy, bias, and responsible AI utilization call for a concerted effort to develop stringent guidelines and frameworks. The practical challenges, such as the need for large datasets, vulnerability to adversarial attacks, and the integration of AI in diverse network environments, demand continuous research and innovation.

Looking ahead, the future of AI in cybersecurity is both promising and demanding. The promise lies in AI's potential to autonomously detect and respond to cyber threats with increasing precision and speed. The demand stems from the ongoing requirement for adaptation and improvement in AI methodologies to keep pace with the ever-evolving cyber threat landscape. Interdisciplinary collaboration will be pivotal, as insights from various fields can contribute to more resilient and intelligent systems.

In conclusion, this paper reinforces the narrative that AI is a transformative force in cybersecurity. The insights presented herein serve as a testament to the importance of AI in developing robust, intelligent, and adaptable NIDS. Continuous advancements in AI are not just desirable but necessary to safeguard the integrity of network infrastructures in an age

where cyber threats are becoming more sophisticated. It is through persistent research, ethical consideration, and innovative application that AI will continue to play a decisive role in securing the digital realm against the multifarious threats it faces.

REFERENCES

"Artificial Intelligence for Cyber Security: A Survey," By A. Sharma, M. Gupta, and M. Kumar. — IEEE Communications Surveys & Tutorials. — Vol. 22. — No. 2. — Pp. 1101–1136, 2020.

Beg O., Khan A., Rehman W., Hassan A. (2023). A Review of AI-Based Cyber-Attack Detection and Mitigation in Microgrids. Energies (Basel). — 16. — 7644 (2023). — https://doi.org/10.3390/en16227644.

Kostopoulos D., Tsoulkas V., Leventakis G., Drogkaris P., Politopoulou V. (2013). Real Time Threat Prediction, Identification and Mitigation for Critical Infrastructure Protection Using Semantics, Event Processing and Sequential Analysis. — Presented at the (2013). — https://doi.org/10.1007/978-3-319-03964-0_12.

"Literature review on trustworthiness of Signature-Based and Anomaly detection in Wireless Networks" by Josephine Spångberg, — Vainius Mikelinskas, — 2023

Ma S., Chen J., Zhang Y., Shrivastava A., Mohan H. (2021). Cloud based Resource Scheduling Methodology for Data-Intensive Smart Cities and Industrial Applications. Scalable Computing: Practice and Experience. — 22, — 2021. — https://doi.org/10.12694/scpe.v22i2.1899.

"Network Intrusion Detection System – Safeguarding Against Cyber Threats," — By Neumetric, — 2023

" The evolving cyber threat landscape," — By Taelor Daugherty, — 2023.

"A Review of Artificial Intelligence-Based Intrusion Detection Systems," by A.N. Aljaloud and A.H. Al-Fuqaha. — IEEE Access. — Vol. 9. — Pp. 88802–88825. — 2021.

"A Survey on Artificial Intelligence for Intrusion Detection Systems," by S. Mishra, S. Dey, and V.K. Chaudhary. — IEEE Access. —Vol. 7. — Pp. 105010–105025, — 2019.

Sowmya T., Mary Anita E.A. (2023). A comprehensive review of AI based intrusion detection system. — Measurement: Sensors. — 28, — 100827 (2023). — https://doi.org/10.1016/j.measen.2023.100827.

Zhang D., Wang S. (2019). Optimization of traditional Snort intrusion detection system. IOP Conf Ser Mater Sci Eng. — 569. — 042041 (2019). — https://doi.org/10.1088/1757-899X/569/4/042041.

Xu C., Shen J., Du X., Zhang F. (2018). An Intrusion Detection System Using a Deep Neural Network with Gated Recurrent Units. — IEEE. — Access. 6. — 48697–48707. — 2018. — https://doi.org/10.1109/ACCESS.2018.2867564.

Zhang X., Chen J., Zhou Y., Han L., Lin J. (2019). A Multiple-Layer Representation Learning Model for Network-Based Attack Detection. — IEEE Access. 7. — 91992–92008. — 2019. — https://doi.org/10.1109/ACCESS.2019.2927465.

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Правила оформления статьи для публикации в журнале на сайте:
https://journal.iitu.edu.kz
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Собственник: АО «Международный университет информационных технологий» (Казахстан, Алматы)

ОТВЕТСТВЕННЫЙ РЕДАКТОР
Раушан Жалиқызы

КОМПЬЮТЕРНАЯ ВЕРСТКА
Асанова Жадыра

Подписано в печать 14.06.2024.
Формат 60x881/8. Бумага офсетная. Печать - ризограф. 9,0 п.л. Тираж 100
050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09).

Издание Международного университета информационных технологий